A MODIFIED HYBRID PROTOCOL(ZRP) USED FOR DETECTION AND REMOVAL OF BLACK HOLE NODE IN MANET

[1] MR. RAJDIPSINH D. VAGHELA, [2] PROF. NISHANT J. GOSWAMI

[1]M.E. [Computer Engineering] Student, Department Of Computer Engineering, Marwadi Education Foundation Group Of Institutes, Rajkot, Gujarat
[2] Asst.Professor, Department Of Computer Engineering, Marwadi Education Foundation Group Of Institutes, Rajkot, Gujarat

rajdipsinhvaghela90@gmail.com, nishant.j.goswami@gmail.com

ABSTRACT: *A Wireless ad-hoc network is a temporary network set up by wireless mobile Computers moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they co-operate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols. However,due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all Datapackets in the network.In Black hole attack malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This Paper Focus on to detect black hole node and remove it. The detection techniques which make use of proactive routing protocol have better packet delivery ratio and correct detection probability, but have higher overheads. The detection techniques which make use of reactive routing protocols have low overheads, but have high packet loss problem. Therefore, Using a hybrid detection technique which combines the advantages of both reactive and proactive routing Protocol to detect the black hole node.*

Keywords— Black hole, Zone routing protocol(ZRP),Packet Delivery Ratio, Throughput .

I: INTRODUCTION

Hybrid protocols exploit the strengths of both reactive and proactive protocols, and combine them together to get better results. The network is divided into zones, and use different protocols in two different zones i.e. one protocol is used within zone, and the other protocol is used between them. Zone Routing Protocol (ZRP) is the example of Hybrid Routing Protocol. ZRP uses proactive mechanism for route establishment within the nodes neighborhood, and for communication amongst the neighborhood it takes the advantage of reactive protocols. These local neighborhoods are known as zones, and the protocol is named for the same reason as zone routing protocol. Each zone can have different size and each node may be within multiple overlapping zones. The size of zone is given by radius of length P, where P is number of hops to the perimeter of the zone. Fig. 1.1, where the routing zone of S includes the nodes A–I, but not K. In the figure the radius is marked as a circle around the node. It should however be noted that the zone is defined in hops, not as a physical distance. The nodes of a zone are divided into peripheral nodes and interior nodes. Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius r. The nodes whose minimum distance is less than r are interior nodes[1].

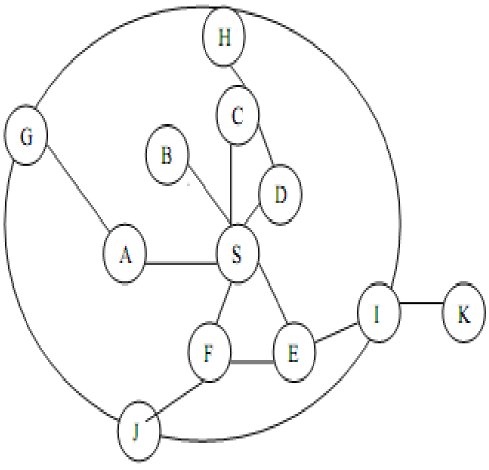

Figure 1.1: Zone routing protocol (radius r = 2)[1]

In Fig. 1.1, the nodes A–F are interior nodes; the nodes G–J are peripheral nodes and the node K is outside the routing one. Note that node H can be reached by two paths, one with length 2 and one with length 3 hops. The node is however within the zone, since the shortest path is less than or equal to the zone radius. ZRP refers to the locally proactive routing component as the IntrA-zone Routing Protocol (IARP). The globally reactive routing component is named IntEr-zone Routing Protocol

(IERP). IERP and IARP are not specific routing protocols. Instead, IARP is a family of limited-depth, proactive link-state routing protocols. IARP maintains routing information for nodes that are within the routing zone of the node. Correspondingly, IERP is a family of reactive routing protocols that offer enhanced route discovery and route maintenance services based on local connectivity monitored by IARP. Instead of broadcasting packets, ZRP uses a concept called bordercasting. Bordercasting utilizes the topology information provided by IARP to direct query request to the border of the zone. The bordercast packet delivery service is provided by the Bordercast Resolution Protocol (BRP).

a) Route Discovery

A node that has a packet to send first checks whether the destination is within its local zone using information provided by IARP. In that case, the packet can be routed proactively. Reactive routing is used if the destination is outside the zone. The reactive routing process is divided into two phases:
1. The route request phase
2 The route reply phase.
In the route request, the source sends a route request packet to its peripheral nodes using BRP. If the receiver of a route request packet knows the destination, it responds by sending a route reply back to the source. Otherwise, it continues the process by bordercasting the packet.In this way,the route request spreads throughout the network.

b) Route Maintenance

Route maintenance is especially important in ad-hoc networks, where links are broken and established as nodes move relatively to each other with limited radio coverage. In purely reactive routing protocols, routes containing broken links fail and a new route discovery or route repair must be performed. Until the new route is available, packets are dropped or delayed. In ZRP, the knowledge of the local topology can be used for route maintenance. Link failures and sub-optimal route segments within one zone can be by passed. Incoming packets can be directed around the broken link through an active multi-hop path. Similarly, the topology can be used to shorten routes, for example, when two nodes have moved within each others radio coverage. For source-routed packets, a relaying node can determine the closest route to the destination that is also a neighbor[23].

