International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 6, June 2016

Security Enhancement Using ZRP in MANET

[1] Neelaveni.R, [2] Sridevi.B, [3] Harini gayathri.P [4] Elamathy.E
[1],[3],[4] MNM Jain Engineering College, [2]Velammal college of Engineering and Technology

***Abstract* - - A MANET is an infrastructure less type network which consist of mobile hosts only. There is no host station; each mobile host must act as a router to forward packets. The mobile node exchange information in a network using routing protocols. MANET is used for various applications such as Military Area, Provincial Level, and Industry Sector. In a MANET, each node not only works as a host but also acts as a router. The infrastructure less structure of a MANET with changing network topology makes them exposed to various attacks such as active attack, passive attack, internal attack and external attack. Black hole is an attack in which a malevolent node transmits malicious broadcast to Route Reply (RREP), it suddenly drops the packet without forwarding it to destination. In co-operative attack, the attackers co-operate with each other and work in a group to destroy the target network. This paper aims to solve the issue of co-operative attack by using reverse tracing scheme based on zone routing protocol mechanism.**

***Keywords*— CBDA, ZRP, Reverse tracing, AODV**

I. INTRODUCTION

A network is the interconnection of nodes or computer system to exchange information. There are many types of networks such as local area network (LAN), wide area network (WAN), mobile area network (MAN). Unlike wired networks, wireless network are not secured and are susceptible to attacks by network intruders. The widespread use of mobile devices among all classes of people MANET comes into existence. MANET (Mobile ad hoc network) is local area network that builds automatic connection to the nodes in the network. Each node in the network communicates with each other nodes using radio waves. Each node has a wireless interface to communicate with each other. Main disadvantage of MANET is the security of data transmitted presence of malicious node in network may disturb the routing process. Security of MANET deals with prevention and detection of misbehaving nodes. Multiple malicious node join together to initiate a attack that cause damage to the network. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. Some of the vulnerabilities are lack of centralized management, no predefined boundary, cooperation. MANET are highly vulnerable to routing attacks such as Black hole attack, Gray hole attack, Warm hole attack, Jelly fish attack. In this paper Black hole is the major attack . DSR algorithm is the existing method, in this paper hybrid level algorithm is used to enhance the routing and efficiency of the network. Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other, however the node 2 can be used to forward packets between node 1and node 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

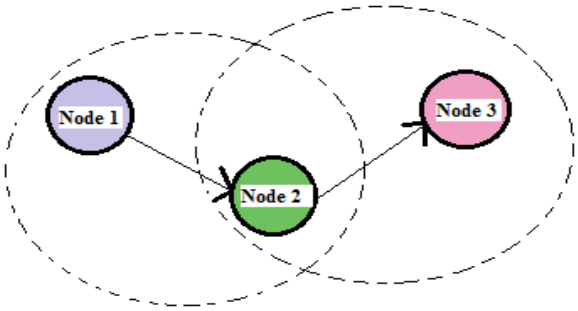


Fig.1

II. PROPOSED APPROACH

In this paper, we have proposed A Cooperative Bait Detection Approach (CBDA) to detect and prevent the malicious node in MANET(Mobile Ad hoc Network) due to Black Hole attacks. In MANET, the nodes are constantly moving and the network is dynamic in nature. Hence MANETs are unprotected to attacks by the malicious nodes. One of these attacks is Black Hole attack. In any network, the Black Holes generally refers to the places in the network when the packets are silently discarded (or dropped) without informing the source that the data will not reach the destination.

Initially packets must be delivered to the destination from the source and we need the information about the delivery path. For this, each node will be

having the details about the neighboring nodes. During the transmission of data, one or more malicious nodes may present in the network, which becomes the Black Holes where data may be discarded. The node at which the packets get discarded are known as the Black Hole nodes. When there is only one Black Hole node, it is known as Single Black Hole Attack. When more than one Black Hole node is present in the network, it is known as Collaborative Black Hole Attack and the damage to the network may be serious. Black Hole nodes or the Malicious nodes has two properties.

