International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-225 PAGE NO: 1401-1406
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

A STUDY OF BLACK HOLE ATTACKS ON AODV PROTOCOL IN MANET

M.Jothilakshmi [1], S.Bharathi [2],
M.Phil Full time Research Scholar, PG and Research Department of Computer Science [1]
Asst. Professor, Department of Computer Science [2]
Vivekanandha College of Arts & Sciences for Women (Autonomous),
Tiruchengode, Namakkal-637 205,
Tamil Nadu, India
Jothividhula@gmail.com [1] , bharathischolar30@gmail.com [2]

ABSTRACT-Ad-hoc network is a collection of dynamic nodes it means any node can join the network and leave the network any time.Wireless communication is less secure than wired communication and that's why it is the vulnerability of mobile ad-hoc network and any threat can easily affect the communication. Many types of attacks are developed today which badly crash the network and make the communication performance degrade. So for avoid these vulnerabilities and make network secure we propose the technique on SECURITY of mobile ad-hoc network. To provide the security of mobile ad-hoc network we generate new techniques for detection of black hole attack. the performance impact of a black hole attack on a mobile ad hoc network and compare it with our modified AODV routing protocol. The simulation work is carried out by OPNET Modeler. To analyze performance of our proposed algorithm we use performance metrics ex. Network throughput, network load, packet send and received, packet dropped and end-to-end delay. we have surveyed and compare the existing solutions to black hole attacks on AODV protocol and their drawbacks.

Keywords : MANET, AODV, Black Hole, DPRAODV, MAODV, SAODV.

I. INTRODUCTION

In recent years mobile ad hoc network [2] (MANET) has a great impact on wireless networks. In MANET, there are no basic network devices, such as routers or access points to transfer data among nodes. Instead, each node acts as a router to establish a route and transfer data by means of multiple hops. Due to the mobility nature of nodes, the network topology changes rapidly and erratically over time. MANETs have many potential applications, like Sensor Networks, Medical Service, Personal Area Network, especially in military and rescue operations such as connecting soldiers in the battlefield or creating a temporary network in place of one, which collapsed after a disaster like tsunami. Mobile ad hoc networks are more vulnerable to security

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-225 PAGE NO: 1401-1406
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

problem than the wired networks and there are several security issues [24] such as no predefined boundary, Adversary inside the network, No centralized control facility, Limited energy resource and changing scale. The network is less centralized, where mobile the nodes are must carry out network organization and delivery of packets themselves. When a node wants to transfer data to another node, packets are transferred through the intermediate nodes, thus, searching and establishing a route from a source node to a destination node is an important task in MANETs. A number of routing protocols have been developed for execute this task. Since, wireless networks came into existence, routing in mobile ad hoc networks has been a challenging task. The major reason for this is the constant changes in network topology due to the mobility of nodes. The available routing protocols are mainly categorized into proactive routing protocols, reactive routing protocols and hybrid routing protocol. In proactive routing protocols, the routing information of nodes is exchanged, sporadically, such as DSDV. In reactive routing protocols, nodes exchange routing information when it is needed such as AODV and DSR. Some ad-hoc routing protocols are a combination of the above two categories which we called as hybrid routing protocols. The primary goal of such an ad hoc network routing protocols are correct and efficient route establishment between a pair of nodes so that messages can be delivered in a timely manner. The rest of the paper is organized as follows. Section 2 provides an overview of AODV protocol and some of the attacks performed at network layer, section 3 describes how the black hole attack is performed on AODV, Section 4 deals with several solutions to black hole attack, section 5 presents a comparison table among the solutions and finally, conclude the paper with plan for future work in Section 6.

II. OVER VIEW OF AODV ROUTING PROTOCOL:

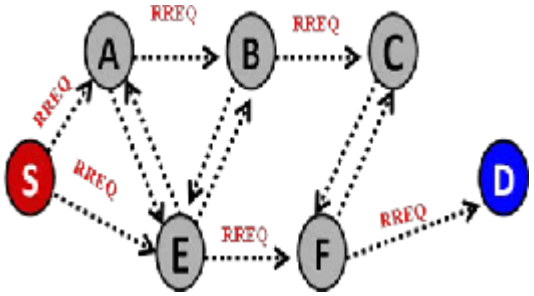

Figure 1.AODV Routing protocol overview

The Ad-hoc On-Demand Distance Vector (AODV) [1][29] is a reactive routing protocol designed to have intention for use in mobile ad hoc networks. It finds a route to a destination when a node likes to Transfer a packet to that destination. Routes are maintained by the source node as long as they needed. Route discovery process is based on the route information is stored in all intermediate nodes along the route in the form of route table entries. Every node has routing table, it has the fields like destination, next hop, number of hops, destination sequence number, active neighbors and lifetime respectively. AODV uses several control packets like route request packet (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used to find active neighbors. Sequence numbers are

