Black Hole Attack Implementation and Detection in Mobile Ad Hoc Networks

Sweta Tarale, Dr. Abha Choubey
Department of Computer Science and Engineering, Shri Shankaracharya Technical Campus, Bhilai, India,
e-mail:swetatarale2012@gmail.com, abha.is.shukla@gmail.com

Abstract- Mobile ad-hoc networks are a collection of mobile hosts that communicate with each other without any infrastructure. Security is an essential requirement in mobile ad-hoc networks to provides protected communication between mobile nodes. MANET are vulnerable to various types of attacks. One of main active attacks is black hole attack, it is a denial of service attack and it drops entire incoming packets between one source to destination. In this paper we studied the details about black hole attack, and mechanism for detection of black hole attack in MANET.

Keywords-*Mobile ad hoc network(MANET),AODV,Black hole attack,Routing protocol.*

*****

I. Introduction

Mobile ad hoc network is one kind of new wireless network structure. In ad hoc network all nodes are movable and the topology of the network is changing dynamically[1]. MANET can be used to enable next generation battlefield applications. MANETs have some special characteristics features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, battery, lifetime, and computation power of nodes etc [2]. One of the most critical problem in MANETs is the security vulnerabilities of routing protocol .In this paper a mechanism is proposed to identify multiple black hole nodes cooperating as a group in ad hoc network. The proposed technique works with slightly modified AODV protocol and makes use of the data routing information table.

The rest of paper is organized as follows: section II presents the related researches. Section III gives overview of AODV protocol and its security problems .Section IV describes proposed algorithm .Section V simulations.Section VI gives conclusion and future scope of work.

II .RELATED WORK

Researchers have proposed various techniques for detection and prevention of Black hole attack in mobile ad hoc network.

In[3] proposed a solution which is based on cluster organization of network. In this scheme they maintain a history table which contain send packets, received packets, and dropped ratio which is calculated by using received packets/send packets for every node, but no simulation or performance evaluation have been done.

[2] introduces the use of Data Routing Information (DRI) to keep track of past routing experience among mobiles nodes in the network and cross checking of RREP messages from the intermediate nodes. The drawback of this technique is that mobile nodes have to maintain an extra database of past routing experience.

In[4] defines how implement Black hole attack in ad hoc on demand distance vector protocol.

[5] proposed new trust management frame work(TMF),which calculates a node's trust value based on observations from neighbor nodes by using Grey theory and fuzzy logic sets.

The TMF chooses multiple rather than a single parameter to obtain trust value. The proposed frame work can do is not only

detecting abnormal trust behavior but also discovering parameter for forming trust values.

[6] In this paper, a defense mechanism is presented against a coordinated attack by multiple black hole nodes in a MANET. The simulation carried out on the proposed scheme has produced results that demonstrate the effectiveness of the mechanism in detection of the attack while maintaining a reasonable level of throughput in the network.

In[7] proposed mechanism using a quantitative method to detect intrusion in MANETS with mobile nodes. This method is a behavioral anomaly based system, which makes it dynamic, scalable, configurable and robust. Finally, verify method by running ns2 simulations with mobile nodes using Ad-hoc on- demand Distance Vector (AODV) routing. It is observed that the malicious node detection rate is very good, and the false positive detection rate is low.

[1] proposed path based method to detect black hole attack, and adaptive algorithm to enhance the detection performance by using detection algorithm, it is based on path based scheme that is a node does not watch every node in the neighbor, but only observes the next hop in current route path.

In [8] the author discuss a protocol DPRAODV and the ALARM used in DPRAODV in this scheme the RREP sequence number is extra checked whether higher than the threshold value or not, if the value of RREP sequence number is higher than the threshold value, the sender is referenced as an attacker and updated it to black list. The ALARM is sent to its neighbor who includes the black list, thus the RREP from the malicious node is blocked but is not processed.

III.AODV AND ITS SECURITY ISSUES

A.AODV Protocol: The Ad hoc On-Demand Distance Vector (AODV) is an embedded MANET protocol that works dynamically to establish and maintain routes, adapting quickly to changing link conditions .AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number.

