Detection and Prevention of Black Hole Attack In Ad Hoc Network Using Cryptographic (Key Exchange) Techniques

[1]Gursharan S Sidhu, [2]Rekha Garg
[1]M.Tech, ECE Department, GGSCMT, Kharar, Punjab, India,
[2]Assistant Professor, ECE Department, GGSCMT, Kharar, Punjab, India.

***Abstract* - Mobile ad hoc networks (MANET) are accumulations of self arranging portable nodes with different topologies and have no altered foundation or infrastructure. MANETs do not have central organization; in this technology every node performs both host like a router and forward each packet among the network in multi-hop way. Because of the focal qualities like lack of centralized monitoring, dynamic network topology, the open medium and management of all networks are not fully secure. All are venerable to various types of attacks. Ad hoc on demand vector (AODV) is one of the routing protocol being used for MANET or wireless network. Black hole attack is one example of similar attacks that is launched on AODV. In black hole attack, the malicious node draws in all packets by erroneously guaranteeing a fresh route to the destination node and ingests them without sending them to destination. AODV is applicable of both unicast and multicast routing. It builds routes between nodes only desired by source nodes. It will maintain these routes as long as needed by the sources. Furthermore AODV protocol uses the sequence numbers to make ensure of freshness of routes. It is a loop-free, self-starting, and scales of large numbers of mobile nodes. In this paper, a new solution against the Black Hole attack is projected. So in this study, we use the AODV protocol for establishing the connections and for detection we use the Diffie-Hellman Technique (with 64 bit DES key exchanges Cryptography Scheme) for key exchange.**

***Index Terms* – MANET, AODV, RREQ (Route Request), RREP (Route Reply), DH (Diffie-Hellman Technique).**

I. INTRODUCTION

Mobile ad hoc network is a self-governing system, where nodes or stations are connected with each other through wireless links. There is no limit on the nodes to join or depart the network, therefore the nodes join or left freely. Mobile ad hoc network has dynamic topology that can change promptly because the nodes move freely and can arrange themselves randomly. This property of the nodes makes the mobile ad hoc networks unpredictable from the point of view of scalability and topology decentralized wireless systems. MANET consists of mobile nodes that are free in moving in and out in the network. Nodes can be a device or host i.e. mobile phone, laptop, personal, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host or router or both at same time. They can form illogical topologies depending on their connectivity with each other in the network. These nodes have the facility to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Security in Mobile Ad Hoc Network is the most important concern for the basic functionality of network. Accessibility of network services, privacy and integrity of the data can be achieved by assuring that security issues have been met. MANET often endure from security attacks because of its nature like medium changing its topology dynamically, MANET work without any centralized medium there is no base station required. In MANET node can communicates with each other on the base of mutual trust. This characteristics makes the MANET more exposed to be exploited by an attacker from inside the network. Wireless links also makes the MANET more liable to attacks which make it easy for the attacker to go inside the network and can easily access to the ongoing communication Mobile nodes present within the range of wireless link can overhear and even participate in the network. MANET must have a secure way for transmission of data and communication and this is quite demanding and impetrative issue as there is increasing threats of attack on the Mobile Network. Security is the most important issue of the day. In order to provide secure communication and data transmission engineer must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, flooding attack, routing table overflow attack, Denial of Service selfish node, impersonation attack are kind of attacks that a MANET can suffer from. MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, any authorization facility, and vigorously changing topology

With the increase of portable devices as well as growing in wireless communication, ad-hoc networking is gaining more importance with the increasing number of wide-ranging applications. Ad-hoc network can be applied anywhere where there is tiny or no communication infrastructure or the existing infrastructure is cheap or difficult to use. Ad hoc networking allows the devices to maintain connections to the network as well as we can easily add and removing devices and make the network. The applications for MANET are assorted ranging from large-scale, mobile, highly dynamic networks, small network.

Black hole attack is one of possible attack in MANET. The black hole attack is attack in which black node advertise itself for having the shortest path to the destination node and source node think that it's a genuine node and send the data to black node result black node will dropped whole data shown in Fig. the source node is 0 transmit a route request message to discover a route for

sending packet destination node 2 route request (RREQ) transmit by node 0 is received by nearest nodes1, 3 and 4.Node. 4 send a route reply message instantly without even having a route to destination node 2. RREP message from a malicious node is the first to arrive at a source node. As it is malicious node now a source node revises it routing table for the new route to the particular destination node and discards any RREP message from other nearest nodes even from an original node. Once a source node saves a route, it starts sending data packets to a malicious node hoping they will be forwarded to a destination node. Malicious node (performing a black hole attack) drops all data packets rather than forwarding them onto destination.

