A Review on Black Hole Attack in Mobile Adhoc Network

Anand Motwani
Asst. Prof. & Head
Department of CSE
NIRT, Bhopal

Jyoti Sondhi
Asst. Prof.
Department of CSE
NIRT, Bhopal

Vimal Dhote
M. Tech. Scholar
Department of CSE
NIRT, Bhopal

ABSTRACT
Mobile ad hoc network is self- configuring and infrastructure less network. Due to its dynamic nature, it is more susceptible to severe type of attacks. An assortment of attacks is there to mischief the dexterous working of MANET. One of these attacks is the Black Hole attack which leads to dropping of messages. Attacking node leading agrees to forward packets and then not succeeded to do so. Black Hole attack may take place due to a malicious node which is consciously misbehaving as well as a smashed node interface. In any case, nodes in the network will continuously trying to find a route for the destination, which makes the node consume its battery in addition to losing packets. In this paper we present the literature study of various approaches of Black hole attack propose by researchers in their research. The merits and demerits of the different approaches are also presented.

Keywords
MANET, Black hole attack, Security threats, dynamic

1. INTRODUCTION
Wireless networks use some kind of radio frequencies in air to transmit and receive data instead of using some physical cables. Wireless networks are formed by routers and hosts. Ad-hoc networks are wireless networks, in which nodes communicate with each other using multi-hop links. Network which support wireless architecture are known as mobile Adhoc Network [1]. Such networks can be used to enable next generation battlefield applications, including situation awareness systems for maneuvering war fighters, and remotely deployed unmanned micro-sensor networks. MANETs have some exceptional characteristic features such as undependable wireless media (links) used for communication flanked by hosts, determinedly changing network topologies and memberships, inadequate bandwidth, battery, existence, and working out power of nodes etc. Ad hoc networks make available a prospect of creating a network in situations where creating the infrastructure would be impossible or prohibitively expensive. Unlike a network with predetermined infrastructure, mobile nodes in ad hoc networks do not communicate by means of access points. Every mobile node operates as a host when requesting/providing information from/to other nodes in the network, and acts as router when ascertaining and maintaining routes for other nodes in the network [2].

The dynamic nature of ad hoc networks requires that prevention techniques should be complemented by detection techniques, which scrutinize security condition of the network and identify malicious behavior. One of the most decisive predicaments in MANETs is the sanctuary vulnerabilities of the routing protocols. A set of nodes in a MANET may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non- existent links, provide incorrect link state information, and flood other nodes with routing traffic. An OADV is a source initiated on-demand routing protocol. On the other hand, AODV [3] is susceptible to the well recognized black hole attack. In black hole attack an attacker node transmits infected packet to an unknown receiver. When a node receives it gets infected and behaves like malicious node and transmitted multiple of reflected packets to others and same procedure used to infect the whole network. The Black Hole attack [4, 5] is a class of denial of service where a malevolent node can magnetize all packets by untrustworthily claiming a fresh route to the target and then saturate up them devoid of forwarding them to the target. Cooperative Black hole means the malicious nodes operate in a group [6].

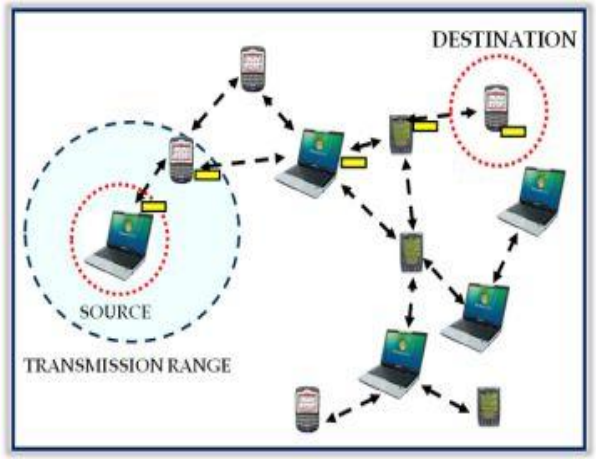

Fig. 1: Mobile ad hoc Network

The remaining part of the paper is prearranged as follows: In section II discusses black hole in AODV routing overview. The Section III presents the literature of previous work done and last section presents conclusion of the paper.

