ISSN 2229-5518

Decoy Black-Hole Attack

Sabeeha Mehtab, Aruna B. Dulloo

Abstract— Mobile ad hoc networks are being widely deployed currently since they provide some features, which are difficult or impossible to be achieved by conventional networks. The application area ranges from the battlefield (sensor nodes in hostile territory) to general transportation that provide useful infrastructure during disaster recovery. Due to the great importance of MANET, security in ad hoc networks is a hot research area and already significant research is done in this field. The use of wireless links in an ad hoc network generates the possibility of link attacks from passive eavesdropping to active impersonation, message replay and message distortion. The Black hole attack is an active insider attack, where a malicious node uses the routing protocol to advertise as having the shortest path to nodes whose packets it wants to intercept. Wide research has been done in this area that motivated us to take this as challenge to integrate a better security solution into the existing AODV routing protocol.We have proposed a DAODV (Decoy Black-Hole AODV) algorithm uses a virtual and nonexistent address as a sender node to misguide and identify Black-Hole nodes. This algorithm works in proactive as well as reactive manner of defense architecture in MANET.

Index Terms—AODV, BlackHole,MANET,RERR, RREP, RREQ, RREQ'.

1 INTRODUCTION

MANET stands for Mobile Ad hoc Network. It is a decentralized autonomous wireless system which consists of free nodes. MANET sometimes called mobile mesh network, is a self-configurable wireless network. A MANET consists of mobile nodes, a router with multiple hosts and wireless communication devices. The wireless communication devices are transmitters, receivers and smart antennas. These antennas can be of any kind and nodes can be fixed or mobile. The term node referred to as, which are free to move arbitrarily in every direction. These nodes can be a mobile phone, laptop, personal digital assistance, MP3 player and personal computer. These nodes can be located in cars, ships, airplanes or with people having small electronic devices [1]. Nodes can connect each other randomly and forming arbitrary topologies. Nodes communicate to each other and also forward packets to neighbor nodes as a router. The ability of self-configuration of these nodes makes them more suitable for urgently required network connection. For example in disaster hit areas where there is no communication infrastructure. It is greatly desired to have a quick communication infrastructure.

There are basically four routing protocol [2] AODV, DSR, DSDV and TORA in mobile ad hoc network. However from the beginning of its design, almost none of the protocol specifies the security measures, but the nature of the wireless ad hoc networks makes them very vulnerable to malicious attacks as compared to traditional wired networks. An attack occurs when an intruder tries to exploit vulnerabilities of a system. This paper is focusing on special active attack- black hole attack. Black hole attack can occur when one of node on path directly attacks the data traffic intentionally by dropping the data traffic passing through it, so that network performance degraded tremendously and there is no security provision in the existing AODV routing protocol against this type of attack. The black hole attack [1] is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets.

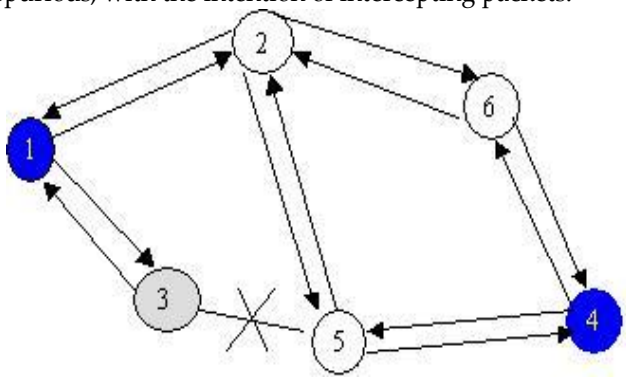

Fig1: Black Hole Attack

1.1 Ad-hoc On Demand Distance Vector Routing Algorithm(AODV):

AODV is a reactive (on-demand) routing protocol that is developed specifically for MANETs. A routing protocol in general performs two activities: Route discovery and Route maintenance. AODV uses similar route discovery as another famous on-demand routing protocol DSR [3]. Route discovery in AODV starts with broadcasting the Route Request Packet