B. Black Hole Attack:

In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network into two disconnected components.[9].

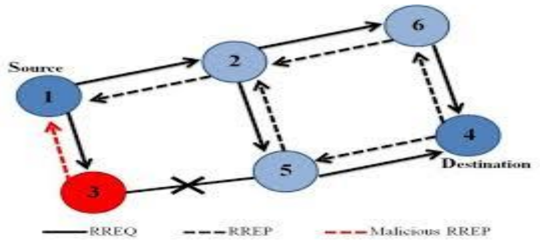

Fig1: Black Hole Attack

C. Cooperative Black Hole Attack:

This attack is similar to Black-Hole attack, but more than one malicious node tries to disrupt the network simultaneously. It is one of the most severe DATA traffic attack and can totally disrupt the operation of an ad hoc network. Mostly the only solution becomes finding alternating route to the destination, if at all exists. According to the original AODV protocol, when source node S wants to communicate with the destination node D, the source node S broadcasts the route request (RREQ) packet. The neighboring active nodes update their routing table with an entry for the source node S, and check if it is the destination node or has a fresh enough route to the destination node. If not, the intermediate node updates the RREQ (increasing the hop count) and floods the network with the RREQ to the destination node D until it reaches node D or any other intermediate node which has a fresh enough route to D, as depicted by example in Figure 1. The destination node D or the intermediate node with a fresh enough route to D, initiates a route response (RREP) in the reverse direction, as depicted in Figure 3. Node S starts sending data packets to the neighboring node which responded first, and discards the other responses. This works fine when the network has no malicious nodes.

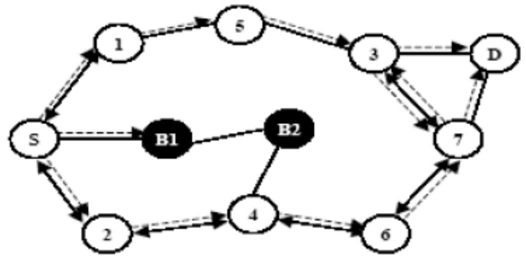

Fig.2. Network flooding by RREQ messages

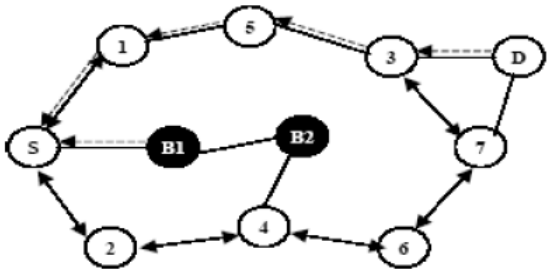

Fig.3. Propagation of RREP messages

IV THE PROPOSED ALGORITHM

In this section the proposed algorithm for detection of cooperative black hole attack is presented. The mechanism modifies the AODV protocol by introducing two concepts:

A..Data Routing Information:

For route discovery process each node maintains additional two bit of information.Every node has its own DRI(Data Routing Information) table. The bit 1 stands for the true and 0 stands for the false.The first bit from stands for information on routing data packet from the node.The second bit through stands for the information on routing data packet through the node[6].Following table is DRI (Data Routing Information) of the node 4 in the figure 3.

Node#	*From*	Through
3	1	0
6	1	1
B2	0	0
2	1	1

Table 1:DRI of node 4

B. Cross Checking:

In this mechanism the source node broadcast a RREQ message to discover Secure route to the destination node.

