BLACK HOLE ATTACK PREVENTION USING RANDOM DISPERSIVE ROUTING FOR MOBILE ADHOC NETWORKS

Kamatchi.V[1], Rajeswari Mukesh[2],Rajakumar[3]

[1,2,3]Department of Computer Science and Engineering
Meenakshi College of Engineering, Chennai, India
kamatchiv@gmail.com[1] , rajimukesh95@yahoo.co.in[2],
rajamce@yahoo.com[3]

ABSTRACT

Mobile Adhoc Networks is a wireless network and it has become an important technology in current years in which security has become an important problem. Black hole Attack is one of the promising and severe security attacks in mobile ad hoc networks which block the communication of secret data during packet delivery. Black hole attack directly attacks the node's data traffic on the path and with intent drops, alters or delays the data traffic passing through that node. In other type of black hole attack which misleadingly replies for the route request which comes from the node which initiates the route discovery process that it has as much as necessary routes to the destination even it does not have path to the destination. This paper deals with prevention of black hole attacks using Shamir's secret sharing and Random Multipath Routing Algorithm

KEYWORDS

Black Hole Attack, Randomized Multipath Routing, Shamir's Secret Sharing, MANET

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a self configuring Network and they are very attractive for military communications in hostile battlefield environments so they are more vulnerable to attack than wired network. In such situations, the ability to reliably communicate and share secret information in the presence of attacker is very difficult and the attackers may attempt both passive and active type of attacks to gain nonauthorized access to classify or modify or disrupt the information process. Nodes usually share the same physical media; they transmit signals and acquire them at the same frequency band. However, due to characteristics like dynamic topology and lack in centralized management security, MANET is exposed to various kinds of attacks. Black holes are the places or the areas within which the attacker can either passively intercept or actively block information delivery and black hole is a malicious node that falsely replies for any route requests and drops all the receiving packets which are forwarded towards the destination. Each and every mobile node in an ad-hoc network moves arbitrarily and acts as both a router and a Host.

The interconnections between nodes have the capacity of changing on a continuous and arbitrary basis. Nodes within the same radio range communicate directly via wireless links, but the nodes that are far away use other nodes as relays.

DOI : 10.5121/ijans.2012.2408

1.1. BlackHole Attack

Black hole attack is one of many possible attacks in MANET. It is a kind of Denial of Service attack. This attack can be easily lessen by setting the promiscuous mode of each node and to see if the next node on the path forward the data traffic as expected.

In the other type, a malicious node sends a forged Route Reply (RREP) packet to a source node which initiates the route discovery to act as a destination node is given in Figure 1. When a source node receives multiple RREP from the same node it compares the destination sequence number contained in RREP packets and decides the greatest one as the most recent routing information and selects the route contained in that RREP packet. When sequence numbers become equal it will selects the route with the smallest hop count number. The data traffic starts flowing toward the attacker when the identity of destination node is spoofed by attacker since attacker sends Highest Destination Sequence number RREP to the source node.

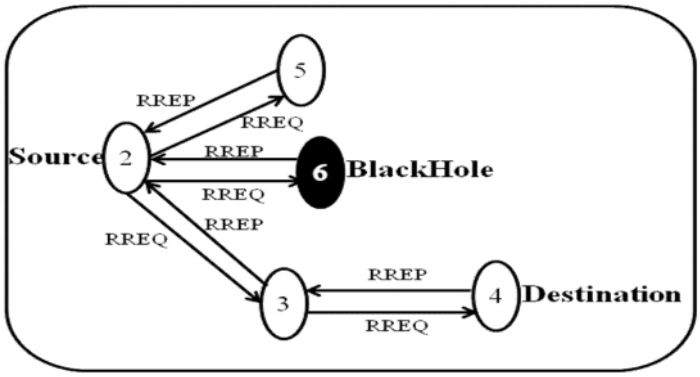

Figure 1. False Route Reply by Black Hole

1.2. Destination sequence Number (DSN)

AODV is a reactive Protocol used to discover the routes to start data communication. It builds the routes using route request and route reply cycles.DSN is a 32-bit integer [1] associated with every route and is used to decide the freshness of a particular route. The larger the sequence numbers contain fresh route information. Node N2 will now send it to node. Both the nodes N2 and N3 do not have a route to Destination D. They should broadcast the RREQ message again to its neighbors.

