ISSN No. 0976-5697

Volume 3, No. 2, March-April 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Solution of Cooperative Black Hole Attack Problem in Mobile Ad-Hoc Network

Priyanka Gupta*
Dept. Of Computer Science & Electronics
AIM & ACT Banasthali University, Tonk,
Rajasthan, India
priyanka.gupta23pg@gmail.com

Kamna Gauri
Dept. Of Computer Science & Electronics
AIM & ACT Banasthali University, Tonk,
Rajasthan, India
kamna.gk@gmail.com

Abstract: Mobile Ad-hoc network is particularly vulnerable due to it's fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. It can be established extremely flexibly without any fixed base station in battlefields, military applications, and other emergency and disaster situation. All signals go through bandwidth-constrained wireless links in an ad-hoc network, which makes it more prone to physical security threats than fixed networks. Wireless networks are not secure due to the attacks of malicious nodes. In this paper we are analyzing and improving security in AODV routing protocol in presence of malicious faults by discovering safe route and avoiding these nodes. We also present a technique for ensuring security from coordinated attack that is caused by multiple black holes acting in a group. In this paper we also analyze the impacts of gray holes (nodes which are between good nodes and black hole nodes) on ad-hoc network routing performance.

Keywords: Mobile Ad-hoc network, routing, AODV, black hole, gray hole

I. INTRODUCTION

Ad hoc networks provide a possibility of creating a network in situations where creating the infrastructure would be impossible or more expensive. Mobile nodes in ad-hoc network communicate to each other without using any fixed structure (access points) [1].In these type of network nodes can leave or enter in the network at any point of time because of dynamic topology.

There are currently three main routing protocols divisions for ad hoc networks [2]

a. Proactive routing protocol
b. Reactive routing protocol
c. Hybrid routing protocol

A. ***Proactive routing protocols*** are table driven. Here information is exchanged periodically as in Destination sequenced distance vector routing (DSDV).

B. ***Reactive protocols*** are on demand basis. Here node exchanges the information to keep track of topology when some source node wants to route the information to destination node as in Dynamic source routing (DSR) and Ad-hoc on demand distance vector (AODV).

C. ***Hybrid Protocols*** use both approaches of reactive and proactive routing as in Zone reactive routing (ZRP).

In the absence of infrastructure there arise many security issues due to dynamic topology and malicious node present in wireless network [3]. Black hole attack is one of the severe problems in AODV routing. It is source-initiated routing .In this when source node wants to send data to destination node. Then intermediate nodes are responsible for find the fresh path for data transfer between source and destination. In this each mobile node keeps the next hop node information in it's routing table. Malicious node does not follow this process. They inform falsely to source node that path is available from source to destination. Source node sends data assuming that path as true through malicious node. Malicious node (refusal of service) blocks that data rather than forwarding it to destination [4]. Mobile nodes in the network always try to find the route avoiding and preventing the effect of black hole. Deng, Li, and Agrawal [5] assume the black Hole nodes do not work in a group and gave a solution to identify a single black hole.

However, the proposed technique cannot be applied to identifying a cooperative black hole attack involving multiple nodes. But here in this paper we present a technique to identify multiple black hole nodes working in a group [6]. With the use of Data routing information table (DRI) this technique is used with slightly modified AODV routing protocol.

In this paper section 2 describes cooperative black hole attack problem ,in section 3 we present a solution to avoid and identify multiple black hole nodes in a network, in section 4 describes the effect of Gray holes and techniques to find them and in section 5 we conclude and discuss future work.

II. COOPERATIVE BLACK HOLE PROBLEM

A. Black hole:

A node in the network having these properties is called black hole it show itself as having valid root to destination while root does not exists actually and black hole consumes the intercepted packets.

B. Gray holes:

A special case of the black hole attack called gray hole attack is described in ([6], [3]). In this case some data is discarded and some data is transferred in forward direction (e.g. routing packets). Detection of gray hole is difficult because nodes stop data transferring not only due to it's malicious nature but also overburden and selfish nature. Selfish nature is the nature in which node does not want to

spend it's battery, CPU utilization and bandwidth because of not having interest to forward it [7]. Due to GRAY holes processing data is transferred to black hole nodes and overall performance of data packet in routing network is reduced.

