Pradish Dadhania, Sachin Patel / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 1, January -February 2013, pp.1487-1491

Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks

Pradish Dadhania*, Sachin Patel**
*(Department of Information Technology, RGPV University, Indore (INDIA)
** (Department of Information Technology, RGPV University, Indore (INDIA)

ABSTRACT
The Wireless mobile ad hoc network (MANET) is a self-configuring network which is composed of several movable mobile nodes. These mobile nodes communicate with each other without any infrastructure. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In Black Hole attack, a malicious node falsely advertises shortest path to the destination node and absorbs all data packets in it. In this way, all packets in the network are dropped. In this paper, performance of AODV and DSR are evaluated in presence of black hole attack (malicious node) and without black hole attack with CBR traffic under different scalable network mobility.
In this paper, via simulation, we evaluate effect and compare it with standard protocol in terms of throughput, Packet delivery ratio and End to End Delay. We have conducted extensive experiments using the network simulator-2 to validate our research.

Keywords - MANET, ADOV, DSR, Black hole,

I. INTRODUCTION
The mentioned before an ad hoc network is a wireless network, which do not have a centralized and fixed infrastructure. MANET is referred to as a wireless ad hoc network in which nodes are free to move arbitrarily and mobile nodes can transmit and receive the traffic. Also mobile nodes can act like routers by forwarding the neighbors traffic to the destination node as the routers are multi hop devices [8]. MANET does not need base stations of wired infrastructure. The mobile nodes in wireless network range can communicate with each other because it is a self organized network. The mobile nodes form a network automatically without a fixed infrastructure and central management [8]. The mobile nodes have transmitters and receivers with smart antennas, which enable the mobile nodes to communicate with each others.

The topology of the network changes every time by getting in and out of the mobile nodes in the network. In the beginning MANET was designed for military use but now the MANET is used in many areas. Such as in disaster hit areas, data collection in some region, in rescue missions, virtual classes and conferences [8]. This concept with ad hoc network makes the full name of mobile ad hoc network (MANET). By growing the network, combined with the node mobility the challenges of self configuration of the network become more evident.

Security in MANET is a very critical and important issue and many techniques were defined for the security of MANET. Intrusion detection technique is investigated in [8].Mobile nodes in the network waste much energy by joining in and out with connection to wireless network. This connection and reconnection create energy limitation in the wireless network. The main purpose of developing the ad hoc routing protocols is to cope with the dynamic nature of MANET. The routing protocols efficiency can be determined by the battery power consumption. Energy is consumed during participation of a node in a network and also in routing of traffic.

There are mainly three types of routing protocol and they are proactive, reactive and hybrid routing protocol. Proactive routing protocol is table driven where as reactive routing protocol is on demand routing protocol. AODV and DSR both are on demand protocol. But the difference between both of these is, DSR a route cache is maintained and due to this over head of memory increases. But in case of AODV, it is a source initiate routing protocol. I n this, routing table is maintained by every mobile node and this routing table consist of next node information for a route to the destination node. The intermediate nodes between the source and destination are responsible for finding a fresh path to the destination in route discovery process of AODV protocol. Malicious node immediately responses to such route discovery process giving false information of having a fresh enough path to destination. Source node assumes that it is sending data packets through a true path but actually it sending the data packets to malicious node. Apart from the malicious node, black hole attack can occur due to damaged node, unintentionally dropping of data packets.