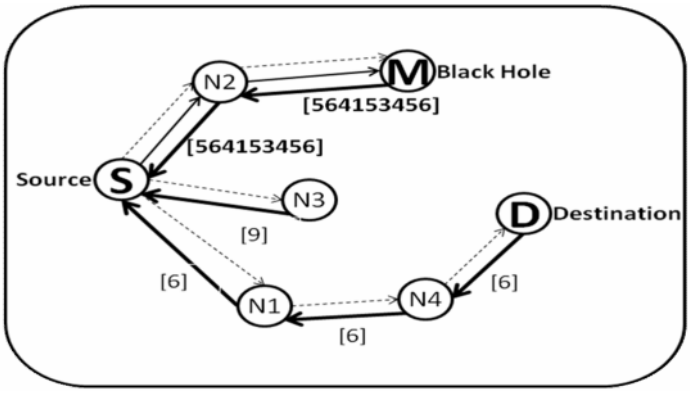

Figure 2. Forged RREP to the Source Node by Black hole

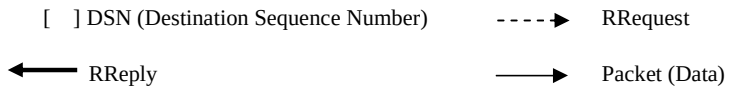

Figure 2 shows that RRequest message broadcasted by the node N2 is also be received by node M which is considered as a blackhole.

Thus, node M being malicious node, would generate a false RREP control message and send it to node N2 with a very high destination sequence number, that subsequently would be sent to the node S[2]. However, in simple AODV, as the destination sequence number is high, the route from node N2 will be considered to be fresher and hence node S would start sending data packets to node N2 then blackhole node stops the delivering the secret data which come from source node and starts dropping the packets intentionally.

2. RELATED WORK

There has been number of research results published in the literature survey that aims at finding the Black hole attacks are discussed.

Sanjay Ramaswamy, et al., [4] proposed a method for identifying multiple black hole nodes.The authors have proposed a solution for cooperative blackhole attacks. They introduced a cross checking and data routing information table. The cost of cross checking is more.

Prashant B. Swadas, et al., [3] proposed"DPRAODV" that is "detection, prevention and reactive AODV". It is to inform the other nodes in the network about the security from blackhole. The ALARM packet is sent when the node is selected as anamoly. This approach increases routing overhead and the average end to end delay.

Rei Heng, et al., [6] proposed a procedure called" distributed and cooperative procedure "to detect black hole node. The simulation result show the higher black hole detection rate and achieves better packet delivery.

Mohammad Al-Shurman, et al., [5] proposed two different approaches to solve the black hole attack.When any packet is transmitted or arrived it is updated. If there is any mismatch or deviation in the sequence number then an ALARM will notifies the black hole node existence to neighbor.

3. THE PROPOSED SOLUTION

The packets are delivered via multiple random routes after secret sharing of all the packets by Shamir's secret sharing method.A four stage approach is considered. They are: 1.Blackhole Attack Implementation, 2.Preventing blackhole using ReceiveRouteReply method, 3.Shamir's Secret sharing of information, 4.Propagation of each information share using Random dispersive routing. By using the 4 stages the BlackHole attack is prevented.

3.1. BlackHole Attack Implementation

In this Approach blackhole attack has been implemented by using modified AODV protocol has shown in the Figure 3.

In this BlackHole node sends the Destination Sequence Number much greater than the Source sequence number to the source node which initiates the route discovery. The sender then sorts the Routing table entries according to the sequence number and starts sending the packets towards the BlackHole node. The Blackhole node then start drops or alters packets which come from the source or neighbour nodes.

The Fixed path or single path has been chosen by the source to send the packets towards the blackhole node using modified AODV.

