A Literature Review on Black Hole Attacks on AODV Protocol in MANET

[1]Rahul singh, Anurag Uphdaya[2]
[1, 2]*M.tech Scholar, CSE Dept, IFTM University*

ABSTRACT
A Mobile ad-hoc network (MANET) is research area with practical applications. The reason behind the fame of MANET is flexibility and independence of network infrastructure. MANET have some inimitable characteristic like dynamic network topology, limited power and limited bandwidth for communication. MANET has more challenge compare to any other conservative network. Routing plays an important role in the security of the whole network. The most common routing protocols used in ad-hoc network are AODV (ad-hoc on demand distance vector) protocol. AODV protocol is susceptible by "Black Hole" attack. In black hole attack a malicious node advertise itself as have the shortest path to the destination node. In this paper we study the routing security issue of MANET and analyze in detail one type of attack the "Black hole" attack. We also present a detailed list of solutions which protect the black hole in MANET's.

Keywords
MANET, Security, Black hole attack, AODV and Packet dropping.

INTRODUCTION

A "mobile ad-hoc network" (MANET) is an independent system of mobile routers (& associated hosts) connected by wireless links--the amalgamation of which form an arbitrary graph. The mobiles devices are free to move aimlessly and systematize themselves illogically thus network's wireless topology may change quickly and suddenly. Such a network may operate in a separate fashion, or may be connected to the larger Internet [1][2]. The people's future existing environments are rising based upon information resource provided by the connections of a variety of communication networks for users. New small devices like Personal Digital Assistants (PDAs), mobile phones, handhelds, and wearable computers enhance information processing and accessing capabilities with mobility Mobile ad-hoc networks (MANETs) are collections of mobile nodes, animatedly forming a temporary network without pre-existing network infrastructure or centralized administration. These nodes can be illogically located and are free to move randomly at any given time, thus allowing network topology and interconnections between nodes to change quickly and impulsively. Node mobility can vary from almost stationary to constantly moving nodes, depending on the particular network's structure and purpose. As a general rule, high mobility usually results in low link ability, whereas low mobility leads to high capacity links. The very dynamic nature of mobile ad-hoc networks creates huge challenges for routing protocols. As MANET networks are infrastructure less there subsist no enthusiastic routers. Instead, every mobile node acts itself as a router and is responsible for discovering and maintaining routes. Furthermore, without federal administration, MANETs can be called independent. To support this kind of autonomy, the routing protocol is required to automatically adjust to frequent environment changes.

In addition to freedom of mobility, a MANET can be constructed rapidly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is striking for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, and so on, unlike the conventional network. A MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes . This feature makes it difficult to perform routing in a MANET compared with a conservative wired network. Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging job.

Therefore, early work in MANET research focused on given that routing service with minimum cost in terms of bandwidth and battery power. There are a wide variety of attacks that object the weakness of MANET. For example, routing messages are an important component of mobile network communications, as each packet needs to be passed rapidly through intermediate nodes, which the packet must navigate from a source to the destination. Malicious routing attacks can object the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that object some particular routing protocols, such as DSR, or AODV [3] [4]. More complicated and subtle

routing attacks have been identified in recent published papers, such as the black hole (or sinkhole) [5], Byzantine [6], and wormhole [7] [8] attacks. Currently routing security is one of the hottest research areas in MANET.

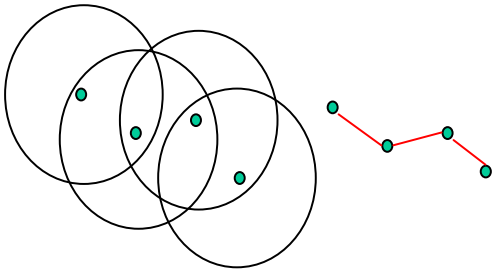

Figure 1 Example Application of MANETs

2. OVER VIEW OF AODV ROUTING PROTOCOL

AODV [9] is a reactive routing protocol intended for a mobile ad hoc network. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it start route discovery by broadcasting a route request (RREQ) to its neighbors. The instant neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives anon will be ignored by the destination node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.

3. BLACK HOLE ATTACK ON AODV PROTOCOL

In a blackhole attack, a malicious node sends bogus routing information, claiming that it has an best route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a bogus Route Reply (including a fake destination sequence number that is made-up to be equal or higher than the one contained in the Route Request) to the source node, claiming that it has a good fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can break/abandon the traffic.

Figure 2 shows an example of a black hole attack, where attacker A sends a fake Route Reply to the source node S, claiming that it has a best fresher route than other nodes. Since the attacker's broadcast sequence number is higher than other nodes' sequence numbers, the source node S will prefer the route that passes through node A.