- At first it attracts the network traffic by advertising itself as shortest valid route to the destination node even though that route does not exist.
- Secondly the Black Hole node will discard or consume the packets, eventually causing the packet loss from the network.

For example, in figure 1, When node "S" wants to send data to destination node "D", it initiates the route discovery process. The malicious node "M" when receives the route request, it immediately sends response to source. If reply from node "M" reaches first to the source than the source node "S" ignores all other reply messages and begin to send packet via route node "M". As a result, all data packets are consumed or lost at malicious node.

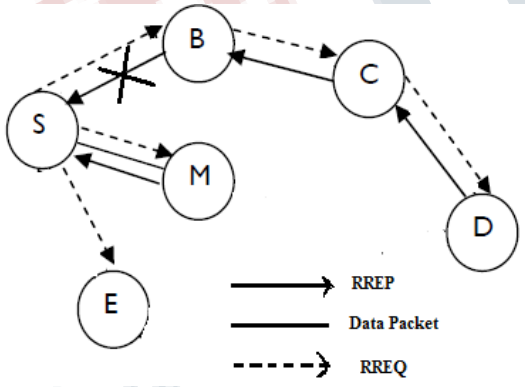


Fig.2 Black Hole Attack

There are three different detection mechanisms to detect and prevent the malicious nodes.

- ❖ Proactive detection schemes
- ❖ Reactive detection schemes
- ❖ Hybrid detection schemes.

Proactive detection scheme is a method used to prevent the attacks in its initial stage. Such that it constantly detects or monitors the neighboring nodes and the resource used for detection is constantly wasted.

Reactive detection scheme is a method used to prevent the attacks by the malicious node, only when the destination node detects the packet discard.

Hybrid detection scheme is the combination of Proactive and Reactive detection scheme.

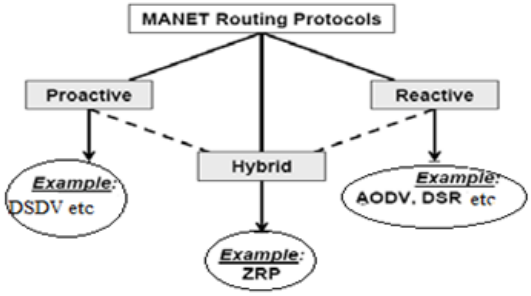


Fig. 3 Classification of Routing Protocols

Cooperative Bait Detection Schemes detects and prevents the Black Hole attacks in MANET by reverse tracing technique. It uses the Hybrid routing algorithm where the Proactive detection scheme is used in the initial step and the Reactive detection scheme at the subsequent steps. Zone Routing Protocol(ZRP) is a wireless networking routing protocol that uses both the Proactive and Reactive Routing Protocols when sending information over the network is used here to detect and prevent the malicious nodes.

III.HYBRID PROTOCOL

ZRP is a hybrid protocol used in wireless networking by combining the best properties of proactive and reactive approaches to achieve cost and energy efficiency by selecting the most efficient type of protocol. ZRP is based on the concept of zones. A zone is defined as the collection of nodes with a minimum distance which is termed as zone radius. Each node individually creates its own zone which is called as routing zone. The minimum distance from the node to the peripheral nodes will be equal to the zone radius. The routing protocol is of two types. They are as follows

***Intra zone*:** In intra zone each node maintain information on path to every other node within its zone in routing table. The table information within the zone is maintained using proactive routing algorithm which results in initial delay when communicating with the nodes. IARP allows for local route optimization through the removal of redundant nodes and the shortening of routes if a routes with fewer hops has been detected. It

provides support for unidirectional links among local nodes.

Inter Zone: IERP is used to communicate between nodes of different zones. It offers enhanced routing discovery. The IERP needs to be able to take advantage of local connectivity provided by IARP. Routing discovery is done through broadcasting that uses Broadcast Routing Protocol only transmit request nodes to peripheral nodes. BRP is used to control traffic between zones. If node has no node to a destination provided by proactive inter zone routing. BRP Is used to spread the reactive route request.