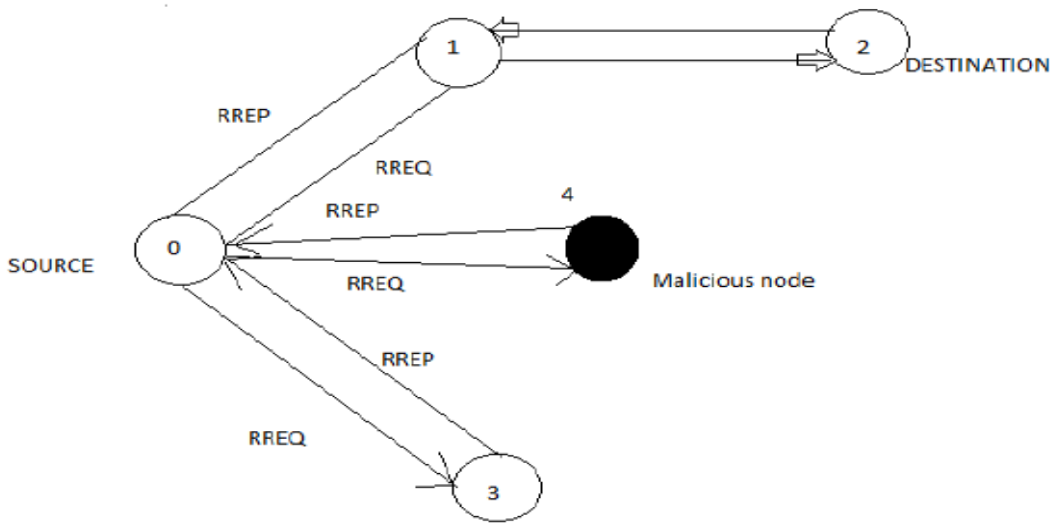

Figure: 1 Black Hole Attack

The Ad hoc On Demand Distance Vector routing algorithm is a routing protocol that is designed for ad hoc mobile networks. AODV is applicable of both unicast and multicast routing. It is the on demand algorithm, meaning that it builds routes between nodes only desired by source nodes. It will maintain these routes as long as needed by the sources. Furthermore AODV protocol uses the sequence numbers to make ensure of freshness of routes. It is a loop-free, self-starting, and scales of large numbers of mobile nodes. AODV builds routes using a route request / route reply query cycle. When a source node want the route to a destination node for which it does not already have route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet and update their information for the source node and then set up backwards pointers to the source node in the route tables addition the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most sequence number for the destination of which the source node is aware. A node receiving the RREQ request may send a route reply (RREP) if that is either the destination or if it have the route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes always track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it further as the RREP propagates back to the source, nodes set up forward pointers to the destination node. Once the source node receives the RREP, it may start to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with smaller hop count, it may update its routing information.

Diffie-Hellman is algorithm to provide the securely transmitting a secret to be shared between two parties over the untrusted network in real time. A shared secret is critical for two parties who have not communicated before; it is used so that they are able to encrypt communications. Today, DH algorithms is used by protocols such as Internet Protocol Security (IPSec), Secure Shell (SSH), and Secure Sockets Layer The protocol allows the two users to exchange a secret key over an insecure medium without any prior secrets. Diffie-Hellman key exchange (DH) is the cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. Diffie-Hellman is not basically a encryption algorithm but a key-exchange algorithm. The protocol has two system parameters p and g. They are both public and may be used by all the users in a system. Parameter p is a prime number and parameter g (usually called a generator) is an integer less than p, with the following property: for every number n between 1 and p-1 inclusive, there is a power k of g such that n = gk mod p. (n – very large prime number g – base or generator. Both the numbers n and g are selected such that n > g and g is the primitive root of n. x and y are secret keys of A and B respectively)

II. RELATED WORK

L Tharani et al. (2015) In this paper ,Black hole attack is a champion amongst the most important security issues in MANET. In this attack, a malicious node imitates a destination node by sending delivered fake RREP to a source node that begins the route discovery, and consequently withdraw data traffic from the source node. We have to end delays among the packet transmission

between the nodes and inspected the effect of black hole attack on AODV tradition. The result shows vital degradation in execution of uniquely named ad hoc on demand vector routing protocol (AODV) under black hole attack) [1].