2. AODV ROUTING PROTOCOL
AODV is distance vector routing protocol that establishes route to the destination when it is desired by the source node. It sustains these routes as and when desirable by the source node. It offers quick adaptation to self-motivated link conditions, low processing, memory overhead, low network deployment, and establishes unicast routes to destinations within the ad hoc network [3]. One of the distinctive features of AODV protocol is its use of destination sequence number associated with all route. Destination sequence number is created by the destination to include route information about it send to the requesting node. In order to correspond amongst the mobile nodes, [3] Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. When a source node desires to attach to a destination node, primary it checks in the presented route table, as to whether a fresh route to that target is existing or not. New adequate route means a valid route entry whose

sequence number is larger than it in the RREQ. Larger the sequence number, fresher is the route. If a new adequate route is presented, it uses the same. If not, the node initiates a Route innovation by broadcasting a RREQ control message to all of its neighbors. This RREQ message will additionally forwarded by the intermediate nodes to their neighbors having a new route to the target. The RREQ message will ultimately reach the target node, which will respond with a route reply message (RREP). The RREP is sent as a unicast to the source node beside the overturn route established during the RREQ broadcast. Likewise, the RREP message allows intermediary nodes to learn a forward route to the target node. Therefore, at the end of the route discovery process, packets can be delivered from the source node to the target node and vice versa. A route error message (RERR) allows nodes to notify errors due to link breakage, such as when a preceding neighbor moves to a novel position and is no longer accessible. Each mobile node would periodically send Hello messages (HELLO), Consequently, every one node knows which nodes are its neighboring nodes. AODV as a reactive routing protocol does not provide nodes an absolute view of network topology. That is, every node only knows its neighbors, and for the non neighbors, it simply knows the next hop to reach them and the distance in hops. However, the security of AODV is conciliated by the Black Hole nodes, as it acknowledges the received RREP having fresher route. The standard AODV routing protocol can not fight the threat of Black Hole attacks, because during the phase of route detection, malicious nodes may forged a sequence number and hop count in the routing message; In this manner, obtaining the route [15] , eavesdropping and plummeting all the data packets as they pass or forward some discriminating packets to the destination.

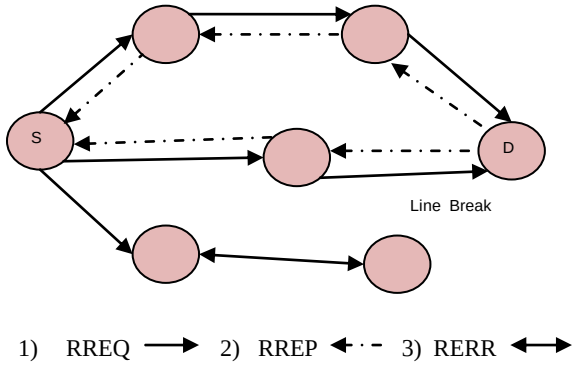

Fig. 2: Working of AODV Protocol

3. BLACK HOLE ATTACK IN AODV

The attacks in mobile ad hoc network are classified into two categories: one is active attack and another is passive attack. The black hole attack is an example of active attack; it can be a single black hole or cooperative black hole. In Mobile Ad hoc Network a packet plummet attack or black hole attack is a diversity of denial-of-service attack in which a router that is thought to impart packets instead discards them [4]. This typically takes places from a router becoming compromised from a number of dissimilar causes. One cause declared in investigation is during a denial-of service attack on the router using a known DoS tool. For the reason that packets are routinely plummeted from a lossy network, the packet drop attack is dreadfully hard to identify and thwart. Node 4 shows the malicious node in the figure 3 operate with each other.

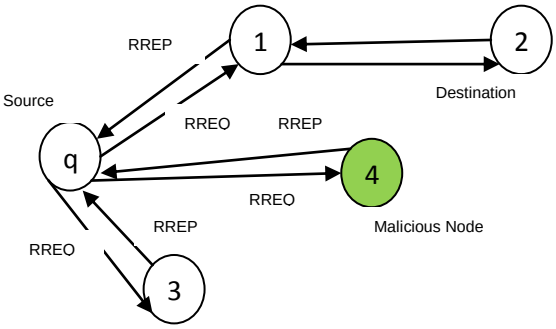

Fig. 3: Single black hole node in AODV protocol

The cooperative black hole is a type of attack in which black hole nodes act in a group together [7]. For example when multiple black hole nodes are acting in coordination with each other, the first black hole node refers to the one of its teammate in the next hop .This type of attack harms the system very much and affect the throughput of the system. The nodes 1, 4 and 6 in the following figure are malicious nodes that act in coordination with each other.