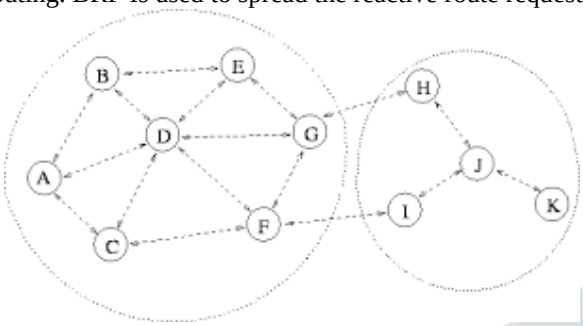


Fig. 4 Zone Routing Protocol

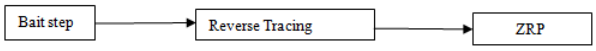
A. Network creation and routing

Wireless Sensor Networks (WSN) consists of several hundreds and thousands of nodes connected with each other for effective communication. Each Sensor Network Node have several parts such as a Radio Transceiver with an internal or external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually battery. Here we have used Network Simulator 2(NS2) for Network Creation and implementation. The network creation is based on two routing methods. They are on demand and periodic routing method. In on demand method the nodes in the network are active only when the transmission takes place or required.

Else the node are in idle or sleep mode. In the periodic method, the nodes are always active and the nodes gives notification periodically hence the power consumption is more due to constant monitoring. We use the on demand routing method. These are randomly created in the network area and are able to move from one place to other. These nodes are divided into zones and the packet transmission occurs in two ways they are inter and intra. We are using intra ZRP for network creation.

B .Working of Sensor Network

Sensor network consists of small or large nodes called sensor nodes. After when the network is created, packets are transmitted from source to the destination. The time taken for the packets to reach the destination is taken as T1 and the destination send back act to the source in time T2. Consider the time taken as Tn when the packets gets are discarded. This packet loss may occur due to link failure and security issue. The security problem arises due to various intruder attacks. In this paper we considered black hole attack, which collapses the entire network and our main goal is to prevent the network from the attack. This can be done by following steps.



C. *BAIT STEP*

In bait step, the source node selects the adjacent node which is trustworthy and it monitors the entire network. Initially the packets are transmitted from source to destination. During the transmission, the black hole node advertise itself as the shortest path to destination and attacks the network. When packet reaches the black hole node, it get discarded or it is consumed by black hole node. The baits node will get the notification from the destination that it does not receive the packets.

D. Bait Detection

Once the source node selects the adjacent node, malicious nodes are detected and prevented from participating in the routing operation, using a reverse tracing technique [9]. *Bait Setup Phase* The source node chooses the adjacent node in such a way that the address of this node is used as bait destination address to bait malicious nodes for sending a reply RREP message. The bait setup phase is activated whenever the bait RREQ′ is sent earlier for seeking the initial routing path.
The bait analysis procedure is as follows.

1. If node „n‟ had not launched a black hole attack, then after the source node „S‟ had sent out the RREQ′, the other nodes has sent the RREP shows that the malevolent node exist in reply routing as shown in Fig.4. Therefore to detect the route a reverse tracing program is initiated.

2. If only node „n‟ has sent the RREP for the RREQ′ from the source node, this indicates that there was no other malevolent node in the network except the node „n‟.

3. If both node „n‟ and the other nodes in the network have sent the RREP shows that the malevolent node is present in the route reply.