II. OVERVIEW OF AODV AND DSR ROUTING PROTOCOLS

2.1 The Ad hoc on-Demand Distance Vector PROTOCOL

AODV is on demand routing, means it start its routing process only when any node in the network desire to transmit the data packets. In AODV, next hop information is started by each node in it a routing table. When a source node cannot reach to the destination node directly, then the source node will immediately initiate a route discovery process. AODV uses several control packets like Route Request (RREQ), Route Reply (RREP) and Route Error Process (RERR). RREQ message is broadcasted, RREP message is unicasted back to source of RREQ, and RERR message is used to notify the loss of link to other node. Route discovery is initiated by broad casting a RREQ to its neighbor and this RREQ is rebroadcasted to their neighbor until it reaches to the destination node. When destination node receives the RREQ, it sends the RREP message to the sender node Routes are maintained in the source node as long as they are needed. Routing table are maintained by every node and have fields like destination, number of hops, next hops, destination sequence number, life time, active neighbor. To find the freshness of route towards destination, sequence number is used. Attacks on AODV can be performed easily as AODV does not have any centrally administered secure routers. Attackers from outside or inside can easily exploit the network. AODV supports shared wireless medium and dynamic topology. It is capable of both unicast and multicast routing. It avoids count to infinity problem of other Distance –vector protocol. It is flat routing protocol and does not need any central administrative system to handle the routing process. It does not require any permanent link between the nodes to transfer data. For transferring the data temporary link would suffice for time being. AODV needs less protection of control message. It is enough to protect RREQ and RREP message in order to provide the security to the protocol.

2.2 Dynamic Source Routing protocol

Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks and was proposed for MANET by Broch, Johnson, and Maltz [2]. In a nutshell, it works as follows: Nodes send out a ROUTE REQUEST message, all nodes that receive this message put themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or are gratuitous. After receiving one or several routes, the source selects the best (by default the shortest), stores it, and sends messages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. When a ROUTE REPLY arrives very quickly after a ROUTE REQUEST has been sent out this is an indication of a short path, since the nodes are required to wait for a time corresponding to the length of the route they can advertise, before sending it. This is done in order to avoid a storm of replies. In case of a link failure, the node that cannot forward the packet to the next node sends an error message towards the source. Routes that contain a failed link can be `salvaged' by taking an alternate partial route that does not contain the bad link.

3 BLACK HOLE ATTACKS ON MANET

MANETs face various securities threats i.e. attack that are passed out against them to interrupt the normal performance of the networks. Black hole attack is one of the security threat in which the traffic is redirect to such a node that actually does not exist in the network. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). In black hole attack, a malicious node uses its routing protocol in order to endorse itself for having the shortest path to the destination node or to the packet it wants to interrupt. This destructive node advertises its availability of new routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [6]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the response of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it is up to the node whether to drop all the packets or promote it to the unknown address [7]. The black hole attack has two properties. First, the node exploits the mobile ad-hoc routing protocol, such as AODV, to promote itself as having a valid route to a target node, even though the route is false, with the aim of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will check and represent the

ongoing attacks. There is a more delicate form of these attacks when an attacker selectively forward packets. An attacker suppress or modifies packets originating from some nodes, while leaving the data from the other nodes unchanged, which limits the suspicion of its wrongdoing.

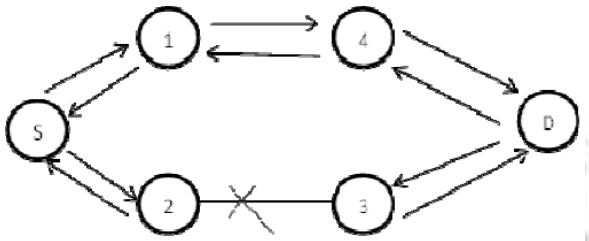


Fig: 1 - BLACK HOLE ATTACKS

4 SIMULATION SET UP

The simulation is implemented In Network Simulator 2 [8], a simulator for mobile Adhoc networks. The simulation parameters are provided in Table 3. We implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen between 0 m/s to the maximum simulation speed. A packet size of 512 bytes and a transmission rate of 4 packets/s,congestion of the network are not likely to occur.

Parameter Value

Examined Protocol	AODV DSR
Application traffic	CBR
Transmission range	250 m
Packet size	512 bytes
Transmission rate	4 packets/sec
Pause time	10 s
Maximum speed	20 m/s
Simulation time	1000 s
Number of nodes	10,20,30,40,50 (attack result on only 50 nodes)
Area	1000 m * 1000 m
Propagation Model	Free space
Maximum Malicious nodes	10/4
Movement Model	Random waypoint
Types of attack	Black-hole

5 RESULTS AND DISCUSSIONS

To ensure a high-quality product, diagrams and lettering MUST be either computer-drafted or drawn using India ink.