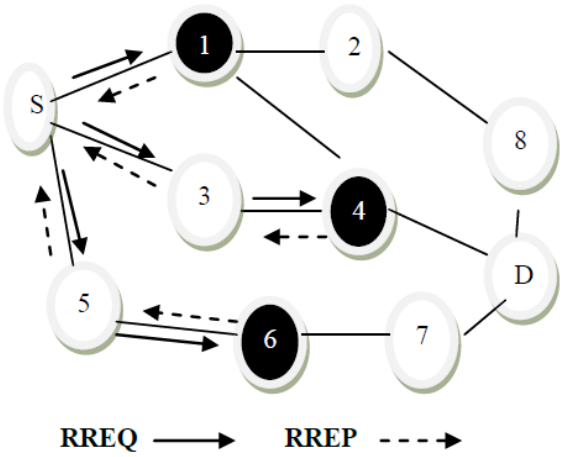

Fig. 4: Cooperative black hole node in AODV protocol [7]

4. RELATED WORK

To combat the black hole attack from the wireless ad hoc network, a lot of work has been done in this field. Various researchers implemented or suggested different techniques to combat it. In this paper a literature study of the previous work is described below:

Nishu kalia, Kundan Munjal [8], present a technique which uses the uzzy based control, to detect and mitigate type of attack, namely malicious packet dropping, in wireless ad-hoc network. A malicious node in a network promises to forward packets but drop or delay them. In this technique, every node in the mobile ad-hoc network sends the route request and waits for the acknowledgment. The requesting node analyzes the behavior of unknown node using fuzzy technique and on the basis of result the node takes this node in the route of the packet. Subsequently, states of the nodes can also be utilized by the routing protocol to bypass those malicious nodes. Their method shows that in a dynamically changing network, the technique can detect most of the malicious nodes with a relatively high positive rate. The packet delivery rate in the MANET can also be increased accordingly.

The authors [9] designed a novel method to detect the black hole attack: DPRAODV, which segregates that malicious node from the network. The agent supplies the Destination

sequence number of arriving route reply packets (RREPs) in the routing table and determines the threshold value to estimates the dynamic training data in every time interval as in [10]. The explanation makes the participating nodes appreciates that, one of their neighbors is malevolent; the node thereafter is not allowed to contribute in packet forwarding operation. In typical AODV, the node that receives the RREP packet first checks the value of the sequence number in its routing table. The RREP packet is accepted if it has RREP_seq_no higher than the one in the routing table. DPRAODV does an addition check to find whether the RREP_seq_no is privileged than the threshold value. The threshold value is vigorously updated as in every time interval. As the value of RREP_seq_no is found to be privileged than the threshold value, the node is suspected to be malevolent and it adds the node to the black list. As the node detected an anomaly, it sends a fresh control packet, ALARM to its neighbors. The ALARM packet has the black list node as a constraint so that, the neighboring nodes know that RREP packet from the node is to be superfluous. In additional, if any node receives the RREP packet, it looks over the list, if the answer is from the blacklisted node; no processing is done for the matching. It merely ignores the node and does not accept a reply from that node again. So, in this way, the malevolent node is isolated from the network by the ALARM packet.

The work in [11], proposed a method based on PL2 whose modification has been done in AODV protocol for ensuring the security against the Black hole attack using NS2 Simulation. This method is based on time and neighborhood parameters. This method first check for malicious activity exists, and then starts detect and remove the Black hole nodes.

In [12], analyzed the effect of black hole attack which is one of the feasible attacks in ad hoc networks. In the first phase they simulate the effect of black hole nodes in the network for AODV routing protocol. In the second phase they have modified AODV routing protocol by tuning the parameters in the RREP packet for detection of the Black hole nodes. They have done simulations by changing the various parameters like number of nodes, mobility, black hole nodes using NS2. They have compared the results with traditional AODV for simulation matrix like PDR and End-to-End delay.