(RREQ) by source with its ID and a unique destination sequence number to all its neighbors [4]. All neighbors that received specific RREQ for the first time then rebroadcast it after storing the ID of the sender. Storing the sender ID represents the reverse path to the source. The route discovery process ends when the destination node receives a RREQ, it sends a Route Reply (RREP) back to source node. RREP uses the reverse path to source which already is maintained by intermediate nodes. The sender then proceeds with data transmission and route maintenance. Unlike its counterpart the DSR routing protocol, a traditional AODV protocol uses a one entry per destination in its routing table . It also adopts different mechanism to maintain routing information. It uses a destination sequence number (carried by all routing packets) to prevent routing loops and to determine freshness of routing information. Another mechanism to avoid stale routes is the use of timer based route expiry. when a node detects that a route to the neighbor is no longer valid, then this node will remove the routing entry from its routing table and send a link failure message, a triggered route reply message to the neighbors that are actively using the route, informing that this route is no longer valid. For this purpose AODV uses an active neighbor list to keep track of the neighbors that are using the particular route. The node that receives this message will repeat this procedure and tell them not to follow that path. The message will be received by the affected sources that can chose to either stop sending the data or finding a new route by sending a new RREQ packet.

1.2 Exhaustive Literature Survey

There are various strategies for enhancing the routing security in mobile ad hoc network. A solution strategy is based on detection and reaction instead of trying to prevent the problem from happening. In [5], a node detects a misbehaving successor along a packet's path by promiscuously listening on its wireless interface waiting for the packet it forwarded to its successor node. They term this detection mechanism as watchdog. After detection of such a misbehaving successor, the detecting node sends a message to the packet's source that its successor node is misbehaving one. But this algorithm suffers from initial black-hole attacks as well as fails in cooperative black hole attack.

ZhaoMin[1] propose an authentication mechanisms, based on the hash function, the Message Authentication Code (MAC) and the Pseudo Random Function (PRF), are proposed to provide fast message verification and group identification identify multiple black holes cooperating with each other and to discover the safe routing avoiding cooperative black hole attack. But this algorithm needs a centralized control as an authorized third party that distribute the shared and secrete keys to the nodes. But puts heavy overhead calculation on the nodes.

Several trust models have been developed for trust management. These models can be classified into two groups: centralized and decentralized models. In centralized models, trust value are maintained by a common central node or an authorized third party. The simplest method is to keep a record which is equal to the number of positive ratings minus that of negative ones. This method is used in eBay's reputation forum[6]. The requirement of a requested third party goes against the nature of MANETs. In decentralized models, each node assigns and keep trust/trustworthiness values for other communicators. Most researchers[7-10]/12 are advocating the use of ratings and prefer making use of rating aggregation algorithms to evaluate the trust from several aspects(e.g. CPU usage, residual energy, band width etc.). However these sophisticated model are not appropriate for MANETs, where resources are limited and network topology is dynamic. several trust models[11-13]13-16 have been developed for peer tom peer system based on shared information .

2 PROPOSED SOLUTION

In this paper, we have proposed an AODV based routing algorithm that can detects avoids Black-Holes in the MANET. We have named this protocol DAODV(Decoy Ad-hoc on-demand distance vector) routing protocol. This protocol takes the advantage of Proactive as well as reactive protocols.

We can divide this protocol in two parts…

Proactive : The sender initially sends a special route request packet just to decoy Black-holes in the MANET with a nonexistent destination address. Black-hole nodes in the network grab the first chance to reply the request and are identified by sender, acting as a proactive protocol. In DAODV's RREP a Record Address field is added over the standard AODV's RREP, this Record Address field contains the address of the last node that has claimed the route for the destination.

Table1: Special Route Request Message(RREQ')

Type [8]	Reserved [16]	Hop count [8]
Broadcast ID [32]		
Virtual Address[32]		
Virtual sequence number[32]		
Originator IP address [32]		
Originator Sequence Number [32]		

Table 2: Route Reply Format(RREP)

Type [8]	L	Reserved [16]	Hop Count [8]
Destination IP address [32]			
Destination Sequence Number [32]			
Originator IP Address [32]			
Record Address[32]			

When the source node receives RREP messages from network, it tags these responders as Black-hole and triggers special route error RERR messages to all its neighbors by broadcasting the addresses of all the black-holes in the network.

Table 3: Special Route Error Message (RERR)

Type [8]	L	Reserved [16]	∞
Black-Hole address [32]			
Originator Sequence Number [32]+1			
Originator IP Address [32]			

Now all the nodes in the network update their routing tables and make a separate list of black-holes in the MANET.

Reactive: After the detection of Black-holes in MANET, the network can start its normal route discovery process. The sender sends a route request RREQ packet in the network same as in standard AODV. All the intermediate nodes maintain the route by storing the address of its predecessor nodes. The nodes which has a path to the destination responds back to the source with RREP by using the processor's address. Source node selects the shortest path from all RREP messages and start sending packets through that route. Every node after forwarding a packet listens to the next node, whether the packet is forwarded or dropped and maintains a log of it. It keeps record of Neighbor (Node Address, No of packet forwarded, No of Packet Dropped, Behavior). It calculate packet delivery ratio= no. of packet forwarded/ no. of packet dropped;

If packet delivery ratio>threshold(already assigned in the network) then the behavior of this node is marked as -1(misbehaving), else +1(properly behaving).