5.1 DSR and AODV are with 50 nodes without attack.

Considering the mobility of nodes and the network size, the overall performance of the protocols can be compared in terms of three parameters:

5.1.1 Throughput

Throughput or network throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. From graph we can analyze as number of node increase in network throughput gets better.

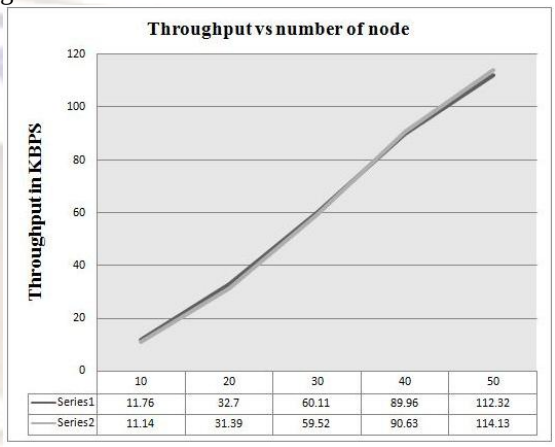


Fig: 2 throughput Of DSR(Sesr.1) and AODV(ser.2)

5.1.2 Average end-to-end delay of data packets

There are possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. Once the time difference between every CBR packet sent and received was recorded, dividing the total time difference over the total number of CBR packets received gave the average end-to-end delay for the received packets. This metric describes the packet delivery time: the lower the end-to-end delay the better the application performance.

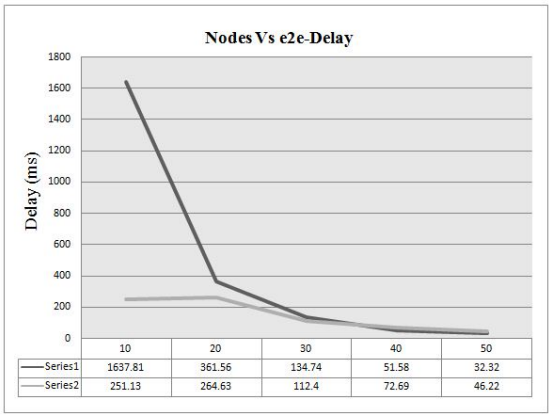


Fig: 3 Average end-to-end delay Of DSR (Series 1) and AODV (series 2)

5.1.3 Packet Delivery Ratio

Packet delivery ratio can be calculated as the ratio between the number of data packets that are sent by the source and the number of data packets that are received by the sink. Graph shows as the number of node increase it gets better because probability of path breakage decrease.

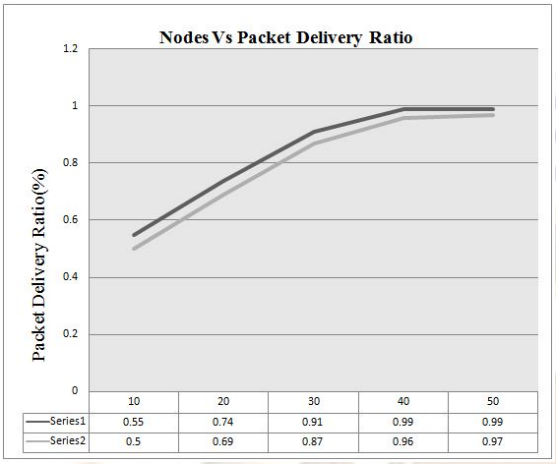
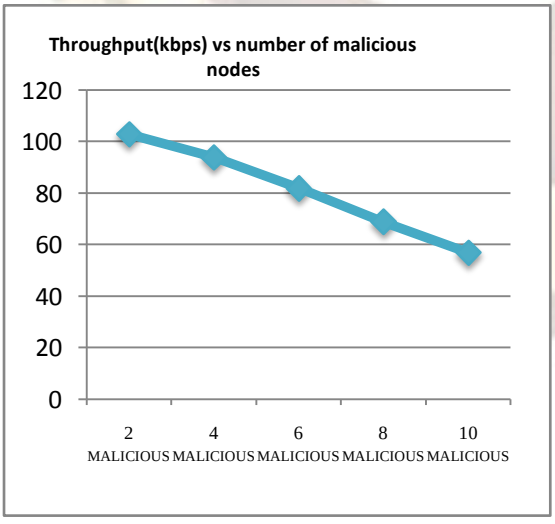