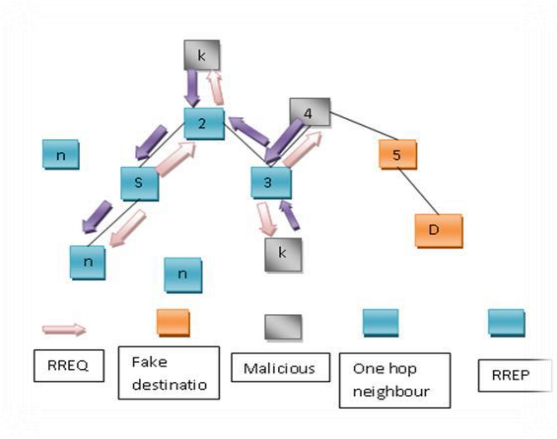


Fig 6. Bait detection

E .Reverse tracing

The reverse tracing program is used to detect the behaviours of malicious nodes through the route reply to the RREQ message. If a malicious node has received the RREQ, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the false path information and the temporarily trusted zone in the route. It should be emphasized that the CBDA is able to detect more than one malicious node simultaneously when these nodes send reply RREPS as shown in figure. The black hole node is detected by reverse tracing. To detect the malicious node, we need to know about the information of the nodes which are used in the routing path. The bait node sends a request to the destination, which consist of its IP address, MAC ID and neighbouring node address. When the request is forwarded, the address of each node in the route will be added to the routing table. When this request reaches the destination its reply back to the source which consist of default MAC ID and IP address. By comparing the routing tables of request and reply, the malicious node can be found when some of the nodes MAC ID may differ from the default ID lists.

E. Zone routing Protocol

When the malicious nodes are found they are need to be discarded, for which the zone routing protocol is used. The bait approach and reverse tracing algorithm are used within a zone is called as intra zone routing. By using ZRP second tracing is done to select the nodes, which are already detected as malicious node in reverse tracing. A data packet is sent by ZRP to delete these nodes, which causes the data packet loss. If packet destination is in the same zone as the source the proactive protocol is used which already consists of routing table used to deliver the packets immediately. If the destination lies outside the packet originating zone, the reactive protocol is used to check each successive zone in the route to find out the destination in other zones. Once the destination zone is confirmed, the proactive protocol is used to deliver the packets. Packets delivered to the nodes outside the sending zone avoid the overhead of checking routing tables along the way by using the reactive protocol to check whether each zone encountered contains the destination node

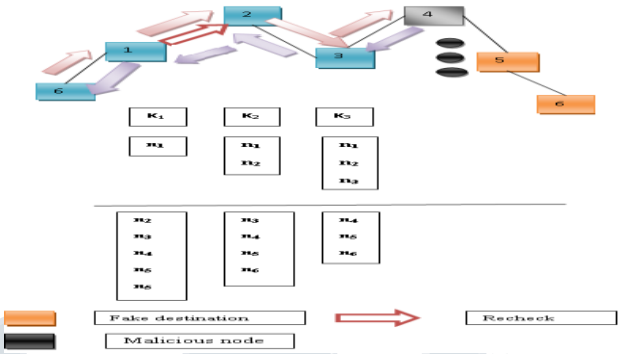


Fig.7 Reverse Tracing

IV CONCLUSIONS

Packet Delivery Ratio is defined as the ratio of the number of the packets sent by the source to the packets received at the destination. Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as: PDR= *S1÷ S2* Where, *S1 is* the sum of data packets received by the each destination and *S2 is* the sum of data packets generated by the each source. Graphs show the fraction of data packets that are successfully delivered during simulations time versus the number of nodes. Performance of the DSDV is reducing regularly while the PDR is increasing in the case of OLSR and AODV.

AODV is better among the three protocols.

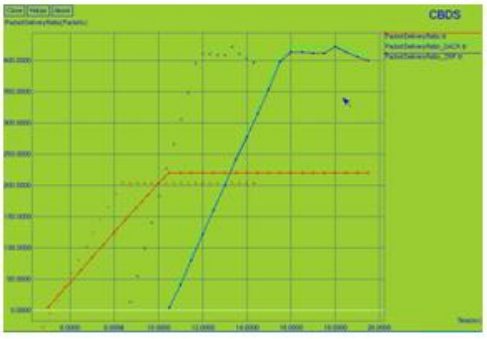


Fig. 8 Packet delivery ratio

Fig.9 Routing overhead

Routing Overhead represents the ratio of the amount of direction finding related control packet transmissions to the amount of data transmission. The increase in routing message overhead reduces the performance of the ad hoc network. The value of routing overhead decreases in case of ZRP .

Average End-to-End Delay is well-defined as the average time taken for a packet to be transmitted from the source to the destination. The average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. Mathematically, it can be defined as: Avg. EED=S/N Where *S* is the sum of the time spent to deliver packets for each destination, and *N* is the number of packets received by the all destination nodes. Throughput is defined as the total amount of data, that the destination receives them from the source which is divided by the time it takes for the destination to get the final packet.