C. Cooperative black hole attack:

In AODV protocol Source node A wants to send data to destination B.A broadcasts route request (RREQ) message to it' s neighboring nodes. Neighboring nodes update their data routing table for that A node and check if it has a fresh route to destination. If it is neither destination nor having fresh route then intermediate node updates RREQ message and floods in the network until it reaches to D or any other intermediate node having fresh route to D.

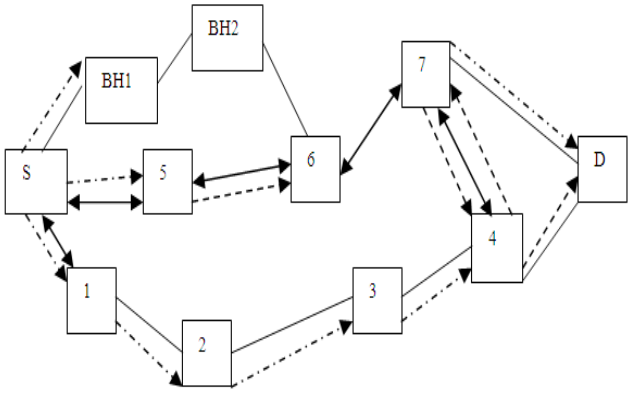

Figure 1. Flooding of RREQ message in network

Then destination node D or the intermediate node with a fresh route to destination D, initiates a route response (RREP) in the reverse direction. Node S sends the data to neighboring node which responded first and discards the other responses. This works well in the absence of malicious node.

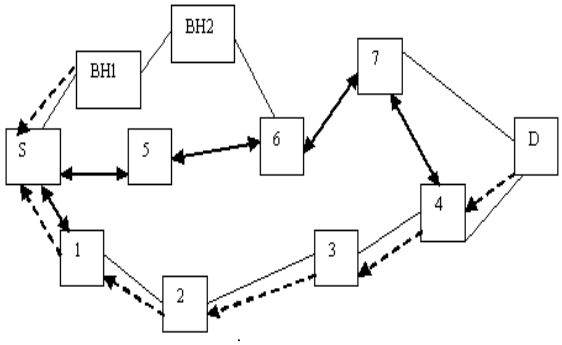

Figure 2. Propagation of RREP message

Researchers have proposed solutions to identify and eliminate a single black hole node[5].In the case of multiple black holes working in the group, first black hole node BH1 refers to it's group mate BH2 as next hop's sends further request(FRq) to BH2 through a alternative route other than BH1[5]. Now S asks BH2 if it has a route to BH1 and to D because BH2 is working in a group with BH1, BH2 will give the positive response further Reply (FRp) in both cases. Now according to [5]node S sends data via that route assuming that route S-BH1-BH2 is safe while data is not passed to destination D**.**

III. SOLUTION

In this technique we present a solution for identifying group of multiple black hole nodes with slightly modified AODV protocol by including Data routing information (DRI) and Cross checking and for preventing this attack an algorithm is also presented here.

A. Solution to identify multiple black hole attack:

a) Data Routing Information:

Each node maintains a data routing information table of 2 additional bits. Here 1 stands for true and 0 for false. First bit 'FROM' stands for information on routing packet from the node and second bit 'THROUGH' stands for information on routing packet through node .Database maintained by node 6 is as below-

Entry 1 0 for node 3 implies that node 6 has routed data from node 3 but not through node 3.Entry 11 for node 5 implies that node 6 has successfully routed data from and through node 5 and 00 entry for malicious node BH2 implies that data cannot be routed from or through this node.

