A SURVEY – DETECTION AND REMOVAL OF BLACKHOLE ATTACK IN MANET

Neha Sharma[1], Anand singh Bisen[2]
[1]M.Tech Scholar, Dept. of CSE, VITM Gwalior (M.P.)
[2]Associate Professor, Dept. of CSE, VITM Gwalior (M.P.)

ABSTRACT:- **Communication networks are often used to transfer vital and confidential information for a variety of purposes, and if we do not update our networks to cope up with the latest challenges, the networks may remain vulnerable, as a consequence may attract the attention of mischievous users to disrupt or destroy the information flow. This has led to heightened awareness of the need to become aware of the current developments in network technologies to protect data and resources from disclosure. Some attacks on networks are planned and specifically targeted, whereas others may be opportunistic, resulting from eavesdropping activities. Further, the threats to network are continually increasing with discovery of new issues, and solutions to counter those issues are needed. With this workshop attempts will be made to provide an insight into the enduring principles of network communication, routing, security and their implementations**

I. INTRODUCTION

Wireless mobile ad hoc network (or simply MANET)) is a self-configuring network which is composed of several movable user device. These mobile device communicate with each other without any infrastructure, furthermore, all of the transmission are take place through wireless medium. MANET is widely used in military purpose, personal area network , disaster area and so on. However, there are still many open issues about MANETs, such as finite transmission bandwidth, security problem, abusive broadcasting messages, dynamic link establishment , reliable data delivery and restricted hardware caused processing capabilities.

The security threats have been extensively discussed and investigated in the wireless networks, the saame situation has also happened in MANET due to the inherent design defects. There are many security issues which have been studied in previous years. For instance, jellyfish attacks, wormhole attacks, black hole attacks and poisoning attacks, packet replication, DoS attacks, distributed DoS (DDoS) attacks, especially, the misbehavior routing problem is one of the popularized threats such as black hole attacks. Some researchers propose their secure routing method to solve thisproblem, but the security problem in MANT is still unable to prevent completely.

In this paper, we studyon different types of black hole attacks in MANET which can be divided into ordinary black hole attack and collaborative black hole attack.

II. ROUTING PROTOCOL

Routing Protocols are classified into following three categories:

1. PROCTIVE
2. REACTIVE
3. HYBRID

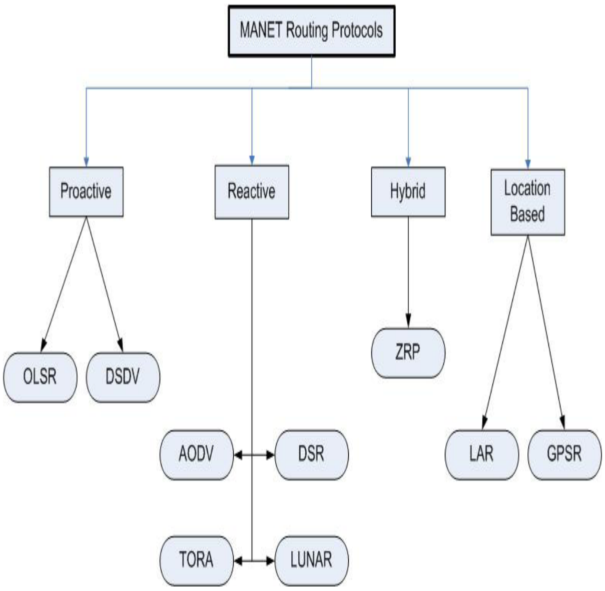

Fig: Classification of MANET Routing Protocols

2.1 Proactive Routing Protocol

A Proactive (Table-driven) Routing Protocol attempts to allow each node using it to always maintain an up-to-date route to each possible destination in the networks, the protocol periodically exchanges routing information with other nodes in order to allow new route to be discovered and existing route to be modified if they break due to factors such as node mobility and environmental changes

2.2 Reactive Routing Protocol

A Reactive (On Demand) Routing Protocol only attempts to a discover a route to some destination when it has a packet to route to some destination when it has a packet route to that destination and does not already know a route there; then source node start the route discovery process for finding the route to the destination.