Mathematically, it can be defined as: Throughput= N/1000 Where *N* is the number of bits received successfully by all destinations.

As we compare, AODV (Ad hoc on Demand Distance Vector Routing) is an up to date routing protocol that adopts a purely reactive approach routing protocols and OLSR (Optimized Link State Routing Protocol) is purely a proactive protocol where ZRP tries to combine the advantages of reactive and proactive routing protocols. With properly configured zone radius, ZRP may outperform both proactive and reactive routing protocols, which increases the efficiency of the routing. Because of high mobility of the nodes in MANETS, always there is a greater chance of frequent link breakages between nodes, this frequent link failures will cause a number of rebroadcasts between nodes which build upon unnecessary delay in MANETS. In this paper, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANETs under black hole attacks using Intra Zone Routing Protocol. Our simulation results have revealed the efficiency of Zone Routing Protocol in terms of Packet Delivery Ratio, Throughput, Routing Overhead, End to End Delay. As future work, we intend to investigate the detection of malicious nodes using Inter Zone Routing Protocol

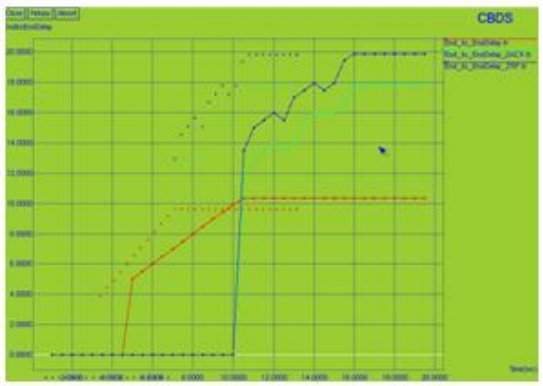


Fig.10 End to end delay

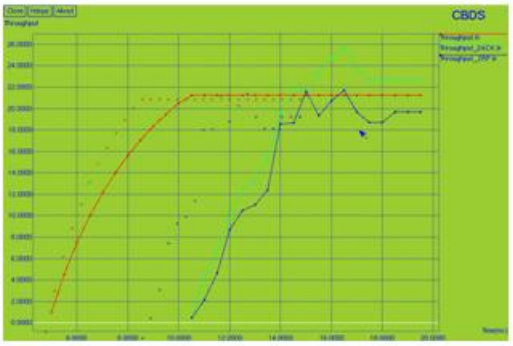


Fig.11.Throughput

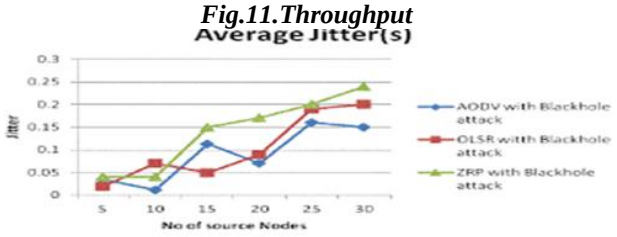


Figure 12: Performance of ZRP

REFERENCES

[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

[11] HizbullahKhattak, Nizamuddin, FahadKhurshid and Noor ul Amin, "Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash", 78-1-4673-5200-0/13, 2013 IEEE.

[12] LathaTamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), IEEE.

[13] Deng Hongmei, Li Wei, and Agarwal Dharma P., "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[14] N. Raj Payal and Swadas Prashant B., "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[15] Harsh Pratap Singh, Virendra Pal Singh, Rashmi Singh "Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review", International Journal of Computer Applications (0975 – 8887), vol. 64, no.3, February 2013.

[16] Bhoomika Patel, Khushboo Trivedi "Improving AODV Routing Protocol against Black Hole Attack based on MANET ", International journal of Computer Science and Information Technology, vol. 5(3),pp 3586-3589, 2014.

[17] Shahram Behzad, Shahram Jamali "A Survey over Black hole Attack Detection in Mobile Ad hoc Network", IJCNS, vol.15, no.3, pp 44-51, March 2015.