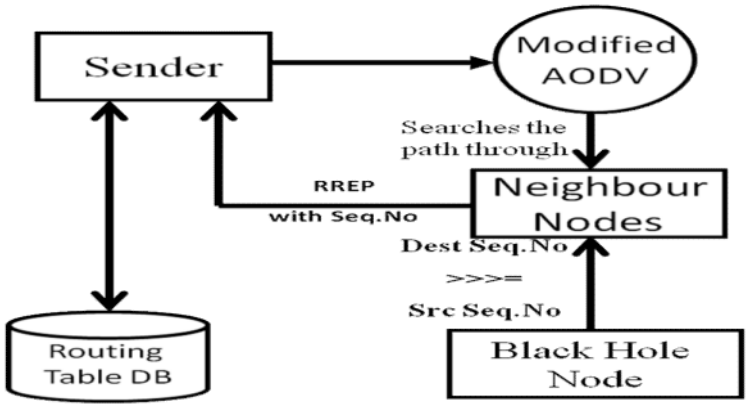

Figure 3.Blackhole Attack Implementation

3.2. Preventing BlackHole using Receive Route Reply (RRR) method

SN-Source Node
DSN-Destination Sequence Number
SSN-Source Sequence Number
NID-Node ID
MN-ID-Malicious Node ID
RT-Routing Table

```
1 SN Broadcasts RREQ
2   SN Receives RREP
3    SN Stores DSN and NID in RT
4     Retrieve First entry from RT
5          IF (DSN>>>=SSN)
6                  {
7                           MN-ID=NID
8                           Black Hole Node
9                  }
10         ELSE
11                 {
12                          Normal Node
13                 }
```

When the Node with largest Sequence number is received by the source it is considered as a black hole and that route toward that black hole is discarded and the routing table is flushed or updated and sorted according to the destination sequence number.

3.3. Shamir's Secret Sharing Method

Algorithm: Shamir's Secret sharing :(T, N) Threshold Scheme

I. Setup Phase: Source

1. Chooses a large prime q
2. Selects a polynomial $\pi \in \prod_{t-1}$ over Zq* such that $\pi(0) \equiv S \pmod q$
3. Computes $si \equiv \pi(i) \pmod q$, i = 1,. . . ,n.
4. Distributes si to the shareholders Di, i = 1,…, n

II. Reconstruction Phase: Any group Γ of t shareholders

1. Compute $\pi(0) \equiv \sum i \in r \; siLi(0) \pmod q$

Note that $Li(0) \equiv \prod j \in r, j \neq i, j/j-i \pmod q$ are nonsecret constants and can be precomputed.