III. OVERVIEW OF AODV

The AODV Routing protocol uses on-demand approach for finding routes between source and destination, that is, a route is established only when it is required by a source node for sending data packets to the destination. It uses destination sequence numbers to identify the latest path. Every node in an Ad-hoc network maintains a routing table in his cache, which contains information about the path to a particular node. suppose a node wants to send packet, it first checks its routing table to check whether a route to the particular destination is available or not. If so, it uses that route to send the data packets to the destination. If a route is not available or the previously entered route is inactivated, then the node starts a route discovery procedure. A RREQ (Route REQuest) packet is broadcasted by the sender node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends RREP (Route REPly) packet to the source. If it is not the destination, then it checks with its routing table to determine if it has fresh route to the destination. If not, it forwards the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the comparison of the destination sequence number in its routing table with the destination sequence number present in the RREQ packet is done. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREP packet, then the node update its routing table. If the number in the routing table is higher than the number in the packet, it denotes that the route is a fresh route and packets can be sent through this route. This intermediate node then sends a Route reply packet to the node through which it received the Route request packet. The RREP packet gets revert back to the source node through the reverse route. The source node then updates its routing table and sends its data packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out many attacks against AODV.

Black hole attack: A Black Hole attack [3] is a kind of denial of service attack where a malicious node gives false information of having shortest route to the destination in order to get all the data packets and drop it. In the following illustrated Figure 1. , imagine a malicious node M. When node S broadcasts a RREQ packet, other neighbor node receives it. Node M, being a malicious node, does not check up with its routing table for the requested route to node D. Hence, it immediately sends back a RREP packet, claiming of having shortest path to the destination. Node S receives the RREP from M immediately and assumes that the route through M is the shortest route and sends packet to the destination through it. When the node S sends data to M, it absorbs all the data and drop the packets thus behaving like a Black hole.

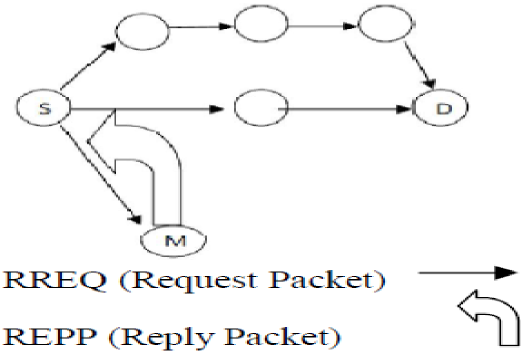

Figure Black hole attack in AODV

IV. SECURITY ATTACK & CHALLENGES

We have to consider external as well as internal attack on MANET. The nature of wireless ad hoc networks makes them very vulnerable to attack. First of all, the mobile nodes are independent and their movements are not controlled by the system, so they can easily be captured, compromised and hijacked. Secondly, since in wireless networks there are no physical obstacles for the adversary, attacks can come from all directions and target any node. Third, in wireless ad hoc networks adversaries can exploit the decentralized management for new types of attack designed to break the cooperative algorithms. Thus following are the ways by which security can be breached. Table I describes various Routing Attack at NETWORK Layer for MANET. In this article Black Hole attack is focus for Combat Approach.

V. PREVIOUS WORK

H. Deng et. al. [8] discussed a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source node gets this information, it sends a RREQ to the next hop to verify that the target node (i.e. the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a Further Request, it sends a Further Reply which includes the check result to the source node. Based on information in Further Reply, the source node judges the validity of the route. In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP. One limitation of the proposed method is that it works based on an assumption that malicious nodes do not work as a group, although this may happen in a real situation.