If the node's behavior is -1, then no further communication is made with this node and this information is broadcasted to the entire network. And once again it initial RREQ' message is triggered to the MANET to identify the Black Holes once again.

Algorithm for Decoy AODV black hole attack in MANETs is as given below-

```
Notations :S: Source Node  IMN: Intermediate Node D: Destination Node
1     Initial( )
2     {
3      S broadcasts RREQ'(Visual and not existing target address);
4     If(S receives RREP messages)
5      {
6      S triggers special RERR messages to its neighbors;
7     All nodes in network update their Routing Table removing Black Hole nodes from the list;
8     }
9     }

10    Start( )
11    {
12     Start standard AODV route discovery;
13    If(RREP  is within Time Limit and Hop Count Limit)
14    {
15    Start sending packets;
16    Every node listens to its next node;
17    If(packet forwarded)
18     {
19    Forward_count= Forward_count +1;
20    Discard Packet from  buffer ;
21    }
22    Else
23    {
24    Resend packet;
25    Drop_count=Drop_count+1;
26    }
27    If(Forward_count/Drop_count> threshold)
28    Initial( );
29     Start( );
30    }
31
32    Else
33    {Send RREQ again;}
34    }
```

Fig 2: Algorithm for DAODV

The flow chart of our proposed mechanism is described as in Fig3. below

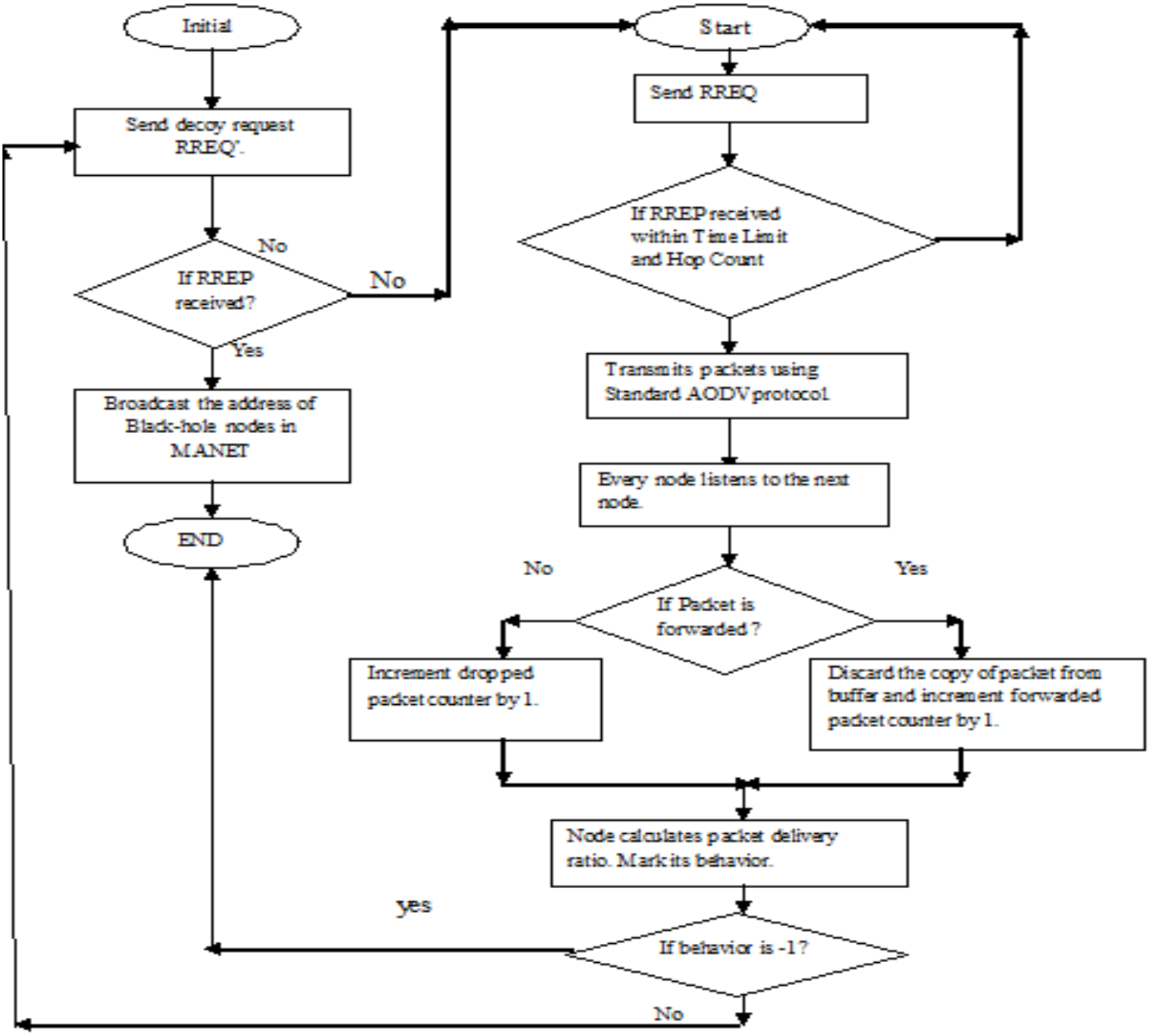

Fig 3: Flow Chart of DAODV

CONCLUSION

In this paper we have proposed an algorithm and named it DAODV. This algorithm detects Balck-hole MANETs. This algorithm works in proactive as well as reactive manner. Our proposed mechanism is capable of handling Black-Holes which are already existing and those which occur during transmission. It works equally fine for cooperative Black-holes, where many other algorithm fails. Although there will be overhead of running initial method and maintaining log at the intermediate nodes for transmitting and dropping packets. It is better from other detection and avoidance algorithm in the sense that most of them use complex heavy calculations of encryption and decryption. But this algorithm will not be able to handle cooperative Black-Holes after the initial method has completed.