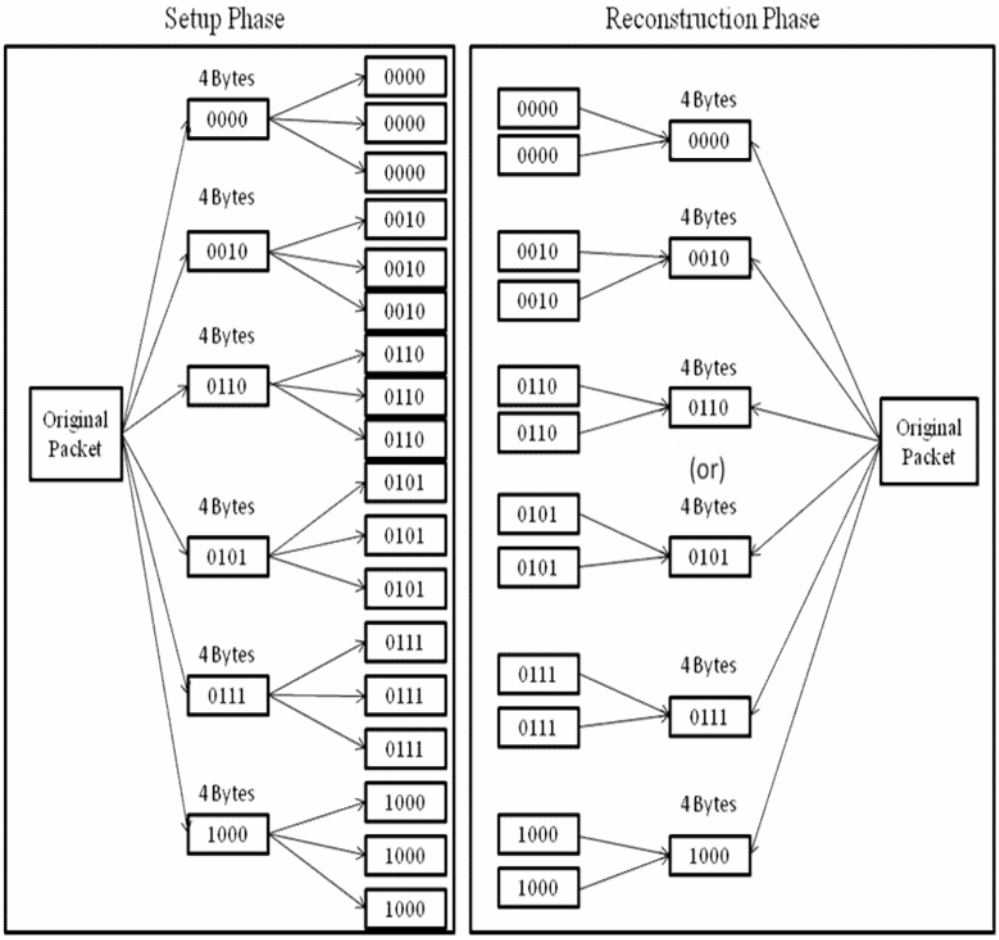

Figure 4.Shamir's Secret Sharing

Figure 4 show the Shamir's (T, N) Threshold scheme phases. In setup Phase the original information packet is divided into some bytes of shares and then copy of the shares are taken and forwarded towards the multiple random routes. In Reconstruction phase upon receiving the copy of some shares and partial bytes of the original information the entire packet has been reconstructed.

3.4. Propagation of Each information share using Random Dispersive Routing

Randomized multipath routing algorithm that can overcome the fixed path or single path problems. This Algorithm shows that multiple paths will be computed in a random way each time when an information packet needed to be sent to the destination, therefore the number of routes selected by different shares of different packets changing. The randomly generated routes are as dispersive as possible.

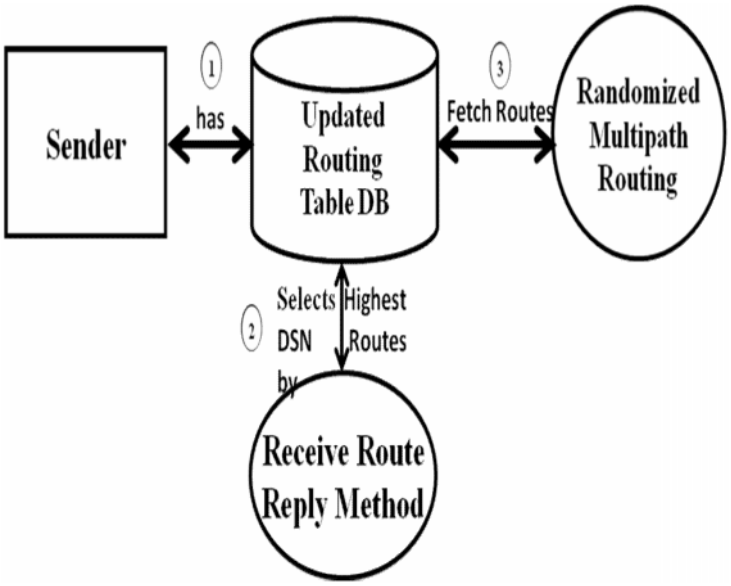

Figure 5.Choosing Random Routes from Routing Table

The figure 5 shows how the multiple random routes have been selected by the source from the updated routing table. The Routing table contains all the routes from the source to the destination after deleting the route highest destination sequence number or abnormal sequence number which is considered as a blackhole node.

The information packets are sent to the randomly selected multiple routes with "n shares' of data so even if the blackhole present in the route, it can hear or absorbs only partial or incomplete data among "n" number of shares is shown in Figure 6. Every time the path has been selected by the sender node which needs to send the data. If the sender receives 'n' shares of the same message, and then the energy consumption is more in receiver.

The sender has to send all the 'n' shares of the messages to the receiver, even if the receiver receives the message, which causes unwanted energy consumption in sender node. So the unwanted energy consumption in both the sender and the receiver node needs to be reduced,.If the receiver receives some shares of the message from 'n' shares, then it should intimate to the sender that the receiver received the message. After receiving the confirmation message from the receiver, the sender node stop the current message transmission and starts to send another 'n'

shares of the message. So the unwanted transmission in the both sender and the receiver node is reduced.