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-225 PAGE NO: 1401-1406
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

used to find the freshness of routes towards the destination. When a route is not available for the destination, a route request packet (RREQ) is flooded throughout the network. The RREQ contains source address International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011 24 along with request ID is incremented each time the source node sends a new RREQ and identifies it uniquely. On receiving a RREQ packet, each node checks the source address and the request ID. If the node has already received a RREQ with the same pair of parameters the new RREQ packet will be discarded Otherwise the RREQ will be either forwarded (broadcast) or replied (unicast) with a RREP packet: once a RREP packet is received, the route is established . A source node may receive multiple RREP packets with different routes. It then updates its routing entries if and only if the RREP has a greater sequence number, i.e. fresh information. While transmitting RREQ packets through the network, each node notes the reverse path to the source. When the destination node is found, the RREP packet will travel along this path. Recently, most research on ad-hoc routing protocols, has been assumed trusted environment but, many usages of ad-hoc network run in untreated situations. Therefore, most ad hoc routing protocols are vulnerable to different types of attacks. These attacks are divided into two categories, called external attacks and internal attacks. Internal attacks are done by authorized node in the network, where as external attacks are performed by the node that they are not authorized to participate in the network. Another classification of attacks is related to protocol stacks, for instance, network layer attacks and some network layer attacks [18] are listed below in Table1.

III. Attacks at the network layer

1. Wormhole : Tunneling the packets using private high speed network.
2. Byzantine : Selectively drop packets by making routing loops, forwarding packets through non-optimal paths with compromised nodes
3. Rushing : Quickly forwards the control messages to gain access to the network.
4. Resource consumption : It injects the packets to get more network resource.
5. Location : Attacker discloses the privacy of a network by knowing the location of anode disclosure
6. Black hole : Drops the packets by sending false route reply messages to the route request.

IV.BLACK HOLE ATTACK ON AODV PROTOCOL:

To perform black hole attack, malicious node waits for RREQ messages from neighboring nodes. When the malicious node receives an RREQ message, immediately sends a false RREP message with a high sequence number and minimum hop count without checking its routing table to make an entry in the routing table of the source node, before other nodes replies to absorb transmitted data from source to that destination and drop them instead of forwarding. Black hole attack [4]

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-225 PAGE NO: 1401-1406
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

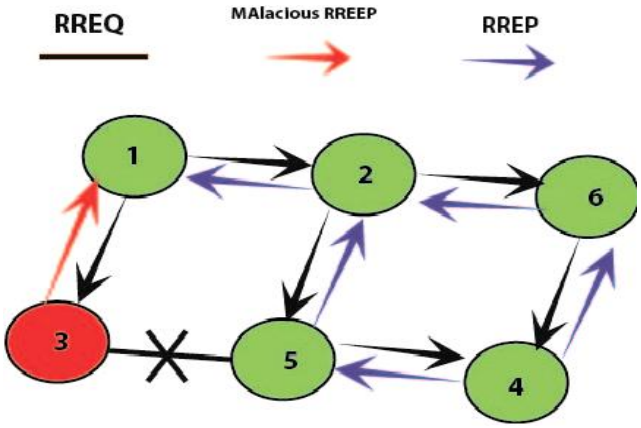

Figure 2. Black hole attack on Aodv

AODV protocol can be performed in two way: 1. black hole attack caused by RREP and 2. black hole attack caused by RREQ are described in table2 as follows:

Table1: Black hole attack

Caused by RREQ	Caused by RREP
Set the originator IP address in RREQ to the originating node's IP address.	Set the originator IP address in RREP to the originating node's IP address.
Set the destination IP address in RREQ to the destination node"s IP address	Set the destination IP address in RREP to the destination node"s IP address
Set the destination IP address of IP header to broadcast address	Set the destination IP address of IP header to the IP address of node that RREQ has been received
Set the source IP address of IP header to its own IP address	Set the source IP address of IP header to its own IP address

V.Various comparison of Black hole attack in AODV Protocol:

Table 2: comparison of Delay of normal AODV, black hole AODV and modified AODV

Nodes	Nodes Normal AODV	Black hole attack with AODV	Modified Black hole AODV
20	22.4009	10.45	28.01
30	19.7989	9.45	20.0655
40	31.6295	11.40	29.81
50	18.1787	9.16	21.45
60	30.9652	8.11	39.45

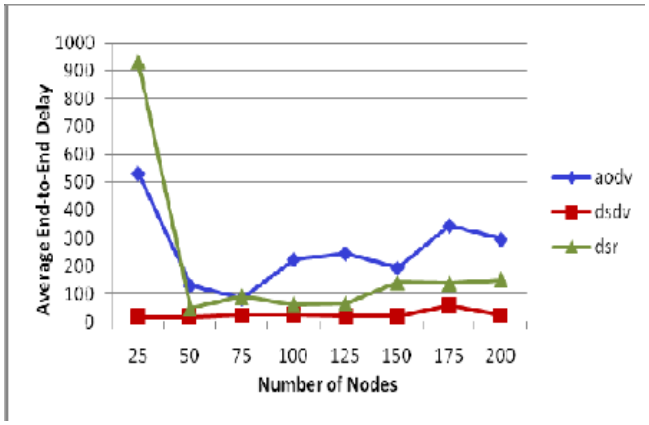

Figure 3: Black hole delay

Table 3: comparison of Throughput of normal AODV, black hole AODV and modified AODV

Nodes	Normal AODV	Black hole attack with	Modified Black hole AODV

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-225 PAGE NO: 1401-1406
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

		AODV	
20	112.86	42.16	113.72
30	111.74	38.34	113.52
40	113.62	41.09	113.55
50	113.5 1	47.49	113.52
60	112.69	58.23	113.55

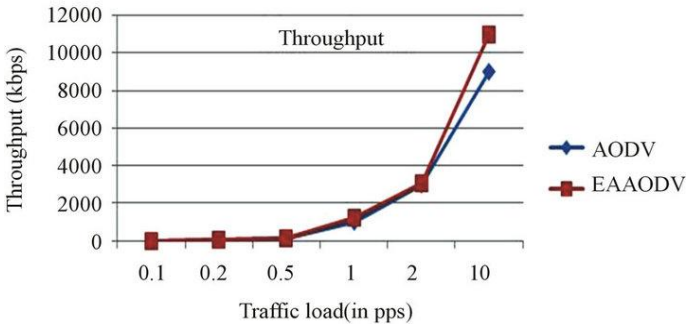

Figure 3: Black hole throughput

V.CONCLUSION:

This paper various works related to black hole attack detection mechanism in AODV-based MANETs. The various authors have given several proposals for detection and prevention of black hole attacks in MANET but every proposal has its own disadvantages in their respected solutions and we made a comparison among the existed solutions. We observe that the mechanisms detects black hole node, but no one is reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations. For future work, to find an effective solution to the black hole attack on AODV protocol.

VI. REFERENCES

[1] Raja Mahmood, R.A.; Khan, A.I.; , "A survey on detecting black hole attack in AODV-based mobile ad hoc networks," High Capacity Optical Networks and Enabling Technologies, 2007. HONET 2007. International Symposium on , vol., no., pp.1-6, 18-20 Nov. 2007

[2] Hao Yang; Haiyun Luo; Fan Ye; Songwu Lu; Lixia Zhang; , "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE , vol.11, no.1, pp. 38- 47, Feb 2004.

[3] N. Bhalaji, A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based MANET", European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011.

[4] H.A. Esmaili, M.R. Khalili Shoja, Hossein gharaee, "Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT), Vol. 1, No. 2, 49-52, 2011.

[5] Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

[6] Osathanunkul, K.; Ning Zhang; , "A countermeasure to black hole attacks in mobile ad hoc networks," Networking, Sensing and Control (ICNSC), 2011 IEEE International Conference on, vol., no., pp.508-513, 11-13 April 2011.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-225 PAGE NO: 1401-1406
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

[7] Sen, J.; Koilakonda, S.; Ukil, A.; , "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on , vol., no., pp.338-343, 25-27 Jan. 2011.

[8] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[9] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008

[10] Songbai Lu; Longxuan Li; Kwok-Yan Lam; Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," Computational Intelligence and Security, 2009. CIS '09. International Conference on, vol.2, no., pp.421-425, 11-14 Dec. 2009

[11] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[12] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010