B. Sun et. al. [9] use AODV as their routing protocol and simulation is done in ns2 simulator. The detection scheme used neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to build the true path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are: Step 1- Collect neighbor set information. Step 2-Determine whether there exists a black hole attack. In Response procedure, Source node sends a modify-Route-Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination.

S. Ramaswamyet. al. presented an algorithm in [10] for identifying cooperative black hole nodes. They are the first to propose a solution to cooperative or group black hole attack. The methodology works with slightly modified AODV protocol by introducing Data Routing Information (DRI) Table and Cross Checking. DRI table contains {Node ID, From, Through}.Every node maintains this table. They rely on reliable nodes (nodes through which the source node has routed data) to transfer data packets. When an intermediate node replies a RREP to a given source node, the Next Hop Node and DRI entry of Next Hop Node should also be sent together. The Source node will then use the information together with its own DRI table to check whether the Intermediate Node is a reliable node. If it is not reliable, then it sends a Further Route Request packet to the node next to the intermediate node and asks NHN: 1) if IN has routed data packets through NHN, 2) who is the current NHN’s next hop to destination, and 3) has the current NHN routed data through its own next hop. The NHN in turn responds with Further Route Reply message including 1) DRI entry for IN, 2) the next hop node of current NHN, and 3) the DRI entry for the current NHN’s next hop. Based on the Further RouteReply message from NHN, source node checks whether NHN is a reliable node or not. Moreover, in the case when the network in not under the attack, the algorithm takes more time to complete. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks.

TABLE I Various Routing Attacks with brief description

S. No	Routing Attack	Brief Description
1	**Black Hole**	Malicious node injects false route replies to the route requests it receives, broadcasting itself as having the shortest path to a destination
2	**Wormhole**	The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network
3	**Replay**	An attacker that performs a replay attack injects into the network routing traffic that has been captured previously .
4	**Denial of Service**	Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network .
5	**Blackmail**	This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender.
6	**Routing Table Poisoning**	In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes .
7	**Rushing Attack**	Rushing attack is the results in DoS when it used against all previous AODV routing protocols

A lot of work have already done on Blachhole attack and they have already analysis about their harms and effects generated on AODV networks, a brief summary of previous research is given as

5. COMPARISON OF PREVIOUS WORK AGAINST BLACKHOLE ATTACK

es Against Black Hole	**Routing protocol**	**Simulator Used**	**Year of Public ation**	**First Author's Name**	**Results**	**Defects**
DRI and cross checking	AODV	No simulator	2003	Ramaswamy S	No simulation results	-
DRI table and cross checking using FREQ and FREP	AODV	-	2007	Weerasinghe H	A higher throughput performance almost 50% than AODV	5-8% more communication overhead of route request
DCM	AODV	NS-2	2007	Yu CW, Wu T-K	The PDR is improved from 64.14 to 92.93% and the detection rate is higher than 98%	A higher control overhead than AODV
Hash based	DSR	-	2009	Wang W	No simulation results	-
MAC and Hash based PRF scheme	AODV	NS-2	2009	Min Z	The PDR is higher than 90% when AODV is inaccessible 50%	The malicious node is able to forge a reply to dodge the detection scheme
Watchdog Protocol with AODV	AODV	NS-2	2014	Tarun Varshney	The PDR and end to end delayis lower as compared to AODV	higher control overhead than AODV And blackhole is detect after communication is staarted

VI. PROPOSED WORK

In this paper, we have proposed an enhancement in AODV protocol for the detection of black-hole nodes in the MANET. According to this method, before sending the Real RREQ, the source node sends a RoutrRequest for the Destination D', which do not exist in the network. This RREQ is named as FakeRREQ. After sending it, the source node waits for RREP's from all possible route . On receiving this RREQ as per their behavior, the black-hole node create a fake Route Reply, and send it to the source node. after getting these replies, source node copies IP addresses of RREP generators from the proposed RREP ORIGINATOR IP ADDRESS field of RREP into a proposed table named as Black-List table.

