Improving ZRP Protocol against Blackhole Attack

[1]Chaitas Shah, [2]Prof. Manoj Patel

[1]M.E.Scholar, [2]Professor
Alpha College of Engineering and Technology, Gandhinagar, India
[1]chaitashah@gmail.com

Abstract - **In Mobile Ad-Hoc Network different types of routing protocols have been discovered. These protocols can be classified into three main categories reactive (on-demand) Ad-hoc On Demand Routing Protocol (AODV), proactive (table-driven) OLSR and hybrid routing protocol Zone Routing protocol (ZRP). Thus routing protocols for Mobile Ad-Hoc Network have to face the challenge of frequently low transmission power, asymmetric links and changing topology. Both proactive and reactive routing protocols prove to be inefficient certain circumstances. The hybrid protocol Zone Routing Protocol (ZRP) combines the advantages of the proactive and reactive approaches and it maintains an updated topological map of a zone centered on each node in the network. Within the zone, routes are immediately available for transmission of packets. Thus for destinations outside the zone, Zone Routing Protocol employs a route discovery procedure, which benefits from the local routing information of the zones. However, due to security vulnerabilities of routing protocols and wireless networks remains unprotected to attacks of the different malicious nodes. One of attacks is the Black hole Attack against network integrity absorbing all data packets in the network. The detection techniques that make use of proactive routing protocol they have better packet delivery ratio and correct detection probability but they have high overheads. The detection techniques which make use of reactive routing protocols have low overheads, but they have high packet loss problem. Therefore in this paper using a hybrid detection technique which combines the advantages of both reactive and proactive routing protocol to detect the black hole node and removing it.**

Key Words - **Ad-hoc On Demand Routing Protocol (AODV), Optimized Link State Routing Protocol (OLSR), Black hole, Zone Routing protocol(ZRP) , Routing Protocols, Proactive, Reactive**

I. INTRODUCTION

By Wireless networks in today's world are gaining popularity to its peak , as users want wireless connectivity irrespective of their geographic position. Also, there is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANETs). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It is an analogy to the black hole in the universe in which things disappear. Here, the node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. Mobile Ad-hoc Networks (MANETs) must have a secure way for transmission and communication which is quite challenging and vital issue. Thus, in order to provide secure communication and transmission, the researcher worked specifically on the security issues in MANETs and also many secure routing protocols and security measures within the networks were proposed. Thus, previously the work is done on security issues in MANETs were based on reactive routing protocol like Ad-Hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Different kinds of attacks were studied according to it their effects were elaborated by stating how these attacks disrupt the performance of MANETs. Thus scope of this paper is to develop a technique to identify Black Hole Attack and then removal of Black Hole Attack in ZRP in Mobile Ad-hoc Networks (MANETs).

Problem Statement

Previously the work is done on security issues i.e. attack (Black Hole attack) involved in MANET were based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV) and also Proactive routing protocol. Black Hole attack is studied under both the reactive routing protocol and also Proactive routing protocol and its effects are elaborated by stating how this attack disrupt the performance of routing protocols in MANET. Thus very little attention has been given to the fact to study the impact of Black Hole attack in Zone Routing protocol (ZRP) a hybrid protocol having advantages of both proactive and reactive protocol, the vulnerability of this protocol against the attacks. There is a need to address the protocol as well as the impacts of the attacks on the ZRP by reducing the effects to minimum and increasing the performance of the protocol in MANET.

Objective

Analyzing the effects of black hole attack with respect to the performance parameters of Average Network Delay, Network Throughput, Total Dropped Packets and Packet Delivery Ratioand also proposing counter measures by modifying ZRP for Black Hole attack which detects the malicious node and prevents the attack and simulating the effect using NS-2.

II. LITERATURE REVIEW

Zone Routing Protocol(ZRP)

The Zone Routing Protocol [1], as its name implies, is based on the concept of zones. A routing zone is defined for each node separately, and the zones of neighboring nodes overlap. The routing zone has a radius r expressed in hops. The zone thus includes the nodes, whose distance from the node in question is at most r hops. An example routing zone is shown in Fig. 1, where the routing zone of S includes the nodes A–I, but not K. In the illustrations, the radius is marked as a circle around the node in question. 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.

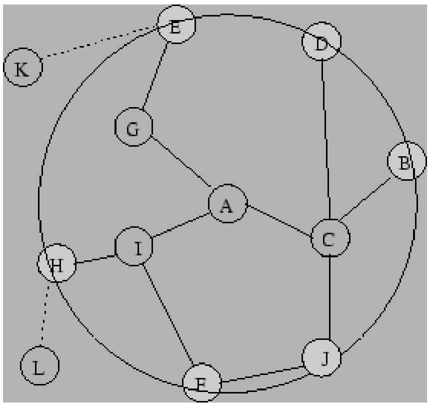

Fig.1 Zone Routing Protocol

Blackhole

In black hole attack [2], [3] 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 [4]. 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 [5].