A.Bhosle et al. (2012) this also proposed an efficient solution for the detection of the Black hole nodes in the Mobile Ad hoc networks based on the AODV routing protocol In this algorithm, known as Modified AODV mechanism a Watchdog mechanism is used. In this mechanism each and every node maintains two extra tables. First one is called the pending packet table and another one is called the node rating table. Pending Packet Table contains Packet ID, Next Hop, Expiry Time and Packet Destination while the Node Rating Table contains Node Address, Packet drops, Packet forwards and Misbehave of the node [2].

Arunima Patel et al. (2012), we focus on analyzing the performance of one of the popular routing protocols for MANET AODV with Black hole AODV. Our aim is to simulate the AODV protocol with and without Black Hole Attack on various performance metric parameters. Thus we have evaluated the performance of AODV protocol with and without Black Hole attack using different performance metrics and by varying the number of nodes as well as the number of black holes. It was observed in results that AODV always perform better in absence of Black Hole attack [3].

Pooja Jaiswal et al. (2012), A specially appointed system is a accumulation of mobile node that powerfully structure a temporary system. It works without the utilization of existing base. One of the vital routing protocols utilized in specially appointed systems is AODV protocol. This is expected to offer a scope of adaptable administrations to portable and migrant clients by method for incorporated homogeneous architecture. Vitality compelled hub, low channel data transfer capacity, node portability, high channel blunder rates, channel variability and bundle misfortune are a portion of the restrictions of MANETs. The security of the AODV convention is traded off by a specific sort of assault called Dark Gap Assault. Dark gap assault is one of the security danger in which the movement is diverted to such a hub, to the point that really does not exist in the system. [4].

Payal N Raj et al. (2009) they proposed the DPRAODV (detection, prevention and reactive AODV) to prevent a black hole attack by informing the other nodes about the malicious node. As the value of Route REP sequence number is to be taken higher than the threshold value, the node is suspected like to be malicious and it can adds the node to the black list. As the node detected an anomaly, now it sends a new control packet that is ALARM to its neighbors. In this research paper the authors taking the protocol DPRAODV to counter the Black hole attacks. DPRAODV checks to find whether the RREP_Seq_No is higher than the threshold value. In this protocol they threshold value is updated at every time interval of the time. If the value of RREP_Seq_No is found to be higher than the threshold value, the node is suspected to be malicious and is added to a list of blacklisted nodes. It will also send an ALARM packet to its neighbors with information of the blacklisted node. Thus, the neighbor nodes know that RREP packets from the malicious node are to be neglected. That is, if any of nodes receives the RREP packet, it looks the list to check the source of the received message. If the reply is from the affected node, the same is ignored. Thus, the protocol though successful, suffers from the overhead of updating threshold value at every time interval and generation of the ALARM packets. The routing overhead, the result is higher [5].

N Vetrivelan et al. (2008) we compare the performance of the three prominent routing protocols for mobile ad hoc networks, Ad hoc On Demand Distance Vector (AODV), Destination Sequenced Distance Vector (DSDV) and Temporally Ordered Routing Protocols (TORA). We have chosen four performance metrics taken such the Average Delay, Packet Delivery, Fraction and Routing Load. Varying MANET Size simulation is used for the popular routing protocols AODV, DSDV and TORA. The simulations are carried out on NS-2. The performance differentials are analyzed using varying network size and simulation times. The simulation results confirm that AODV performs well in terms of Average Delay, Routing Load concerns; TORA performs in Packet Delivery Fraction [6].

Hesiri Weerasinghe, (2008), proposed the solution which finds the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution of this can adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This can use algorithm uses a methodology to detection multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. And the protocol that is used is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP) [7]

III. PROBLEM DEFINITION

Black hole attack is also one of the possible attack which harms the security of MANET because now a day mostly the people can use the ad-hoc network to transmission of data so it is very important to prevent the mobile ad-hoc network to the black hole attack In a black hole attack when the node want to communicate with each other before the communications route will be establishing between them during the route establishing communication node will send the route request than destination node will send the reply but in during these communication black node or malicious node will also the reply to the source node .source node trust that this reply is send by the original node. Source nod send the data to that node and data will drop because that node was not original node that is malicious node that is black hole attack. or we can say that when communication is going smoothly and a intruder node comes in between those two nodes then it can fetch the data and results in a drop of packets which leads to packet drop hence packet could not able to reach the destination it also effects the security as well as QOS of the network.