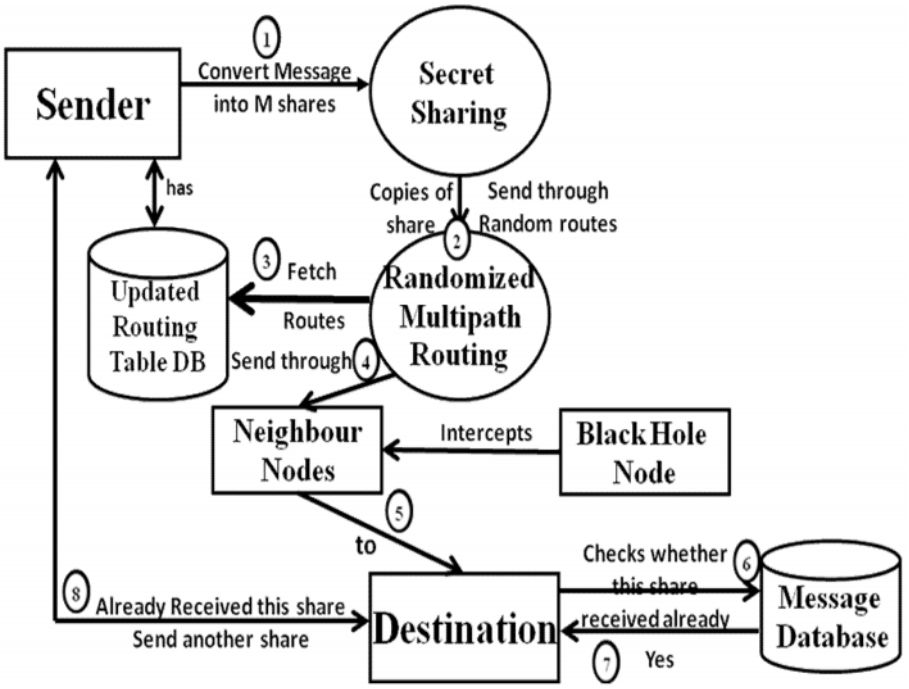

Figure 6. Randomized Multipath Routing and Shamir's (T,N) Threshold scheme

4. SIMULATION AND RESULTS

The simulation is done with the help of NS-2 (v-2.34) network simulator. The implementation of the protocol has been done using C++ language in the backend and TCL language in the frontend on the Red hat Linux operating system.

Table 1.Simulation Parameters

Number of Mobile Nodes	20
Topology	1500m x 1500m
Number of Black Hole Node	2
Pause Time	5s
Traffic	Constant Bit Rate
Maximum Speed of Node	20 m/s
Packet Rate	4 Packets/s
Routing Protocol	AODV
Communication Traffic	CBR
Maximum No. of Packets in Queue	1000