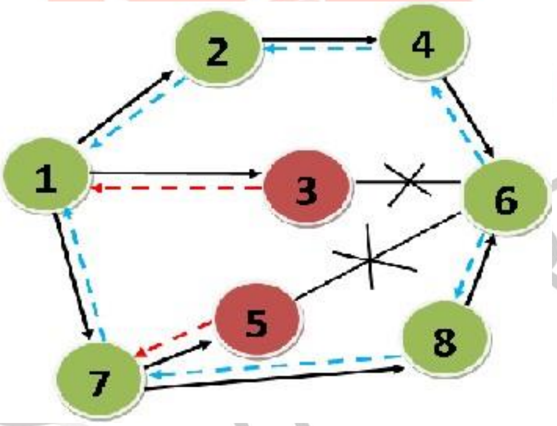

Fig.2 Blackhole Attack

Black hole Attacks are classified into two categories

1. Single Black Hole Attack [6], [7]
   In Single Black Hole Attack only one node acts as malicious node within a zone. It is also known as Black Hole Attack with single malicious node. Collaborative Black Hole Attack [7], [8] In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.
2. Collaborative Black Hole Attack [7], [8]
   In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

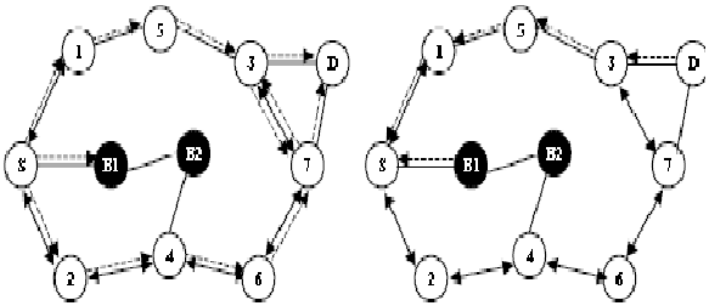

Fig.3 Collaborative Blackhole Attack

Techniques of Blackhole Detection

There is lot of work done in MANET for detection of Black Hole attacks some of existing techniques of it for different routing protocols are as follows:

Table 1Techniques of Detecting Blackhole Detection

Schemes	Routing protocol	Simulator	Results	Defects
Neighborhood based And Routing Recovery [9]	AODV	NS-2	The probability of one attacker can be detected is 93%	Failed when attackers cooperate to forge the fake reply packets
Random Two hop ACK and Bayesian Detection Scheme [10]	DSR	GloMoSimbased	The true positive rate can achieve 100% when existing 2 witness	The proposed scheme is not efficient when k equals to 3, reducing the true positives
DPRAODV [11]	AODV	NS-2	The PDR is improved by 80 85% than AODV when under blackhole attack	A little bit higher routing overhead and end-to-end delay than AODV
IDS based on ABM [12]	MAODV	NS-2	The packet loss rate can be decreased to 11.28% and 14.76%	Cooperative isolation the malicious node, but failed at collaborative blackhole attacks
Prevention of Black Hole Attack in Mobile Ad-Hoc Network[13]	AODV	NS-2	Provides better Additional Security	Decreased PDR and end to end Delay
Bluff-Probe Based Black Hole Node Detection and prevention[14]	ZRP	Qualnet	Provides low overhead and better performance	Used only for light weight network
Enhancing Security of Zone-Based Routing Protocol using Trust[15]	ZRP	NS-2	Improves packet Delivery Ratio	Cost of this improvement increased in end to end and routing overhead.

III. PROPOSED WORK

Proposed Algorithm Flowchart

The Flow Chart of the proposed system:

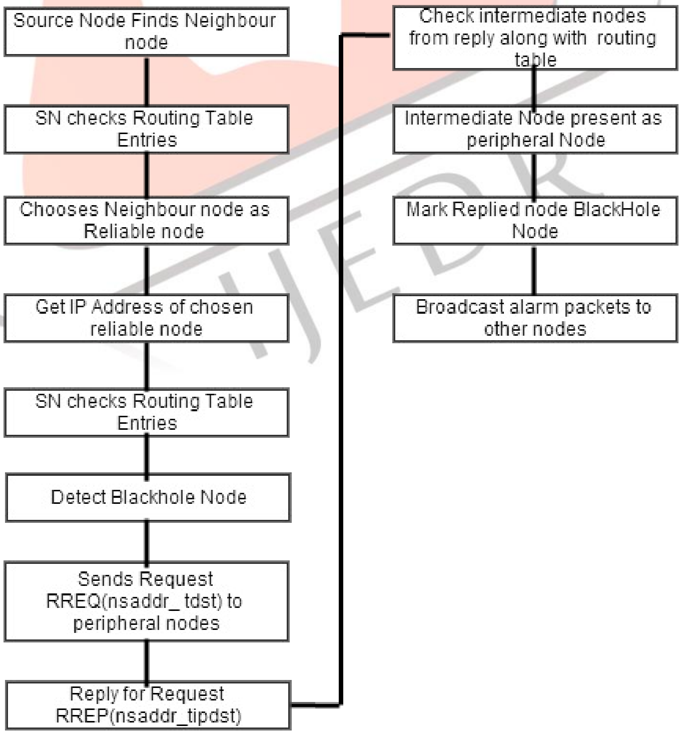
Source Node Finds Neighbour node
SN checks Routing Table Entries
Chooses Neighbour node as Reliable node
Get IP Address of chosen reliable node
SN checks Routing Table Entries
Detect Blackhole Node
Sends Request RREQ(nsaddr_ tdst) to peripheral nodes
Reply for Request RREP(nsaddr_tipdst)
Check intermediate nodes from reply along with routing table
Intermediate Node present as peripheral Node
Mark Replied node BlackHole Node
Broadcast alarm packets to other nodes