Objectives of Problem

- The study focus on analysis/study of black hole attack in MANET and its consequences.
- Simulating the black hole attack using Reactive Routing protocols.
- Detection of black hole attack and prevent with the solution.
- The main aim of the work is to provide the security to the MANET from black hole attack.
- Data should be through to the destination/original node.

IV. METHODOLOGY

We are using the AODV protocol for route establishing because this protocol is on demand protocol and for detection of black hole attack we are using x-or of the ip address and random number, after the detection we can use the Diffie-Hellman algorithms to create the secure channel between the source and sender. The proposed methodology is implemented in NS-2. NS-2 is an open-source simulation tool that runs on Linux. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired and wireless (local and satellite) networks. Now we can give the screenshot of my simulation process.

A. Simulations When Black Hole Attack

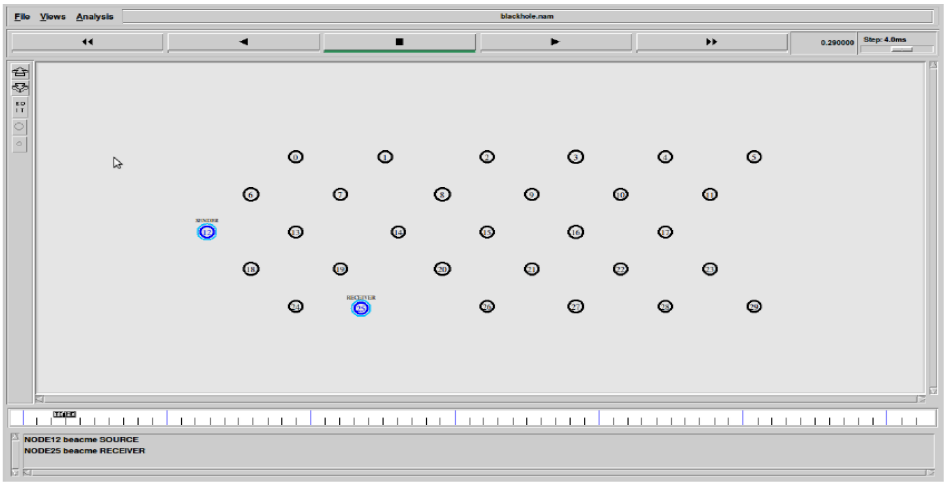

Figure 2.1.1 Source and Destination Node in Ad-hoc network

Figure 2.1.1 shows the network having total 29 nodes and shows the source node12 and destination node29.