The intermediate node generates RREP message provides its Next Hop node and the DRI entry for the Next Hop Node. Upon receiving RREP message from intermediate node the source node checks own DRI table to whether intermediate node is a reliable node then source node routing data through intermediate node . If intermediate node is unreliable then source node sends further request message to the NextHop Node then Next Hop Node sends further reply message to the source node which includes next hop node of a current next hop node and DRI of Intermediate node and DRI entry of current's next hop node. Based on route reply message source node checks whether next hop node is a reliable node or not . If next hop node is a reliable node source node checks whether intermediate node is black hole node. If the second bit of the DRI table entry from intermediate node is 1 and first bit of DRI entry from next hop node is 0 then intermediate node is black hole node. If the intermediate node is black hole node source node ignores all the RREQ packets from the black hole node and broadcasts the list of black hole node . If the intermediate node not a black hole node and next hop node is reliable node the source node sends data packets to the destination.

V.SIMULATIONS

The experiments for the evaluation of the proposed scheme have been carried out using the network simulator *ns-2.*

Network Designing and AODV Evaluation:
Mobility: 10-35 m/s
Packet rate: 4/s
Number of nodes: 100
Network Size: 1000 x 1000
Max propagation range: 250 m
Mac: 802.11
Routing Protocols: AODV
Transport Protocol: UDP
Traffic: CBR
Simulation Time: 100s
Results:

- Average Throughput vs. Mobility
- Average delay vs. Mobility
- PDR vs. Mobility
- Packet dropped vs. Mobility

AODV under Malicious Attackers Evaluation:
Mobility: 10-35 m/s
Packet rate: 4/s
Number of nodes: 100
Network Size: 1000 x 1000
Max propagation range: 250 m
Mac: 802.11
Routing Protocols: AODV
Transport Protocol: UDP
Traffic: CBR
Simulation Time: 100s
Attackers: 10 %
Results:

- Average Throughput vs. Mobility
- Average delay vs. Mobility
- PDR vs. Mobility
- Packet dropped vs. Mobility

Modified AODV for the Malicious Attacks detection:
Mobility: 10-35 m/s
Packet rate: 4/s
Number of nodes: 100
Network Size: 1000 x 1000
Max propagation range: 250 m
Mac: 802.11
Routing Protocols: MDAODV (Malicious Detection based AODV)
Transport Protocol: UDP
Traffic: CBR
Simulation Time: 100s
Attackers: 10 %
Results:

- Average Throughput vs. Mobility
- Average delay vs. Mobility
- PDR vs. Mobility
- Packet dropped vs. Mobility

In this phase of simulation we modified AODV protocol for detection of the black hole attack using black hole attack detection algorithm[2].In this algorithm when Source Node(SN) broadcasts ReadRequest(RREQ),then if Read Reply(RREP) send by Destination Node(DN) or reliable node then source node route data packets otherwise source node send Further Request(FR$_q$) and Identity of the node(ID) of Intermediate Node(IN) to NextHopNode(NHN) then source node receive FurtherReply(FR$_P$), NHN of current NHN,and DRI(Data Routing Information) entry for current IN(Intermediate Node).when source node receives these information algorithms checks NextHop Node (NHN) is reliable node and Intermediate Node(IN) not a black hole node then it route data packets ,otherwise it shows there is insecure route and its Intermediate Node(IN) is black hole and nodes from Intermediate Node to the node that generated RREP are black holes and if IntermediateNode(IN) is not reliable node then current IntermediateNode(IN) is a Next Hop Node(NHN). By using this algorithm Source Node(SN) finds secure route to the destination and improves performance of the network by detecting black hole attack.In figure 4 throughput is plotted against mobility.It is observed that throughput is better with AODV. The throughput is reduces when network is under the black hole attack.In figure

5 number of packet dropped against mobility is plotted.It is observed that performance of network is decreases under black hole attack due to more packet dropped.