In the future work we will enhance DAODV for the above said problem to resist cooperate Black –Hole attack at any stage and we will also try to verify and validate this algorithm on a standard simulator.

REFERENCES

[1] XIAOGENG ZHAO,''An Adaptive Approach for Optimized Opportunistic Routing Over Delay Tolerant Mobile Ad Hoc Networks'', Computer Science Department, December 2007

[2] GORANTALA K., "Routing Protocol in Mobile Ad-hoc Networks," Technical report Department of Computer Science from UMEA University, June **2006**.

[3] JOHNSON D., D,MALTZ D.. "Dynamic source routing in ad hoc wireless networks". Editors T. Imielinski and H. Korth, Kluwer Academic Publisher, 1996.

[4] C. E. Perkins and E. M. Royer. "Ad hoc on-demand distance vector routing". Proc. of *IEEE* Workshop on Mobile Computing Systems and Applications (WMCSA), 1999.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of MOBICOM, Boston MA USA, pp 255-265 **2000**.

[6] RESNICK P., ZECKHAUSER R.: 'Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system', in BAYE M. (ED.): (Elsevier Press, 2000, 1st edn.), 'Advances in applied microeconomics: the economics of the internet and E-commerce', pp. 127–157

[7] BUCHEGGER S., BOUDEC J.L.: 'A robust reputation system for p2p and mobile ad-hoc networks'. Proc. Int. Workshop on the Economics of Peer-to-Peer Systems, Cambridge, MA, USA, June 2004, pp. 119–123

[8] JØSANG A., ISMAIL R.: 'The beta reputation system'. Proc. 15th Bled Electronic Commerce Conf., Bled, Slovenia, June 2002, pp. 1–14

[9] SABATER J., SIERRA C.: 'Regret: reputation in gregarious societies'. Proc. Int. Conf. Autonomous Agents, Montreal,Canada, 2002, pp. 194–195

[10] SRIVATSA M., LIU L.: 'Securing decentralized reputation management using trustguard', J. Parallel Distrib. Comput., 2006, 66, (9), pp. 1217–1232

[11] SELC¸UK A.A., UZUN E., PARIENTE M.R.: 'A reputation-based trust management system for P2P networks'. Proc. Int.Symp. on Cluster Computing and the Grid, Chicago, USA, April 2004, pp. 251–258

[12] XIONG L., LIU L.: 'PeerTrust: Supporting reputation-based trust in peer-to-peer communities', IEEE Trans. Knowl. Data Eng., 2004, 16, (7), pp. 843–857

[13] SONG S., HWANG K., ZHOU R., KWOK Y.-K.: 'Trusted P2P transactions with fuzzy reputation aggregation', IEEE Internet Comput., 2005, 9, (6), pp. 24–34