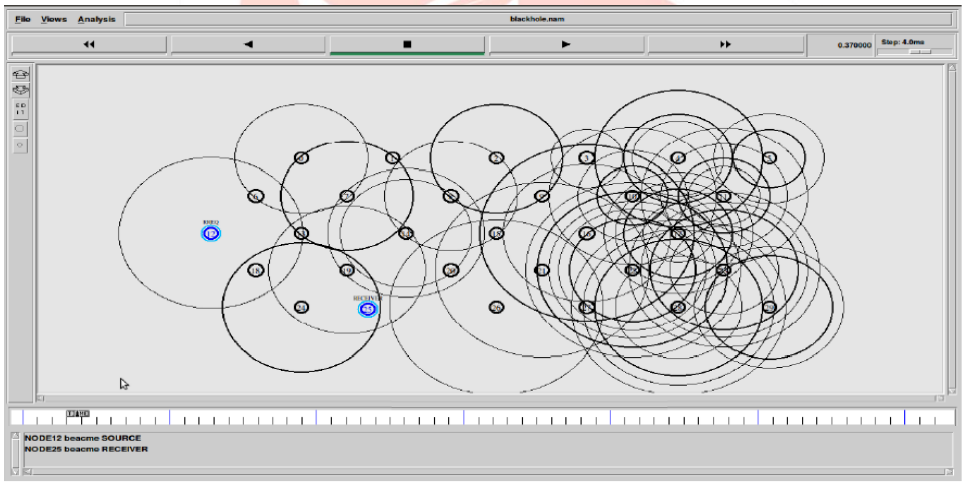

Figure 2.1.2: Route Request of Source Node

Figure 2.1.2 shows that source node is sending the route request

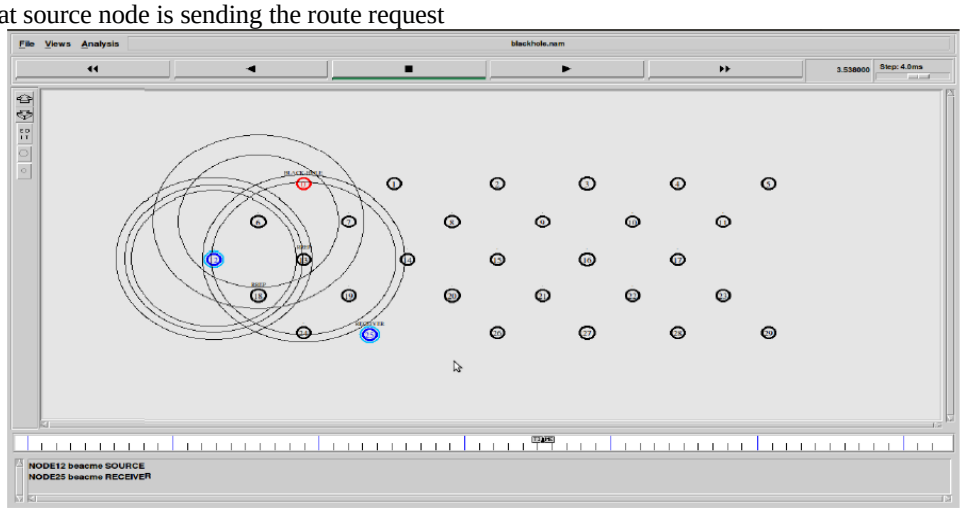

Figure 2.1.3: Route Reply of Neighbor node 30 (Black hole)

Figure 2.1.3 show the route reply of nodes including the reply from Black Hole (Node30)

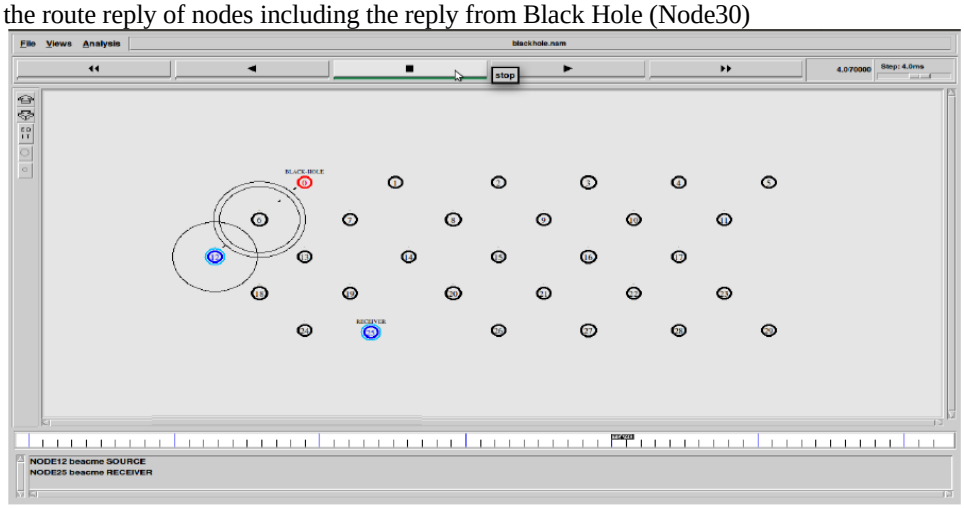

Figure 2.1.4: Route Setup and Data Transfer

Figure 2.1.4 shows the black node is sending the route request and source node sends the data.