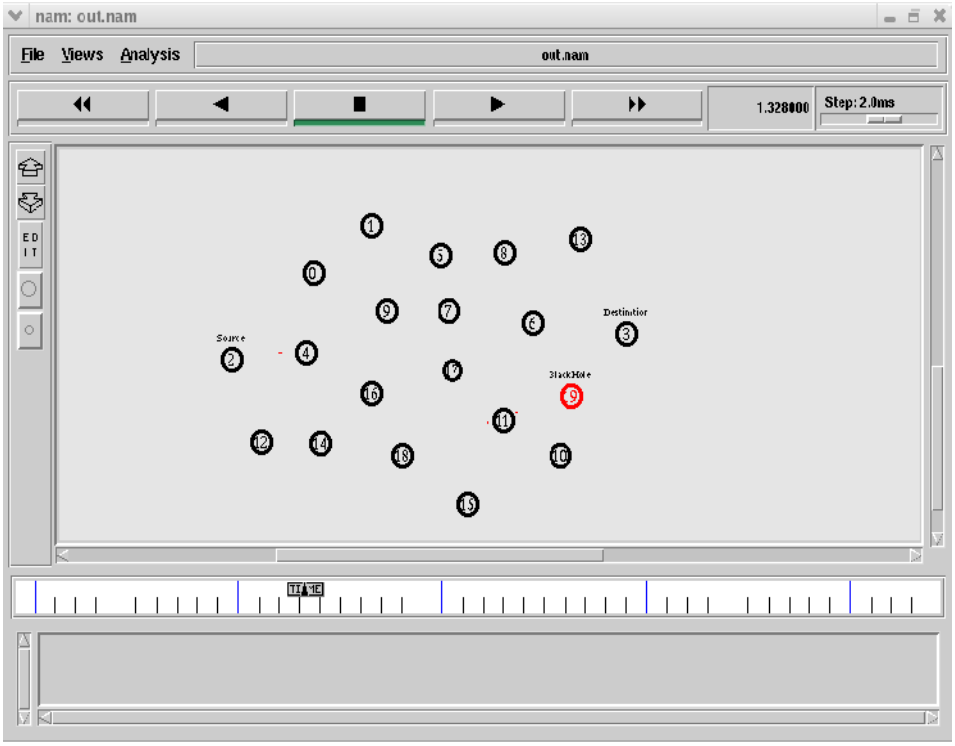

Figure 7. BlackHole Attack

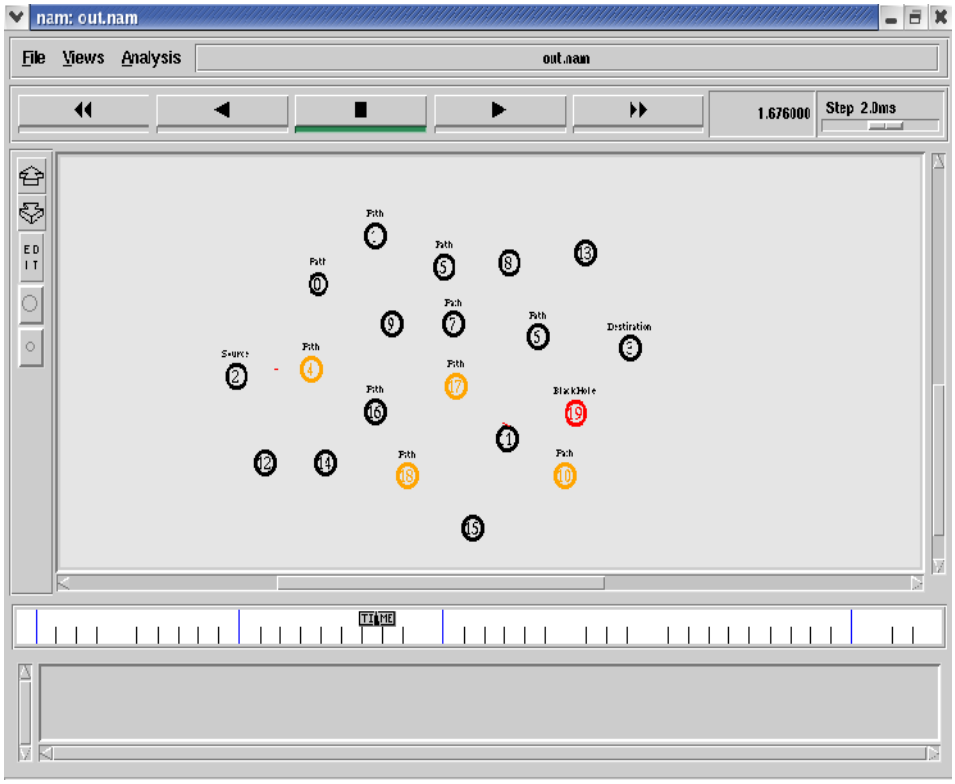

Figure 8. Prevention of Blackhole using DSN

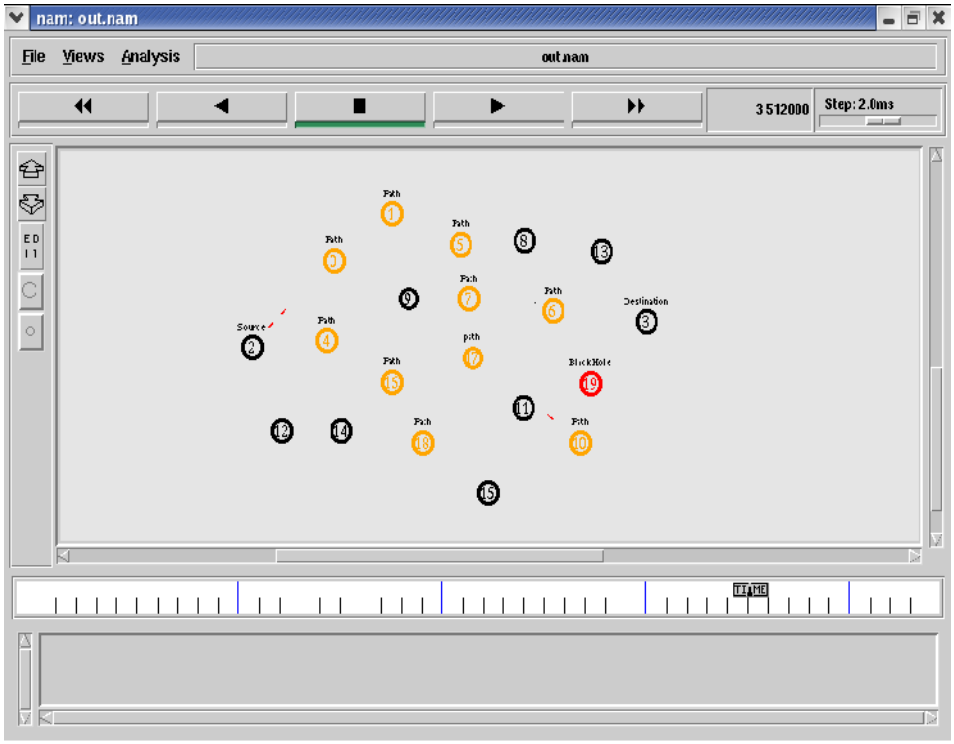

Figure 9. Random Multipath routing

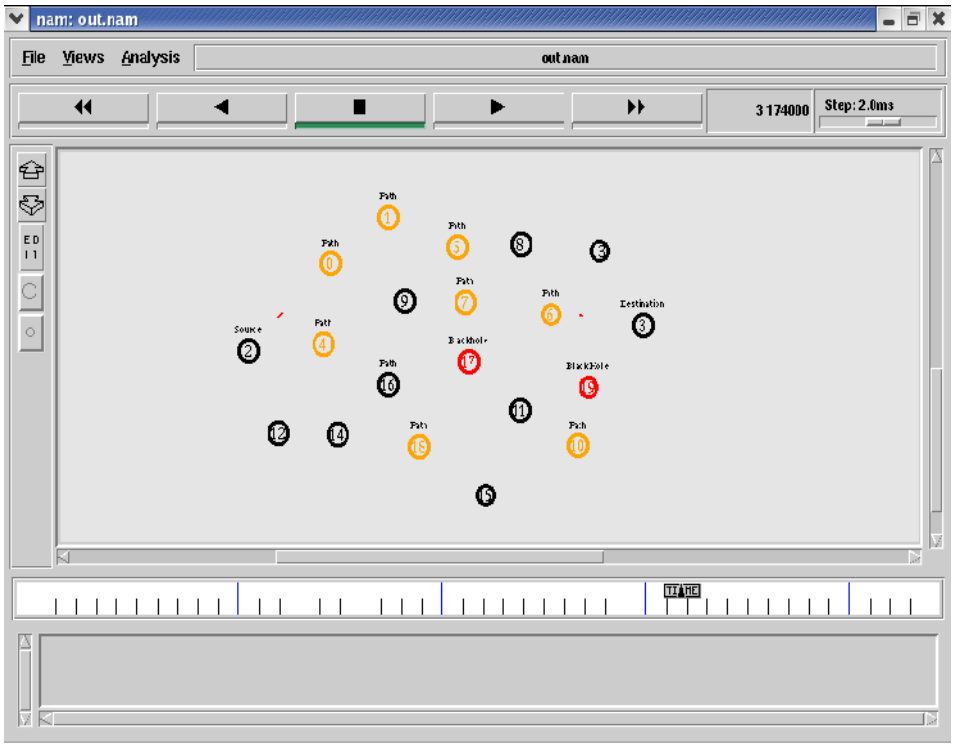

Figure 10.With Blackhole Packet transmission using Random routes

The Figures 7, 8, 9 and 10 shows how the blackhole attack has been implemented using RRR method and the how the highest destination sequence number route is discarded from routing table and random paths are chosen from refreshed routing table. Also shows how the secret