Cooperative Black Hole Detection Mechanism in Mobile Ad Hoc Network

Mithilesh Izardar
BE Student
SIT, Lonavala

Mohd. Rizwan Khan
BE Student
SIT, Lonavala

Siddhartha Mishra
BE Student
SIT, Lonavala

ABSTRACT
A MANET (mobile ad hoc network) is a collection of independent nodes that communicate with each other by organizing a multi-hop radio network by sustaining connections that are decentralized. MANET has open medium, includes dynamically changing topology, absence of centralized monitoring points and less clear lines of defense, and because of this security in a MANET is a critical issue. Ad hoc on- demand distance vector (AODV) is a well-known routing algorithm. It is assailable to attacks like black hole and gray hole. In a black hole attack a malicious node act like ordinary node, but if a data packet passes through malicious node it consumes data packet and never forward it to neighboring nodes, whereas in a gray hole attack the malicious node will forward the data packet with selective data. In this paper we are presenting a defense mechanism for detection of cooperative black hole attack by multiple black hole nodes and the prevention of attack in multiple base stations. The simulation carried out on the proposed mechanism has produced results that elaborate the detection mechanism against the attack while maintaining a level of throughput in MANET.

Keywords
Mobile ad hoc network (MANET), Black Hole, malicious node ,Gray Hole, Routing, AODV.

1. INTRODUCTION
A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. MANET can be used in various fields like battlefield application, micro-sensor network, situation awareness system etc. Various characteristics of MANET are unreliable wireless media used for communication between hosts, changing network topologies, limited bandwidth, lifetime computation power of nodes, battery, flexibility etc. MANETs are capable of defending various attacks which includes denial of service, impersonation, passive eavesdropping etc. To improve the security of MANET, authentication and redundant transmission can be used. The ad hoc network has the dynamic feature to decide the path for data packet. So an ad hoc network always requires a security or detection mechanism to prevent attacks.

In a MANET, security of routing protocol is critical problem. More than one node can be compromised in a MANET such a way that they act like a malicious node so detection of these nodes will not be easy. These nodes may generate false data or drop the data packet. These nodes also have the ability to change the path of data packets. These nodes also generate message to non-existence links or provide incorrect link state information. MANET uses ad hoc on-demand distance vector (AODV) routing protocol [1]. It is source initiated on demand routing protocol. AODV is prone to black hole attack. In [2], the authors have proposed that black hole nodes in a MANET work independently and proposed an algorithm to prevent a single black hole, but the proposed algorithm does not work in case of cooperative black hole attack. In this paper the proposed mechanism uses *data routing information table.* (Section) to detect the cooperative black holes.

The paper is organized as follows. Section II discusses about the attacks .Section III will give you brief knowledge about AODV protocol. Section IV will describe the proposed algorithm and security protocol. Section V presents the results obtained from simulation. Section VI concludes the paper and highlights the future scope of the same.

2. ATTACKS
2.1 Black hole attack
Mobile ad-hoc network (MANET) is a collection of wireless nodes which interacts with each other when required. There is no specific fixed path in between nodes because of which security and data protection is a challenging task. There are several attacks which can cause data loss or compromise the security of MANET, some of which are black hole, gray hole, impersonation, passive eavesdropping. When a data packet is send to any intermediate node and the intermediate node never passes the data packet to its neighboring node then we assume the node as a black hole node. After the black hole node is identified, sending of data packet is ceased.

A black hole node is an independent node which resides in MANET and tries to communicate with any of the node present in the network.

The black hole node causes two things. First, the node can alter the routing protocol such as AODV by publicizing itself as having shortest path to the destination. Second, the black hole node consumes the data packets.

2.2 Co-operative black hole attack
In case of black hole, we have multiple algorithms to prevent the attack from a single black hole. But in case of multiple black hole attack, more then one black hole node cooperates with each other by sending requests to each other. If the source node requests to send the data packet to the destination, it has to pass through the intermediate nodes. Suppose source node S releases Route Request (RReq) to black hole node B1 then B1 refers to its associative black hole node B2, the source node S sends a Further Request (FRq) to B2. The source node S asks B2 that if it has a route to destination node or B1. As B2 is black hole node its Further Reply (FRp) will be "OK" to both the enquiries. So here the data will be lost.