Fig. 4 Flow Chart of Proposed Algorithm

The algorithm for Modified-Zone Routing Protocol is as follows:

Step 1. Find neighbor node along with a source node of the protocol.
Step 2. Source node will check routing table entries for these particular neighboring nodes in the protocol.
Step 3. Choose a neighbor node as a reliable node and get IP address of selected reliable node.

Step 4. Now to detect Black Hole node it will send request to outlying nodes.
RREQ (snaddr_t dst) IERP/BRP for reliable node's IP.
Step 5. Get reply for request from the outlying nodes RREP(snaddr_t ipdst)IERP/BRP.
Step 6. Check intermediate nodes which replied along with source's routing table.
Step 7. If any intermediate node is present as outlying node in source's routing table then mark that node which replied as Black Hole node and broadcast alarm packet message about that node and alert the other nodes to update their routing tables so as to prevent Black Hole attack.

Functional Description

Now this algorithm code for detecting and preventing black hole node has been added in Zone Routing Protocol(ZRP). Here local communication takes place at that time when the source node sends find neighbor packet to identify its neighbors along the network. Then it marks any neighbor node as reliable node. Now the source node again sends the request packet to outlying nodes and IERP with its reliable node's address as a destination node with whom it wants to communicate in the network. After getting replies, it will check whether the reply is from interzone or not. If the reply is from interzone then it will check for the intermediate node's address from where it got the reply from the node. If the intermediate node address is same as its outlying node's address in its routing table. Then it is sure that the relied node is outside the zone i.e. IERP but actual node is present in its neighbor which means within same zone. So replied sender is definitely a Black Hole node and thus black hole node is detected. Now broadcast the IP of Black Hole node using alarm packets to all other nodes in the network so as to discard it from routing table entries of the nodes.

IV. CONCLUSION AND FUTURE WORK

A Black Hole attack is one of the serious security problems in MANETs. Thus many solutions have been proposed. The proposed technique is hybrid in nature and based on the concept of ZRP. This provides a solution for identification of Black Hole Attack and removal of Black Hole from the network. This proposed technique gives a better solution towards Black Hole Attack within the network. The 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 has been simulated. We can see there is a boundary overlapping is major issue in ZRP protocol. Also, there is a need to analyze Black Hole attack in other MANETs routing protocols such as TORA, GRP and FSR. Also other types of attacks such as Wormhole, Jellyfish, Sybil, Byzantine attacks are needed to be studied in comparison with Black Hole attack. They can also be categorized on the basis of how much they affect the performance of the network.

REFERENCES

[1] Nicklas Beijar, Networking Laboratory, Helsinki University of Technology "Zone Routing Protocol (ZRP)"

[2] E. A .Mary Anita and V. Vasudevan, "Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Adhoc networks using Certificate Chaining", International Journal of Computer Applications (0975 – 8887) Vol. 1, Issue 12, pp. 21-28, 2010.

[3] Umang S, Reddy BVR, Hoda MN, "Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption", IET Communications Vol.4, Issue17, pp2084–2094. doi: 10.1049/ietcom. 2009.

[4] K. Biswas and Md. Liaqat Ali, "Security Threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology Sweden, March 2007.

[5] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006.

[6] N. Bhalaji and A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet", European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011.

[7] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 0-7695-2842-2/07, 2007.

[8] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, LNAI 4819, pp. 538–549, 2007 .

[9] Sun B, Guan Y, Chen J, Pooch UW (2003) Detecting Black-hole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[10] Djenouri D, Badache N (2008) Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing.

[11] Raj PN, Swadas PB (2009) DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET. International Journal of Computer Science.

[12] Su M-Y (2011) Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications.

[13] Santhosh Krishna B V, Mrs.Vallikannu A.L, "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism" International Journal of Scientific & Engineering Research, Vol. 1, Issue 3, ISSN 2229-5518, December-2010.

[14] Prof. Sanjeev sharma, Rajshree, Ravi Prakash Pandey, Vivek Shukla, 2009 IEEE International Advance Computing Conference (IACC 2009),March 2009 "Bluff-Probe Based Black Hole Node Detection and prevention"

[15] Yasser EIRefaie, Laila Nassef, Imane Aly Saroit, The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May 2013 Computer Networks Track "Enhancing Security of Zone-Based Routing Protocol using Trust".