Fig 4 Packet Delivery Ratio of DSR (Series 1) and AODV (series 2)

5.2 DSR and AODV are with 50 nodes with attack.

It is observed from the Fig that, the impact of the Black hole attack to the Networks throughput. The throughput of the network also decreases due to black hole effect as compared to without the effect of black hole attack. We vary the speed of the node and take the result to the different node speed.



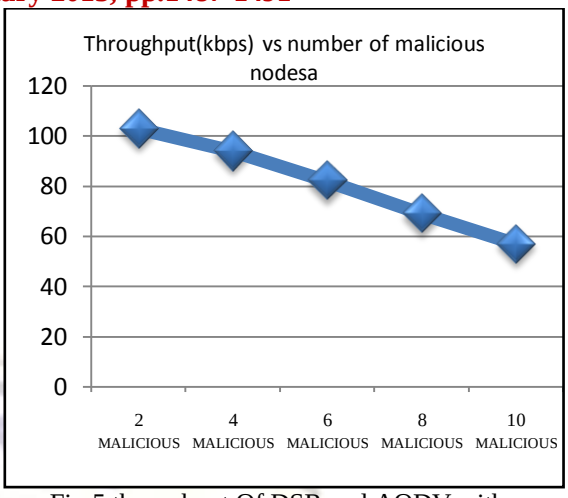


Fig 5 throughput Of DSR and AODV with malicious nodes

Fig shows the graph for end to end delay. Graph shows as the number of malicious node increase it gets decrease output. In the DSR End to end delay is decreased and in AODV that increased.

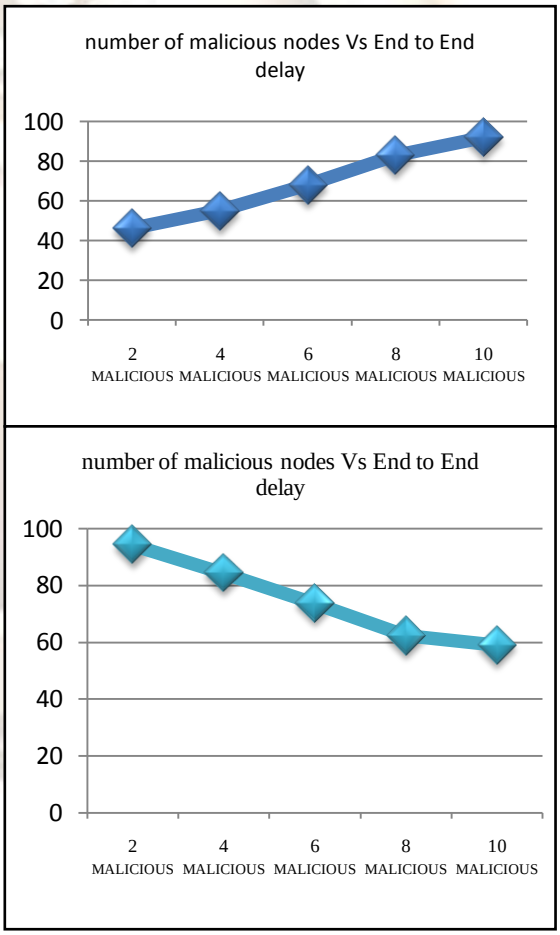


Fig 6 Average end-to-end delay Of DSR and AODV with malicious nodes

Fig shows the graph plotted between the numbers of malicious nodes and the packet delivery ratio. It

is inferred from the graph that since there is no mechanism available to detect malicious node in DSR, the packet delivery ratio decreases as the no of malicious node increases.