shares are delivered to the destination using random routes and the blackhole presence in random routes.

4.1. Packet Delivery Ratio

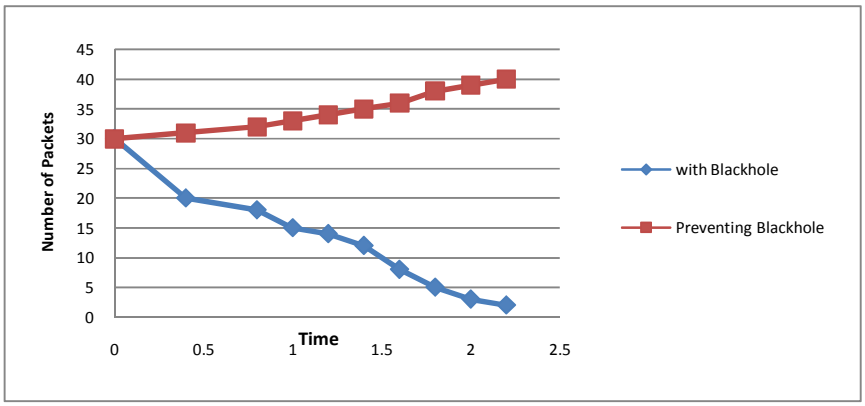

Figure 11. Packet Delivery Ratio

Figure 11 shows the effect of blackhole on throughput of received packets after deleting the blackhole using the single path and the effect of using random routes to secure the packets with increased throughput. Clearly throughput has been increased to the maximum. The simulation result has shown that by using random path PDR has been increased to 77% than using the fixed path with 65% of PDR.