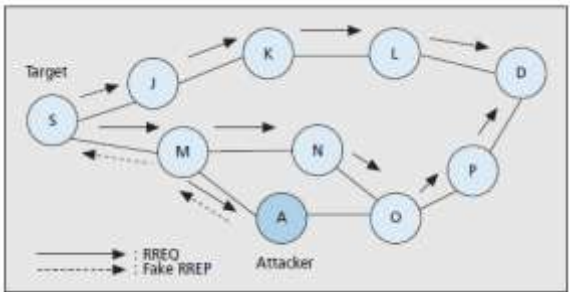

Figure 2 Example of black hole attack on AODV

4. SOLUTIONS TO BLACK HOLE ATTACK IN MANET

In this section, we will review the several solutions to black hole attacks**.**

Hongmie Deng et.al.[10] proposed One possible solution to the black hole attack problem is to reject the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. Using this method the intermediate node do not reply, so in some sense they keep away from the black hole problem and put into operation a tenable AODV protocol. But there are two associated disadvantages. First, the routing wait is really increased, especially for a large network. Second, a malicious node can take further action such as make a reply message on behalf of the destination node. The source node cannot classify if the reply message is really from the destination node or made-up by the malicious node. In this case, the method may not be ample.

To avoid the state of the intermediate node attractive further action such as make the reply message on behalf of the next hop node. When the source node receives the Further Reply from the next hop, it extracts the check result from the reply packets. If the result is yes, they set up a route to the destination and start to send out data packets. If the next hop has no route to the ask intermediate node, but has a route to the object node, they throw away the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. At the same time, send out the alarm message to the whole network to separate the malicious node. If the next hop has no route to the requested intermediate node, and it also has no route to the destination node, the source node start another routing discovery process, and also propel out an alarm message to separate the malicious node. Using this method, they evade the black hole problem, and also avoid the network from further malicious behavior. They don't disable the ability of a replying message from

intermediate nodes, but the routing overhead is vastly increased if they do the check process to every intermediate node that sends a reply message. Moreover, they do not need this mechanism in a normal network environment. They propose to use this method whenever they discover any suspected node in the network. To get the suspected node, any intrusion detection methods can be used. They use the IADM for the prior work to find the suspected node. Whenever they are doubtful, they trigger they method to identify if the suspected node is actually malicious or not.

Al-Shurman et.al. [11] planned a solution that requires a source node to wait until a RREP packet appear from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node adjudicators that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs turn up.

Satoshi Kurosawa et. al. [12] uses an anomaly detection scheme. It uses dynamic training method in which the training data is revised at regular time intervals. Multidimensional feature vector is defined to express state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one detained in the list. They calculate mean vector by calculating some mathematical calculation. They evaluate distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. The updated data set to be used for next detection. Repeating this for time interval T anomaly detection is complete.

Latha Tamilselvan et. al. [13] proposed a improved solution with the modification of the AODV protocol, which circumvent multiple black holes in the group. It uses loyalty table where every node that is participating is given a loyalty level that will offer reliability to that node. Any node having 0 values is considered as malicious node and is removed from the network. The loyalty levels of nodes are updated based on their trusted participation in the network. Upon receiving the data packets, the destination node will send an acknowledgement to the source; thereby the intermediate node's level will be increased. If no acknowledgement is received, the intermediate node's level will be decreased. The main drawback of this solution is processing delay in the network.

Zhao Min et.al [14] discussed an authentication mechanism for recognize black hole nodes in MANETs. An authentication mechanism is build based on the concept of the hash function, MAC, and PRF, which is used for checking the RREPs at source node to send the data packets. The projected mechanism removes the need for a PKI or other forms of authentication infrastructure, however it needs to be discuses, how to handle unlimited message authentication by switching one-way-hash chains and how to prevent a malicious node cannot fake a reply if the hash key of any node is to be released to all nodes.

XiaoYang Zhang et.al. [15] discussed a new detection method based on checking the sequence number in the Route Reply packets by making use of a new message created by the destination. In this method, when an .intermediate node unicasts a RREP packet, the node also unicasts a newly defined control message to the destination node to request for the up-to-date SN. Upon receiving, the destination node unicasts a reply message to inform the source node of the up-to-date SN. This reply from the destination node permits the source node to verify if the intermediate node has sent a faked RREP message by checking if the SN in the RREP message is larger than the up-to-date SN. This method has more network overhead and time delay since node in the network produces new packets.

Payal N. Raj et. al. [16] modify the behavior of AODV to include a mechanism for checking the sequence number of the received RREP. As the source node receives the RREP it evaluate the sequence number of the received RREP to a threshold value. The replying node is alleged to be a black hole if its sequence number is greater than the threshold value. The source node adds the alleged node to its black list, and proliferates a control message called an alarm to publicize the black list for its neighbors. The threshold is the calculated average of the difference between the destination sequence number in the routing table and the destination sequence number in the RREP within certain periods of time. The main advantage of this protocol is that the source node publicizes the black hole to its neighbors in order to be ignored and eliminated.