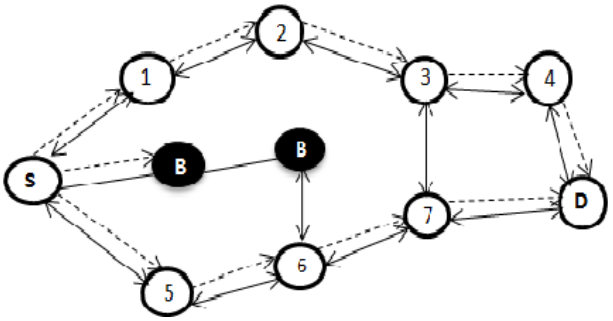

Fig.1. Network flooding by RREQ messages

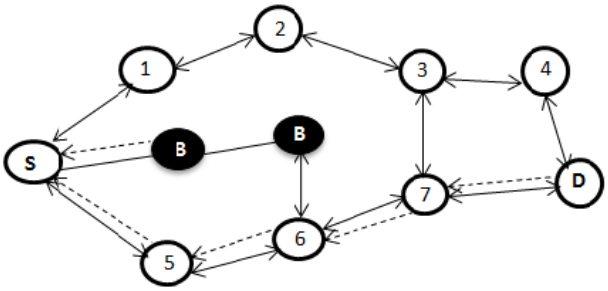

Fig.2. Propagation of RREP messages

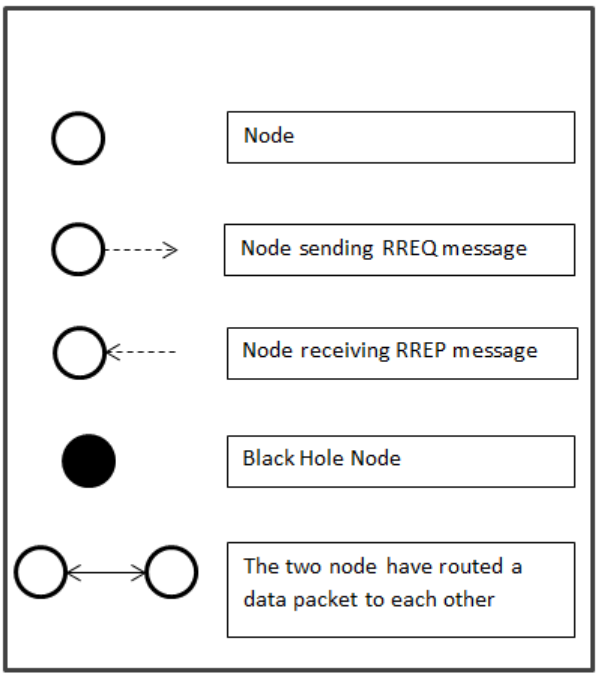

Fig 3. Symbolic notations used in diagrams

3. AODV PROTOCOL

AODV is an instant reactive routing protocol. It does not require maintaining information about the routes from source to the destination node which are not in active communication. Instead of which the mobile nodes quickly obtain routes to the destination node. Each mobile node will have routing table in which the next hop node information for the route to destination node is stored. There are two methods to find a route to the destination node. First, if a fresh route is available in routing table then the route has to be a specified route in routing table. Second, if the former method fails, we have to go through a procedure which is as follows.

The source node initiates a process to find route to the destination node by broadcasting a *RouteRequest* (RREQ) message to its neighbors. When the neighboring node receives a RREQ message they update their routing table with reverse route to the source node. Any node which has received the RREQ message and does not have a route to destination node will also broadcast a RREQ message to its neighbors. The node will increment the hop count then forward the RREQ. A *RouteReply* (RREP) message is send to the Source node when the RREQ message reaches to the node, whether it is destination node itself or the intermediate node that has route to the destination. The RREP message is a unicast message for source node.

AODV uses this sequence number to determine the aliveness of the route and to ensure the loop-free route. When there are multiple routes from source to destination, AODV uses sequence number to select the route for data packet transfer. If multiple routes with highest sequence number are there then the protocol will choose the route with less hop count. To keep the route entries fresh timers are used.

To refresh and maintain the connectivity of the neighboring nodes, AODV protocol sends a 'hello' message periodically. *RouteError* (RERR) occurs when any error happens during the data packet travelling, such as when a link breaks. RERR packets are transmitted along the reverse path to the source node. While transmitting along the reverse path the entries in routing table are invalidated.

In AODV there is no direct mechanism or algorithm to prevent or detect the malfunctioning of a node. The malfunctioning of a node can be IP spoofing, packet dropping, MAC spoofing, depletion of data information from control packets or data packets. To prevent malfunctioning of nodes protocols like SAR [15] have been developed to secure AODV protocol.

4. DATA ROUTING INFORMATION

Data routing information is a table which is used for checking the identity of node and history of data routing. Whenever the RREQ message is broadcasted the intermediate node has to respond to that. Each node maintains a DRI table. It contains three entries (i)Node ID (ii)From value (iii)Through value .

Bit 0 stands for "FALSE" and bit 1 stands for "TRUE".