Now the source node send a actual RREQ and also send blacklist table to all nodes, after that nodes mark this blacklist nodes as malicious node, in future if any reply is coming from this malicious nodes then nodes first check this node is malicious or not if it is malicious then node discard RREP come from malicious node other wise it forward to the source node.With the help of this method we can detect and remove blackhole node even multiple blackhole node from the network for smooth and efficient transfer of data packets from sender to receiver.

PROPOSED ALGORITHM:-

Notations:

SN: Source Node

IN: Intermediate node

DN: Destination node

FRREQ: Fake RREQ

```
1. SN broadcasts FRREQ.
2. If source node  receives Route Rply for fake route request
3. source checks the RREP packet for the address of the node initialized RREP and marks the node as malicious and save it to blacklist table.
 4.Now source node Send actual RREQ for the destination and also append the malicious node list in RREQ Packet.
5. If RREQ Received by Inetrmediate node
{
then it exatract the blacklist table and mark the malicious node in his neighbour table. In future if RREP is received from malicious node the intermediate node discard this RREP by checkhing his neighbor table .
}
6.If RREP is Sent by Destination node Consider the route to be safe and start routing the data packets
Else
If RREP is send by intermediate node then every receiving node check that this RREP is not sent by malicious node from blacklist table if it is from blacklist table then discard it otherwise forward to the source.
```

VII. CONCLUSION

Black Hole Attack is a big security threat of network that degrades the working prformance of the AODV protocol. Its detection is the main issue .Many researchers have proposed different types of detection and removal mechanisms for removing black hole attack. This paper has discussed about various method for black hole attack detection in MANETs and identify their drawbacks. We compared various methods and observe that these technique detects malicious node, but no one is perfect in all aspects since most of the mechanism having some drawbacks such as large time delay, much routing overhead because of newly introduced routing packets.But in this method we just add fake RREQ mechanism for finding blackhole attack and remove by low overhead technique. In future, we will simulate this mechanism in network simulator (NS2) .

VIII. REFERENCES

[1] shashi gurung, aditya kumar, krishan kumar saluja," survey of black hole attack detection in mobile adhoc networks" in Proceedings of International Joint Conference, 7th July 2013, Goa, India, ISBN: 978-81-927147-7-6

[2] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao," A survey of black hole attacks in wireless mobile ad hoc networks" in Human-centric Computing and Information Sciences 2011, 1:4

[3] Rohit Pal, Mukesh Azad, Santosh kumar," An Approach to Combat the Blackhole Attack in AODV Routing Protocol" in *International Journal of Computer Applications (0975 – 8887) Volume 77 – No.11, September 2013*

[4] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan," Mitigation of Black Hole Attacks for AODV Routing Protocol" in International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(2): 336-343 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085)

[5] S.V.Shirbhate, Dr.S.S.Sherekar, Dr.V.M.Thakare," A Novel Framework of Dynamic Learning Based Intrusion Detection Approach in MANET" in International Conference on Computing Communication Control and Automation 2015

[6] C. E. Perkins, E.M. Royer , "Ad-hoc on-demand distance vector routing," Mobile Computing Systems and Applications, 1999. Proceedings ,WMCSA '99. Second IEEE Workshop on, vol., no., pp.90-100, 25-26 Feb 1999.

[7] C. E. Perkins, E.M.B .Royer, S. Das , "Ad hoc on-demand distance vector (AODV) routing," IETF Internet Draft, MANET working group, Jan.2004.

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

[9] B. Sun, Y. Guan, J. Chen and U. Pooch," Detecting Black-hole Attack in Mobile Ad Hoc Networks". Paper presented at the 5th *European Personal Mobile Communications Conference*, Glasgow, United Kingdom, and 22-25 April 2003.

[10] S. Ramaswamy, H. Furong, M. Sreekantaradhya, J. Dixon and K. Nygard ," Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". Paper presented at the *International Conference on Wireless Networks*, Las Vegas, Nevada, USA, 23-26 June 2003.