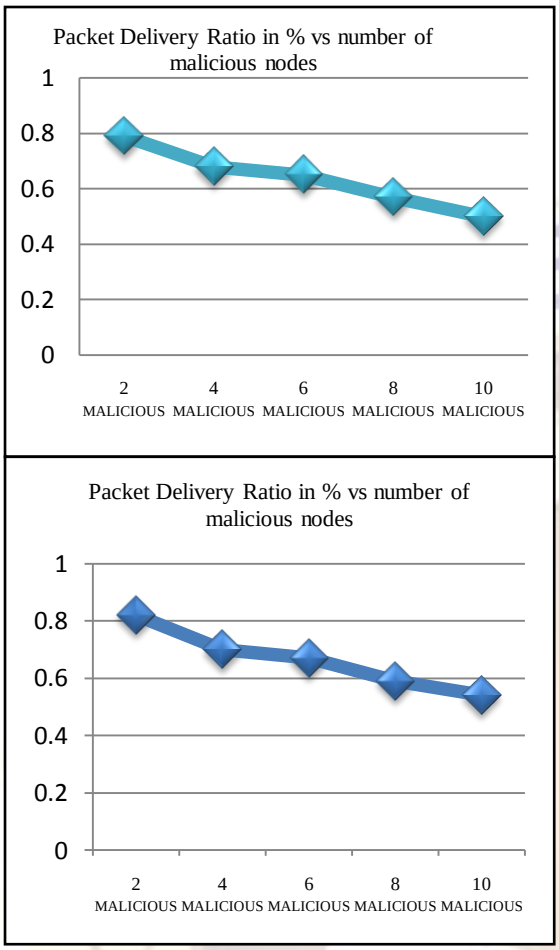


Fig 7: Packet Delivery Ratio Of DSR and AODV with malicious nodes.

6 CONCLUSION

We have done simulation for 50 nodes ad hoc network. As a traffic parameter we have used Constant Bit Rate. As far as mobility concern we are using Random Way Point Model. We have taken average of 10 simulations to make result more appropriate. We analyze both protocols in terms of throughput, Delay, Routing Overhead and Packet Delivery Ratio.

We have analyzed during Black Hole Attack, based on the number of attacker, the Packet Delivery Ratio is high or low. If the number of them increases, the Packet Delivery Ratio is low, because we are dropping data packets. As far as throughput concern, as number of malicious node increase our throughput decreases because nodes are not able to find path towards destination and that causes dropping. Based on our research and analysis of simulation result we draw the conclusion that AODV is more vulnerable to Black Hole attack than DSR.

REFERENCES

[1] Varsha Patidar,Rakesh Verma, "Risk Mitigation of Black Hole Attack for Aodv Routing Protocol," *IOSRJCE, Volume 3, Issue 3,July-Aug.*

[2] N. Bhalaji, A. R. Sivaramkrishnan, Sinchan Banerjee, V. Sundar, and A. Shanmugam. , "Trust Enhanced Dynamic Source Routing Protocol," *World Academy of Science, Engineering and Technology 49 2009.*

[3] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767-782, May 2001.

[4] Nor Surayati Mohamad Usop, Azizol Abdullah, Ahmad Faisal Amri Abidin, ''Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment'', *IJCSNS International Journal of Computer Science and Network Security*, VOL.9 No.7, July 2009 Q. Feng , Z. Cai, J. Yang, and X. Hu . "A Performance Comparison of the Ad Hoc Network Protocols." Second International Workshop on Computer Science and Engineering. 2009.

[5] E. Gerhards-Padilla, N. Aschenbruch, and P. Martini. "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs." 32nd IEEE Conference on Local Computer Networks. 2007.

[6] Rajiv Misra and C.R.Manda, ''Performance Comparison of AODV/DSR On-demand Routing Protocols for Ad Hoc Networks in Constrained Situation'', *Indian Institute of Technology, Kharagpur (India).*

[7] Vahid Nazari Talooki & Koorush Ziarati, ''Performance Comparison of Routing Protocols For Mobile Ad Hoc Networks'', *Dept. of Computer Science and Engineering, School of Engineering, Shiraz University*

[8] marjan kuchaki rafsanjani, ali movaghar, and faroukh koroupi, ''Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes'', World Academy of Science, Engineering and Technology 44 2008.