Node id	FROM	THROUGH
1	0	0
2	1	1
3	`1	0
4	1	1

5. CROSS CHECKING

To prevent the attacks on a MANET, we have proposed a scheme called cross checking. In this scheme the reliability of a node is checked before transferring of data packet. The reliable node means the Source has transferred the data packet previously. In proposed scheme we are going to change the AODV protocol. In the modified protocol, the source node (SN)

will broadcast a RREQ message. The intermediate node (IN) will reply to SN via RREP message with its NHN's information and with DRI table. When the SN receives the message from IN the SN will check its own DRI table to see weather IN is reliable or not. If IN is used previously for data routing with SN then it is reliable else it will send a *FurtherRequest* (FRq) toIN's NHN to check the IN's reliability. SN request two checks for IN, first is that if NHN has routed data packet successfully with IN and second is that who is the NHN's next hope node to destination and third is that if NHN has routed data through Its own NHN. After receiving the FRq the NHN response with FRp message which contains these information first, DRI entry for IN. Second, the info for NHN's next hop and third, NHN's next hope node's DRI entry. Now SN will check for NHN's reliability , if NHN if NHN is reliable then SN will check IN's second bit of DRI entry if it is 1 then it has routed data through NHN if first bit is 0 then NHN has routed data packet from IN so SN will know that the IN is a black hole. If IN is a black hole then SN will reverse its path from Intermediate Node If NHN is reliable node and IN is not a black hole then SN will send the data packet through this route.

6. SIMULATIONS

All the experiments which are carried out for the working of proposed scheme are done with the help of network simulator ns-2. The 802.11 MAC layer implemented in ns-2 is used for simulation. An improved version of random waypoint model is used as the model of node mobility [16]. The Performances of mainly three protocols have been examined : (i) Standard AODV protocol, (ii) AODV with the proposed algorithm, and (iii) AODV with three malicious nodes cooperating in a blackhole attack. The environment developed to carry out the tests uses two parameters: (i) the number of active connections in the network and (ii) the mobility of the nodes. The following parameters for simulation are used as written in Table II.

Sr. No.	Parameter	Value
1	Simulator	NS 2.35
2	DoS Attack	Gray hole, Gray Hole Attack
3	Channel Type	Wireless channel
4	Antenna Type	Omni directional
5	The protocol used	AODV
6	Underlying MAC Protocol	IEEE 802.11
7	Propagation Model	Two-Ray Ground
8	Queue	PriQueue
9	The number of Malicious nodes Detected	Two or more nodes which are dropping packet
10	Nodes	21

7. CONCLUSION

In this paper, security issues related with routing in MANETs are discussed in brief, and in specific the cooperative blackhole attack has been explained in detail. With the help of security protocol that has been proposed in the paper can be utilized to identify and discover multiple blackhole nodes in a MANET and find a safe routing path from a source node to a destination node avoiding the blackhole nodes. The proposed work has been experimented by implementing it in the network simulator ns-2, and the results explains the effectiveness and efficiency of the mechanism. In future the proposed security mechanism can be extended and explored, so that it can defend against other attacks like resource consumption attack and packet dropping attack. Working on the protocol for efficiently and effectively defending against grayhole attack- an attack where some nodes flip their states from blackhole to honest intermittently and vice versa, is also an interesting future work.

8. REFERENCES

[1] C. Perkins, E. Belding-Royer, and S. Das, "Ad-hoc on-demand distance vector (AODV) routing", Internet Draft, RFC 3561, July 2003.

[2] H. Deng, H. Li, and D. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, Vol. 40, No. 10, Oct 2002.

[3] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks, In Proceedings of the 8th International Conference on Mobile Computing and Networking (Mobicm 2002), pp. 12-23, ACM, Atlanta, GA, Sept 2002.

[4] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks", In SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, Jan 2002.

[5] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "A secure routing protocol for ad hoc networks", In International Conference on Network Protocols (ICNP), Paris, France, Nov 2002.

[6] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad hoc networks", In International Conference on Network Protocols (ICNP), pp. 251-260, 2001.

[7] J.Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks", In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), 2001.

[8] F. Stajano and R. Anderson, "The resurrecting duckling", Lecture Notes in Computer Science, Springer-Verlag, 1999.

[9] S. Marti, T. Giuli, K.Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of MOBICOM 2000, pp. 255-265, 2000

[10] S. Buchegger and J. Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation Of Nodes- Fairness In Dynamic Ad hoc NeTworks", In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, Jun 2002.

[11] S. Buchegger and J. Boudec, "The effect of rumor spreading in reputation systems for mobile ad hoc networks", In WiOpt '03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Mar 2003.

[12] M. Jakobsson, J. Hubaux, and L. Buttyan, "A micro-payment scheme encouraging collaboration in multi- hop cellular networks", in Proceedings of Financial Crypto 2003.

[13] S. Bansal and M. Baker, "OCEAN: Observation- based cooperation enforcement in ad hoc networks", Technical Report, Stanford University, 2003.

[14] J. Sen, M. Girish Chandra, P. Balamuralidhar, S.G. Harihara, and H. Reddy, "A distributed protocol for detection of packet dropping attack in mobile ad hoc networks", in Proceedings of IEEE International Conference on Telecommunications (ICT'07), May 2007, Penang, Malaysia.

[15] S. Ki, P. Naldurg and R. Kravets, "Security aware ad hoc routing for wireless networks", in Proceedings of the 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing, Poster Session, pp 299- 302, Long Beach, California, October 2001.

[16] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful", in Proceedings of IEEE INFOCOM, pp. 1312 – 1321, 20