Node Number	Data Routing Information	
	From	Through
3	1	0
5	1	1
BH2	0	0
7	1	1

Figure 3. Data Routing Information for node 6

b) Cross Checking:

Normally we rely on re liable nodes to transfer data packets. In modified AODV protocol our proposed technique is described as in example in this network –

When node BH1 responds to source node S with RREP message then it provides the information about it's next node hop BH2and DRI (if BH1 has routed information to BH2).Here black hole node BH1 lies about the path by sending DRI value 0 1 .Upon receiving this DRI value from BH1 source node S checks it's own DRI table to see that whether BH1 is reliable node. Since S has never sent any data to BH1 before, BH1 node is not reliable to node S. Then S sends FRq to node BH2 via a alternative path S-5-6-BH2 and asks BH2 has routed data from BH1, who is BH2's next hop, and if BH2 has routed data packets through BH2's next hop. Since BH2 is collaborating with node BH1.It replies positively to all the three requests and gives node 7 as next hop randomly. When node S contacts to node 7 via alternative path S-5-6-7 to cross check claim of node BH2, Node 7 responds negatively. Since node 7 has neither route to node BH2 nor received data packets from node BH2, DRI value corresponding to node BH2 is 00. Based on this information source node S infers that BH2 is black hole node. If node BH1

was assumed `to route data packet through node BH2, It should have validated the node before sending it. Node BH2 is invalidated through node 7, BH1 is incorporated with node BH2.Both node BH1 and BH2 are marked as black hole nodes. This information is propagated through network leading to lists as black holes. Then further S discards any further responses from BH1 or BH2 and looks for alternative valid route to D. Purpose of crosschecking the intermediate nodes is to secure a network from multiple black hole nodes. Cost of crosschecking nodes can be minimized by allowing nodes to share sharing the trusted nodes list with each other.

B. Solution to prevent multiple black hole attack:

a. Algorithm to prevent cooperative black hole attack in MANETs:

Notations:
SN: Source Node
IN: Intermediate Node
DN: Destination Node
NHN: Next Hop Node
FRq: Further Request
FRp: Further Reply
Reliable Node: The node through which the SN has routed data
DRI: Data Routing Information
ID: Identity of the node

b. Description of algorithm:

Source node S broadcasts RREQ message to discover a secure route to destination.IN generates RREP to provide it's NHN and it's DRI entry for NHN. After receiving RREP message from IN SN checks it's DRI entry to know whether in is reliable node. If SN has used IN to route the data earlier then IN is reliable.SN initiates sending data through IN. Else IN is unreliable and sends FRq Message to know the identity of IN and asks NHN(1)if IN has sent data through NHN(2)current NHN's next hop to destination(3)if NHN has sent data through it 's next hop.NHN responds FRp message(1)DRI value for IN (2)Current NHN's next hop(3)DRI value for next hop node .Based on this FRp message SN determines that NHN is reliable node or not. If NHN is reliable then SN will check if IN is reliable or not. If first bit is 0 in DRI (NHN has sent data from IN) and second bit is 1 in DRI (IN has sent data through NHN) then IN is black hole. If IN is not black hole and NHN is reliable then path is secure then SN initiates sending data via IN. If IN is black hole then SN identifies all nodes involved with it. Then SN ignores all RREP received from black holes and broadcasts the list of black holes. If NHN is an unreliable node, source node treats current NHN as IN and sends FRq to the updated IN's next hop node and repeated process.

IV. CONCLUSION AND FUTURE WORK

Here in this paper proposed solution has been presented for AODV routing protocol. This can be applied for identifying the black hole acting in group with each other, finding out path from source to destination avoiding these nodes and reducing the impact of gray hole nodes which switch from good nodes to black hole nodes) and techniques for their identification.

As future work, we can try to simulations to analyze performance of this proposed solution based on different factors as impacts of false positives on routing network throughput, response time. We can find those techniques to improve response time so that we can measure this time in network because there may be time wastage in finding whether there is malicious node in the fresh route or not in AODV protocol.

V. REFERENCES

[1]. S. Corson and J. Macker, "RFC 2501 Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," 1999.

[2]. Elizabeth M. Royer, and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, April 1999.

[3]. B. Wu et al., "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer,vol. 17, 200 6.

[4]. Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black hole Attack in Mobile Ad Hoc Networks" Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, APRIL 2004, pp. 96-97.

[5]. H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[6]. Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, 2002.

[7]. Banerjee Sukla," Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks," Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.