In Ref. [3], recommend a method of defense against black hole attack in ad hoc networks. In their proposed method, as soon as the Route Reply packet is received from one of the intermediary nodes, another Route request is launched from the source node to a neighbor node of the intermediary node in the pathway. This is to make certain that such a path exists from the intermediary node to the destination node. Let the source node S launch Route request packets and receive Route Reply through the intermediate malicious node M. The Route Reply packet of M surrounds information concerning its next hop neighbor node. Let it enclose information about the neighbor E. Then, the source node S sends an additional Route request packets to this neighbor node E. Node E counters by sending an additional Route Reply packet to source node S. While node M is a malevolent node, and thus not accessible in the routing record of node E, the more Route Reply packet launch by node E will not enclose a route to the malevolent node M. Other than if it surrounds a route to the target node D, subsequently the new route to the target through node E is preferred, and the formerly chosen route through node M is superfluous. While this method utterly abolishes the black hole attack by a single attacker, it not succeeded completely in identifying a cooperative black hole attack regarding multiple malicious nodes.

The proposed system [13] starts route detection process of default AODV in the occurrence of an attacker. Source node S Wishes to send data to target D broadcast RREQ; A malicious node MN replies back with RREP enclosing abnormally high destination sequence number misleading S as if it has a fresher route to D; another normal intermediate node IN sends RREP having acceptably higher sequence number. As RREP of the attacker holds higher destination sequence number of all received RREPs, source node unknowingly chooses path through MN to transfer data packets and therefore, (malicious node)MN intercepts and drops some or all of the received packets that causes denial-of-service in the network. This concern states the necessity of a variation of AODV protocol that proficiently discovers a secure route to the destination.

Simulation of Black hole Attackin wireless ad-hoc Networks [14], the paper proposed an IDS system to resolve the discriminatory black hole attacks in MANET, and plants an anti-blackhole mechanism (ABM) in all IDS nodes. The ABM utilizes two supplementary tables called RQ table and SN table. The RQ table stores the RREQ message within IDS node's transmission range. The contents enclosing the source and target ID, source sequence number, maximum hop count value, broadcasting node ID and termination time. The IDS nodes use SN table to approximate the doubtful values nodes within its transmission range. The components of SN table comprising the node ID, doubtful values and status. If an intermediate node never broadcasts a RREQ for a route but sends a RREP packet, the doubtful value will be added one in the neighbor IDS node's SN table. Besides this, another new Block table is added into the main routing table in order to record the catalog of black holes. The basic skeleton of proposed IDS is introduced as follow. In the beginning, the ABM function in a sniff mode is executed by the IDS nodes. According to the asymmetrical dissimilarity between the routing information transmitted from a uncertain node, ABM can estimate a value of the suspicious node. If the value surpasses the predefined threshold value, it can be regarded as a black hole. When a ordinary node receives a Block message broadcasted by the IDS node, this node adds the malicious node which is stored in the Block message into the Block table. After that, the ordinary node forwards RREP packet to ascertain the routing. If the RREP packet is obtained from its neighbor node which noted in the Block table, the ordinary node drops this RREP packet to thwart the malicious attack.

In Ref. [15] proposed a neighborhood-based and routing recuperation method. This recognition method based on a neighborhood-based method to distinguish the black hole attack, and a routing recovery protocol to put together the correct path [15][16]. This method is employed to recognize the nodes which are unconfirmed .In this method, source node sends a alter Route Entry control packet to target node to refurbish routing path in the recovery protocol. In this system, not only an inferior discovery time and privileged throughput are attained, but the precise detection possibility is also achieved. The foremost restriction of this method is that it becomes useless when the attacker agrees to counterfeit the fake reply packets.

A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol [17], Harsh Pratap Singh, Rashmi Singh describe clock synchronization technique, in this paper, they proposed a technique in which broadcast synchronization (BS) and relative distance (RD) technique of clock synchronization is

used to thwart the black hole nodes. In this internal and external clock node evaluate with the threshold clock if both the clock time is greater than the threshold then it is found that the node is malicious. This method can easily identify and avoid the block-hole node.