II: Introduction about Black Hole

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address. The method how malicious node fits in the data routes varies. how black hole problem arises:

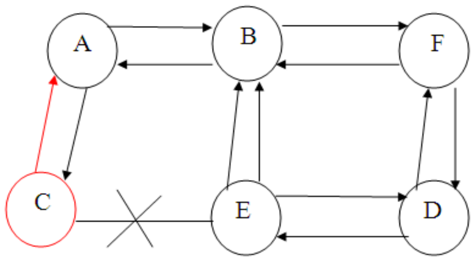

Figure 2.1: Single Black hole attack[7]

Here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost.

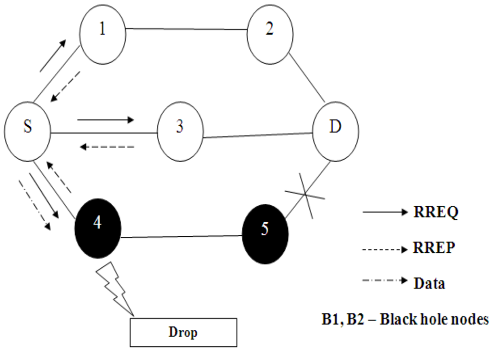

Figure 2.2: Co-operative Black hole attack[10]

III: Proposed Work and Algorithm

Majority of black hole detection methods are uses an AODV protocol, and proactive or reactive protcol so there is hybrid protocol ZRP is used to detect the blackhole node in MANET. Proactive and reactive has such problem like packet delivery ratio and routing overhead problem so there is taking advantages of combine protocol using hybrid ZRP protocol to detect the black hole node.

The probabilistic algorithm is like:
Here one assumption is taken. All interior node and peripheral node is trusted node.

Step 1- Finding the all neighbour node from the source node.

Step 2- Source node get the routing table information about all neighbour node.

Step 3- Choose one of the trusted node.

Step 4- Using neighbour (trusted) node sending (routing request) RREQ (s_addr,d_addr) to peripheral nodes.

Step 5- Getting RREP (s_addr.n_ip) from the nodes. Check if it is any intermediate node between interior node or peripheral node working as peripheral node it is a black hole broadcast the message and alert to other nodes.

IV: SIMULATION AND RESULTS

Protocol	ZRP
Simulation Time	500 sec
Simulation Area (m * m)	500 * 500
Number of nodes	20
Number of black hole node	1
Mobility(m/s)	0-250
Packet size	512 Bytes
Performence parameter	Average Network Delay, Network Throughput, Total Dropped Packets, Packet Delivery Ratio.