4.2. Packet Loss Ratio

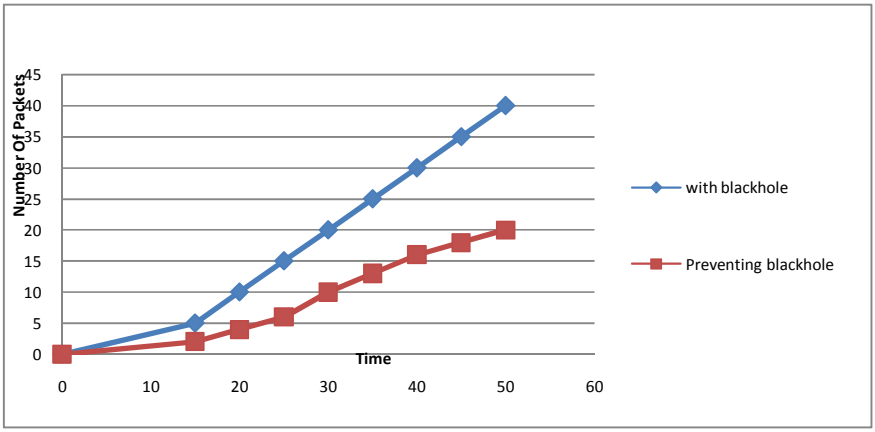

Figure 12. Packet Loss Ratio

As speed increases, the position of a node will clearly change more rapidly. This will cause more and more packets to time out before reaching their destinations. PLR informs about the amount of control packets fails to reach the destination in a timely manner. By sending the packets through random routes the blackhole interception rate is reduced to low thus the delay in sending of

packets is reduced. The simulation results has shown that the PLR is decreased to 0.16ms by sending packets via random path where as PLR is 1.5ms in the case of fixed path.

5. CONCLUSION AND FUTURE WORK

By using Random dispersive routes maximum throughput is achieved with reduced delay even after blackhole presence. Energy consumption at both sender and the receiver is reduced and high security is achieved. Communication between sender and receiver is achieved with minimal energy factor. Future work can include the areas to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes.

REFERENCES

[1] Lalit Himral, vishal Vig "Preventing AODV Routing Protocol from Black Hole Attack." International Journal of engineering Science and Technology, Vol3 No.5, May2011, pp 3927-3932.

[2] T. Claveirole, M. D. de Amorim, M. Abdalla, and Y. Viniotis. Securing wireless sensor networks against aggregator compromises. IEEE Communications Magazine, pp 134–141, Apr. 2008.

[3] Payal N. Raj and Prashant B. Swadas, "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.

[4] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard,"Prevention of cooperative black hole attack in wireless ad hoc networks," International Conference (ICWN'03), Las Vegas, Nevada, USA, 2003,pp 570-575.

[5] Seong-Moo Yoon and Seungjin Park ,Mohammad Al-Shurman,"Black Hole Attack in Mobile Ad Hoc Networks", ACM South East Regional Conference, Proceedings of the 42nd annual Southeast regional conference, pp 96-97,2004.

[6] Rei Heng, Cheng and Shun Chao Chang, Chang Wu Yu, Tung-Kuang, Wu, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 International Workshop, Nanjing, China, May 2007, pp 538–549.

Authors

V.Kamatchi has completed her B.Tech I.T from Vel Tech Engineering College, M.B.A from Anna University and M.E CSE from Meenakshi College of Engineering. She has 4.5 years of teaching experience from Vel Tech Multi Tech Engineering College as a Lecturer and currently working as an Assistant Professor in the Department of Information Technology in Indira Institute of Engineering and Technology. She has presented 2 papers in international conferences and 2 papers in National conferences. Her Research Area includes Mobile Adhoc Networks and Network Security.

Dr.Rajeswari Mukesh has obtained her Ph.D from JNTU Hyderabad. She has nearly 20 years of teaching experience. Her area of interest is Network Security. She has published papers in several refereed international journals and conferences. She is right now guiding 4 research scholars. She has received grants from AICTE, TNSCST and CSIR for projects and conducting conferences.

P.Rajakumar has completed his B.E CSE from Meenakshi College of Engineering and M.E CSE from Sri Muthukumaran Institute of Technology. He has 4 years of Teaching experience and working as a Assistant Professor in Meenakshi College of Engineering and also handled project for U.G and P.G Students.