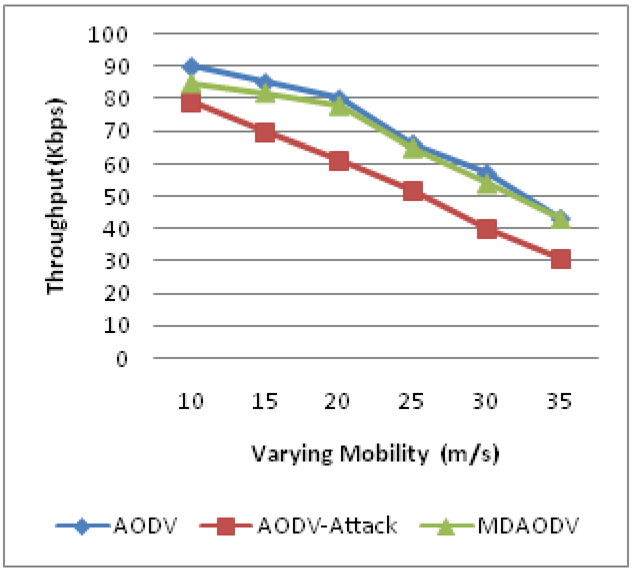

Figure4. Throughput vs. Mobility

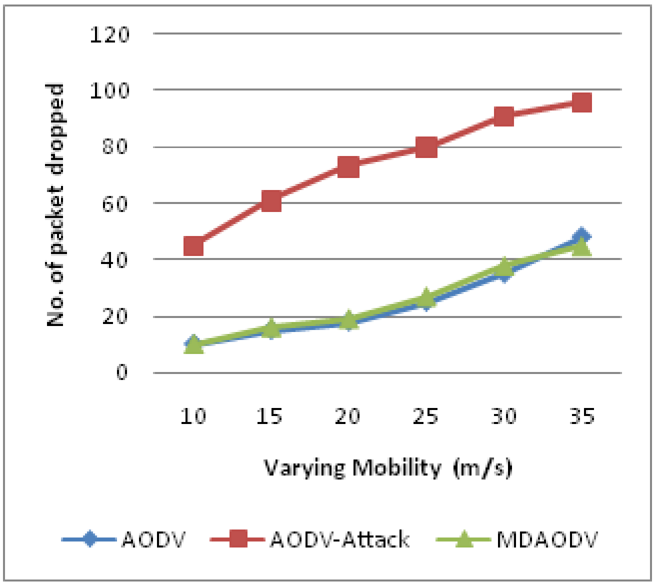

Figure5. No. of Packets vs. Mobility

VI. CONCLUSION

In this paper we have studied detailed about mobile ad hoc network. We also studied AODV routing protocol and its security issues and black hole attack in MANET. We give feasible solution for detection of black hole attack in the network. As a future scope, we apply this mechanism for detecting of other types of attacks in the network such as gray hole attack, packet dropping attack for improving the performance of network.

REFERENCES

[1] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An adaptive approach to detecting black and gray hole attack in ad hoc network,24th IEEE conference on Advanced Information Networking and Applications,2010.

[2]] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A mechanism for detection of cooperative black hole attack in MANET, second IEEE international conference on Intelligent System, Modelling and Simulation,2011.

[3] Shirsty Chandel, Ashish Tiwari, "A weighted clustering algorithm for improving MANET security", International Journal of Computer Science and Information Technology research,2014.

[4] Monika Roopak, Prof. BVR Reddy, "Black hole attack implementation in AODV routing protocol, International Journal of Sceintific and Engineering Research,2013.

[5] Ji Guo, Alan Marshall, Bosheng Zhou, "A new trust management framework for detecting malicious and selfish behaviour for MANET,International Joint Conference of IEEE,2011.

[6] Sanjay Ramaswamy, Huirong Fu, Monalar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of cooperative black hole attack in wireless ad hoc network, IACC.

[7] Suman S Chandrakar, Brajeshpatel, Amit Kumar Chandanan "Detection of suspected nodes in MANET" ACEEE International Journal on Network Security 3, 1 (2012) 6 ACEEE Int. J. on Network Security , Vol. 03, No. 01, Jan 2012.

[8] Payal N.Raj, Prashant B. Swadas, "DPRAODV: A dynamic learning system against black hole attack in AODV based MANET,International Journal of Computer Science Issues,2009.

[9] Sweta Tarale,Dr. Abha Choubey,"Detection of Black Hole Attack in MANET: A Review,International Journal on Recent and Innovation Trends in Computing and Communication,2018.