Alem, Y.F et.al. [17] Proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent attacks by the both single and multiple black hole nodes. IDAD assumes every action of a user can be examined and irregularity activities of an intruder can be identified from normal activities. To find a black hole node IDAD needs to be provided with a pre-collected set of irregularity activities, called review data. Once audit data collected and it is given to the IDAD

system, which is able to compare every activity with audit data. If any activity of a node is out of the activity listed in the audit data, the IDAD system separates the particular node from the network. The decrease of the number of routing packets in turn minimizes network overhead and assist a faster communication.

Ming-Yang et. al [18] proposed an intrusion detection system called Anti-Blackhole Mechanism (ABM) in which the doubtful value of a node is estimated according to the amount of irregular difference between RREQs and RREPs spreaded from the node; all nodes perform ABM. With the requirement that intermediate nodes are forbidden to reply to RREQs, if an intermediate node is not the destination and never transmits RREQ for a specific route, but forward a RREP for the route, then its doubtful value will be raised in the nearby node's suspicious node table. When the doubtful value of a node goes ahead of threshold, a Block message is broadcasted by the node to all other nodes in the network to separate the doubtful node cooperatively. Though, the solution assumes that an authentication mechanism already exists in MANET.

Lalit Himral et.al [19] have proposed method to find the secured routes and avert the black hole nodes (malicious node) in the MANET by checking whether there is huge difference between the sequence number of source node or intermediate node who has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is accumulate as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, definitely it is from the malicious node, immediately confiscate that entry from the RR-Table. The planned method cannot find multiple black hole nodes.

Kamarulari fin Abd et.al.[20] have planned an ERDA solution to progress AODV protocol with minimum modification to the existing route discovery method recvReply() function. There are three new elements introduced in modified recvReply() function namely: table rrep_table to store incoming RREP packet parameter mali_list to keep the detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table. When RREQ packet is sent out by the source node S to find a fresh route to the destination node D. RREP packet established by node S will be captured into rrep_tab table. Since the malicious node M is the first node to response, the routing table of node S is updated with RREP information from node M Since the value of parameter rt_upd is „true, node S accepts the next RREP packet from other node to update the routing table although it arrives later and with a lower destination sequence number than the one in the routing table. The current route entry in routing table will be overwritten by the later RREP coming from other node. ERDA method offers a simple solution by eliminating the false route entry and replaced the entry with later RREP. However, it cannot notice obliging black hole attack.

Kitisak Osathanunkul et. al.[21] the plan of SETX protocol is to give a method to stop black hole nodes from promotion a made-up forwarding delivery ratio (df) of a wireless link between itself and one of its neighbors'. Non-supportive black hole attacks mean that malicious nodes perform the attacks separately. They do not work together in launch an attack. There is another type of black hole attacks, by which malicious nodes share out routing information with each other and initiate black hole attacks in association. This latter attack type is called cooperative black hole attacks . Our SETX protocol cannot frustrate cooperative black hole attacks, as it is possible for several cooperative black hole nodes to help each others to achieve the necessary probes. For example, if a black hole node, A, has missed out some probes, but if black hole node B or C are able to receive the probes that A badly needs. Then B or C can tunnel these probes to A. So A can use these probes to encourage the designer that he has a better df value, thus a better route to the intended destination.
A trust management scheme can be worn to deal with cooperative black hole attacks. Trust management schemes are a method that allows nodes to observe the behavior of their neighbors'. If their neighbors' intentionally drop a packet, the trust level will be precious. If the trust level of a neighboring node drops below a given threshold level, this neighboring node will be measured as a malicious node. This trust based approach to countering cooperative black hole attacks means that black hole nodes may be able to attack the network (i.e. drop the packets) for a while before they are detected. Once they have been detected, an alarm can be sent out to other nodes. In addition, adopting a trust based scheme can be more complicated. This often means that the nodes in the network would have to passively listen to the neighbors' packet transmissions and exchange trust related values among them. This will consume network bandwidth and impose additional overheads to the network, but it can be a solution against cooperative black hole attacks.

Seryvuth Tan et. Al.[22] Security issues have generally been ignored while designing routing protocols for ad-hoc networks. Because of the properties of the normal AODV protocol, it is easy

to infringe the security of a MANET. AODV is vulnerable to many types of malicious attacks including black hole attacks. In this paper investigate some of the existing solutions for these attacks. In this paper projected a novel approach for detecting and preventing these attacks and securing a route to the destination in an resourceful manner. The simulation results show in this paper SRD-AODV mechanism greatly increases the packet delivery ratio for three types of environments with node mobility when black hole attacks are going on on the network. in this paper will improve the security mechanism for data transmissions tin this paper the origination nodes or source node and destination node after a route has been reputable.