5. CONCLUSION AND FUTURE WORK

Mobile Adhoc network may operate in an individual manner. Multi hop, mobility, large network size pooled with device heterogeneity, bandwidth and battery power restrain make the design of acceptable routing protocols a major challenge. In this paper, we are presenting a survey of black hole attack in MANET. After studying all the approaches examines that the most of the approaches has low packet delivery ratio and also high overhead. In future work, develop such approach which can efficiently minimize all these constraints.

6. REFERENCES

[1] Anu Bala, Rajkumari and Jagpreet Singh ”Investigation of Blackhole Attack on AODV in MANET” In Journal of Emerging Technologies in WEB Intelligence, Vol. 2, No. 2, May 2010

[2] Dixon, and Kendall E. Nygard. "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks." In International Conference on Wireless Networks, pp. 570–575, 2003.

[3] C. Perkins, E. Belding-Royer, and S. Das, “Ad-hocon-demand distance vector (AODV) routing”, InternetDraft, RFC 3561, July 2003.

[4] Hongmei Deng, Wei Li, and Dharma P. Agarwal, “Routing Security in Wireless Ad Hoc Networks”, University of Cincinnati, IEEE Communication magazine,Vol.40, no.10, October 2002.

[5] Chen Hongsong, Ji Zhenzhou and Hu Mingzeng, “A Novel Security Agent Scheme for Aodv Routing ProtocolBased on Thread State Transition”. Asian Journal of Information Technology, 5 (1):54-60, 2006.

[6] Bracha Hod, “Cooperative and Reliable Packet-Forwarding on top of AODV”,www.cs.huji.ac.il/dolev/pubs/reliable-aodv.pdf, 2005.

[7] Mamta Sengar, Pawan Prakash Singh, Savita Shiwani3, “Detection of Black Hole Attack In MANET Using FBC Technique”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March – April 2013 ISSN 2278-6856.

[8] Nishu kalia, Kundan Munjal “Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.

[9] Payal N. Raj, Prashant B. Swadas “DPRAODV: A Dyanamic Learning System AgainstBlack Hole Attack In Aodv Based Manet” IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009.

[10] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, Abbas Jamalipour, and Yoshiaki Nemoto, “Detecting Black Hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Vol.5, No.3, P.P 338-346, Nov. 2007.

[11] Vasanthavalli.S, R.Bhargava Rama Gowd,S.Thenappan “Peruse Of Black Hole Attack and Prevention Using AODV on MANET”, International Journal of Innovative Research in Science Engineering and Technology,Vol. 3, Issue 5, May 2014, ISSN: 2319-8753.

[12] Dhaval Thakar, Nainesh Prajapati “A Modified AODV – Algorithm for prevention of Black hole attack in Mobile Adhoc Networks” International Journal of Conceptions on Electrical and Electronics Engineering Vol. 1, Issue 1, Oct 2013; ISSN: 2345 – 9603.

[13] Rutvij H. Jhaveri,Sankita J. Patel,Devesh C. Jinwala "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP 2013.

[14] Dokurer,Seimih “Simulation of Black hole Attackin wireless ad-hoc Networks” Master’s Thesis Atihm University,Septeber 2006

[15] Fan-Hsun Tseng, Li-der chou and Han-chieh chao, “A survey of black hole attack in wireless mobile adhoc networks”, springer journal 2011.

[16] Sun B,Guan Y and Pooch UW, “Detecting Black hole Attack in Mobile Adhoc Networks” ,Paper presented T 5th European Personal Mobile Communication Conference, April 2003.

[17] Harsh Pratap Singh, Rashmi Singh, “A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol”, International Conference on Electronics and Communication Systems (ICECS) 2014 , Page(s):1 - 8 Print ISBN:978-1-4799-2321-2

Table 1: Advantages and disadvantages of the approaches

Author/ Researchers	Techniques/ Approaches	Years	Advantages	Disadvantages
Sengar et al.	fuzzy based control	2013	Speed, Ease and has more efficiency	Each node should monitor to its neighbor node
Swadas et al.	DPRAODV	2009	It achieve higher packet delivery rate	It enhance overhead
Bhargava et al.	PL2	2014	It provide fast focusing on neighbor	It has limited coverage for detection and grid size
Su et al.	IDS for ABM	2006	Low- false positive rate for the detection	Limited bandwidth, memory and processing capability
Tseng et al.	neighborhood-based	2011	Low false alarm rate and it is more efficient for the detection	Limited bandwidth consumption is more