Table 1: Simulation Parameters

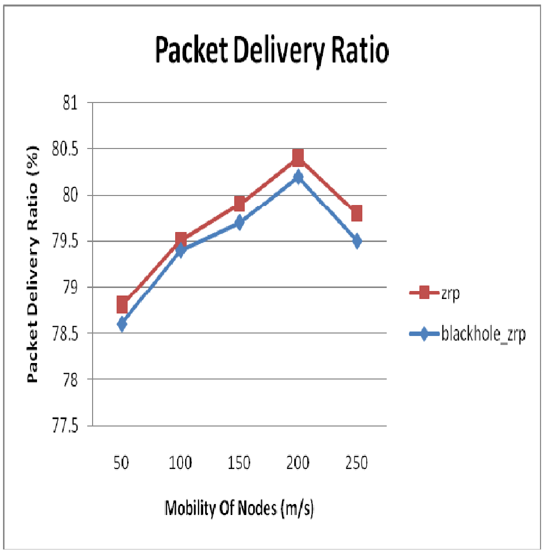

Figure 4.1 Packet Delivery Ratio vs mobility of nodes

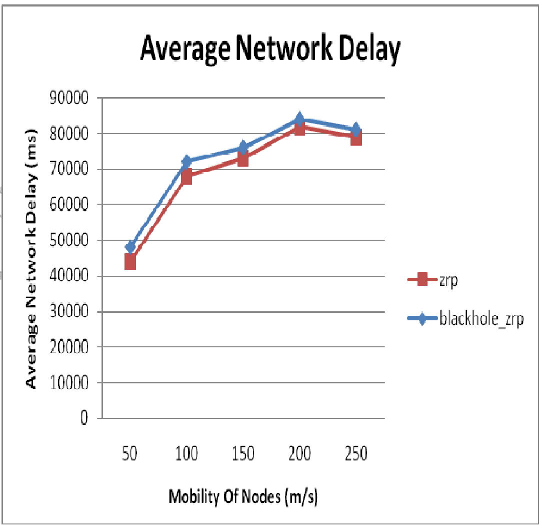

Figure 4.2 Average Network Delay vs mobility of nodes

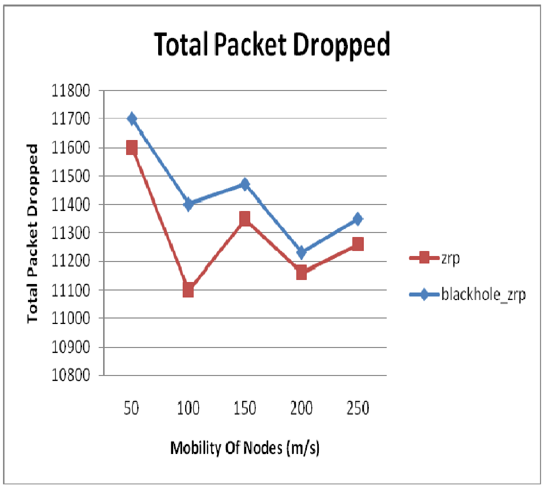

Figure 4.3 Total Packet Dropped vs mobility of nodes

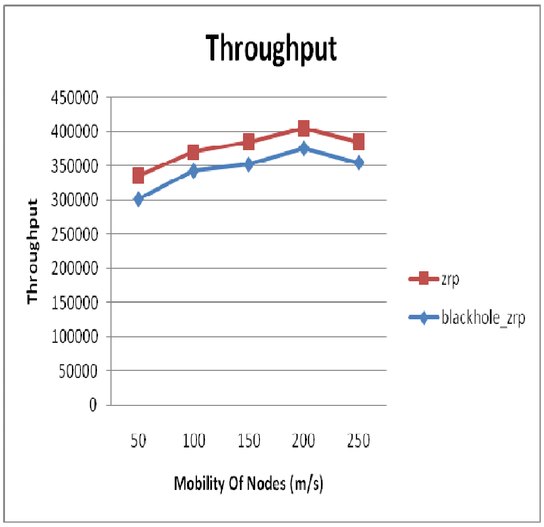

Figure 4.4 Throughput vs mobility of nodes

V: CONCLUSION AND FUTURE SCOPE

A Black Hole attack is one of the serious security problems in MANETs. Although many solutions have been proposed. This proposed technique is hybrid in nature and based on the concept of ZRP. It provides a solution for identification of Black Hole Attack and removal of Black Hole from the network. The proposed technique gives a better solution towards Black Hole Attack within the network. Black Hole attack with four different scenarios with respect to the performance parameters of Average Network Delay, Network Throughput, Total Dropped Packets and Packet Delivery Ratio had been simulated. There is a boundary overlapping is major issue in ZRP protocol. There is a need to analyze Black Hole attack in other MANETs routing protocols such as TORA and GRP. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network.

REFRENCES

[1] Dilli Ravilla, V.Sumalatha, Dr Chandra Shekar Reddy Putta," Hybrid routing protocols for ad hoc wireless networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.4, December 2011.

[2] Akanksha Saini, Harish Kumar "Effect Of Black Hole Attack On AODV Routing Protocol In MANET", IJCST Vol. 1, Issue 2, December 2010.

[3] Rashid Hafeez Khokhar, Md A sringadi&Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks" International Journal of Computer Science and Security, volume 2 issue 3 pp.18.

[4] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei"A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", WIRELESS/MOBILE NETWORK SECURITY, Springer 2006.

[5] RajenderNath, Pankaj Kumar Sehgal, Atul Kumar Sethi, "Effect of Routing Misbehavior in Mobile Ad Hoc Network" ISBN 978-1-4244-4791-6/10,IEEE 2010

[6] Elizabeth M. Royer, C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE 2009 .

[7] Himani Yadav, Rakesh Kumar, "A Review on Black Hole Attack in MANETs", International Journal of Engineering Research and Applications (IJERA) ,Vol. 2, Issue 3, May-Jun 2012, pp.1126-1131

[8]Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile adhoc networks", Tseng etal. Human-centric Computing and Information Sciences 2011.

[9] Djenouri D, Badache N, "Struggling Against Selfishness and Black Hole Attacks in MANETs", Wireless Communications & Mobile Computing Vol.8, Issue 6, pp 689-704, August 2008.

[10]Tamilselvan L, Sankaranarayanan V, "Prevention of Black hole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

.