Gayatri Wahane et. Al.[23]cooperative black hole attack and its entail on the AODV-based routing protocol has been discussed. The route discovery process in the AODV is helpless to Cooperative black hole attack and therefore, it is very vital to have an efficient security method built into the AODV protocol in order to mitigate the effect of such attacks. True-Link-crosschecking method is designed to separate and mitigate the consequence of black hole attacks in MANET. True-Link-crosschecking enhances AODV protocol to get better the network performance by civilizing routing update condition. The improvement only involves a minimum modification in DRI based cross checking with True-link rendezvous phase by changing the existing AODV protocol scheme. This solution reduces routing overhead and delay. It achieves maximum throughput when number of nodes and pause time more. In proposed work in this paper have reduced end to end delay as well as routing overhead. In future work, in this paper are planning to reduce routing overhead by making nonce more secure and timestamp in link verification.

Apurva Jain et al.[24] In this paper, customized AODV, which is TAODV (Trust based AODV), is a network. TAODV has several significant features as Nodes perform trusted routing behavior mainly according to the trust relationship s among them. A node that performs black hole behavior will be detected and challenge by the whole network TAODV mollify the effect of Black Hole attack but average end-to-end delay increases in TAODV. In Indoor environment Pareto traffic condition, gives the best result as far as average throughput is consider. However, Exponential traffic condition gives the best result for average end-to-end delay and CBR traffic condition traffic condition the best result for packet delivery ratio. In Outdoor environment, Pareto traffic condition gives the best result for average throughput and packet delivery ratio and Exponential traffic condition gives the best result for average end-to-end delay.

5. CONCLUSION:-

As we already know why MANET is so popular in present scenario? It has some extra usual features due to which it is acceptable globally. MANET have so many features and as well as it have some security issues. In this paper we have just provide a list of solutions in MANET on a explicit attack that is black hole attack. There are so many solutions which provide better security in case of single malicious node but these solutions are not effective in case of multiple malicious node. Some solutions may require some special hardware like GPS. In this paper a brief introduction is provide for each solution with their upgrading and drawbacks. Fir future research work researchers have to focus on improving the effectiveness of the security scheme as well as minimize the cost to make them appropriate for a MANET environment.

6. Reference:-

[1] C. Perkins, Ad Hoc Networks, Addison-In this papersley, 2001.

[2] S. Ci et al., "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks,"IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006, pp. 1302–10.

[3] M. Zapata, Secure Ad Hoc On-Demand Distance Vector (SAODV). Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.

[4] Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. Proc. of MobiCom 2002, Atlanta, 2002.

[5] Y. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing. IEE Security & Privacy, pp. 28-39, 2004.

[6] B. Ain this paperrbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

[7] Y. Hu, A Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks. Proc. of IEEE INFORCOM, 2002.

[8] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002

[9] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc Ondemand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

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

[11] Mohammad Al-Shurman et. Al" Black Hole Attack in Mobile Ad-Hoc Network" ACMSE'04, Apri l 2-3, 2004, Huntsville, AL, USA .

[12] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipthey, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic

Learning Method", International Jtheynal of Network Securi ty, Vol.5, Issue 3, pp: 338–346, 2007

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

[14] Zhao Min; Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", Information Engineeri ng and Electronic Commerce, 2009. IEEC '09.International Symposium on, vol., no., pp.26-30, 16-17 May 2009.

[15] XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET," Autonomous Decentralized Systems, 2009. ISADS '09. International Symposium on, vol., no., pp.1-6, 23-25 March 2009.

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

[17] Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd

[18] Ming-Yang Su, "Prevention of Selective Black hole Attacks on Mobile Ad hoc Network through Intrusion Detection Systems", Computer Communications, 2010. Communications, 2007, pp. 21-26.

[19] Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack" International Jtheynal of Engineeri ng Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[20] Kamarulari fin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, "Mitigation of Black Hole Attacks for AODV Routing Protocol", Society of Digital Information and Wireless Communications (SDIWC) Vol01_No02_30, 2011.

[21] Kitisak Osathanunkul and Ning Zhang" A Countermeasure to Black Hole Attacks in Mobile Ad hoc Networks" 978-1-4244-9573-3/11/$26.00 ©2011 IEEE.

[22] Seryvuth Tan and Keecheon Kim "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs"978-0-7695-5088-6/13 © 2013 IEEE.

[23] Gayatri Wahane, Ashok M. Kanthe and Dina Simunic "Detection of Cooperative Black Hole Attack using Crosschecking with TrueLink in MANET" 978-1-4799-3975-6/14/$31.00 ©2014 IEEE.

[24] Apurva Jain and Anshul Shrotriya "Investigating the Effects of Black Hole Attack in MANET under Shadowing Model with Different Traffic conditions" IEEE International Conference on Computer, Communication and Control (IC4-2015).