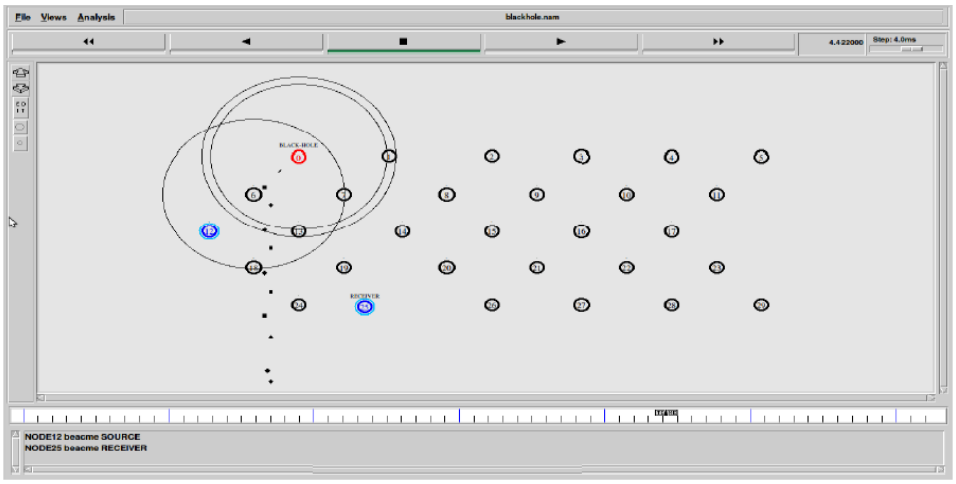

Figure 2.1.5: Loss of Data

Figure 2.1.5 shows that when the data is send to black hole node and whole the data is dropped by black node

B. Simulations Using proposed Methodology

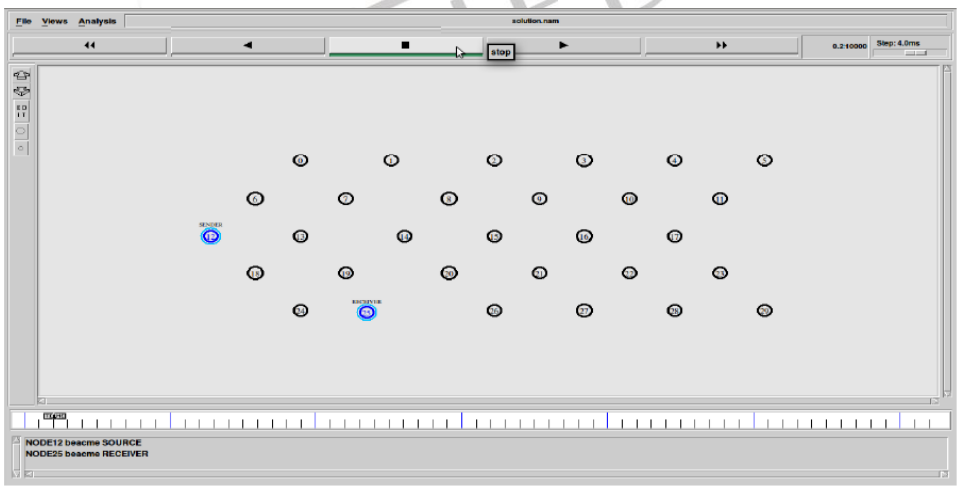

Figure 2.2.1: Source and Destination Node

Figure 2.2.1 shows the creation of ad-hoc network and total number of nodes taken and also the source and destination nodes.

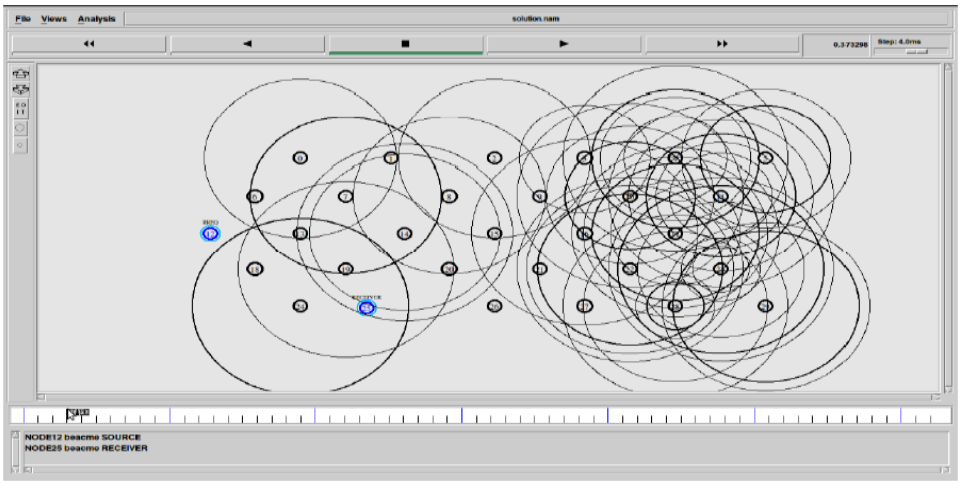

Figure 2.2.2: Sending Route Request

Figure 2.2.2 shows the route request send by the source node to other nodes

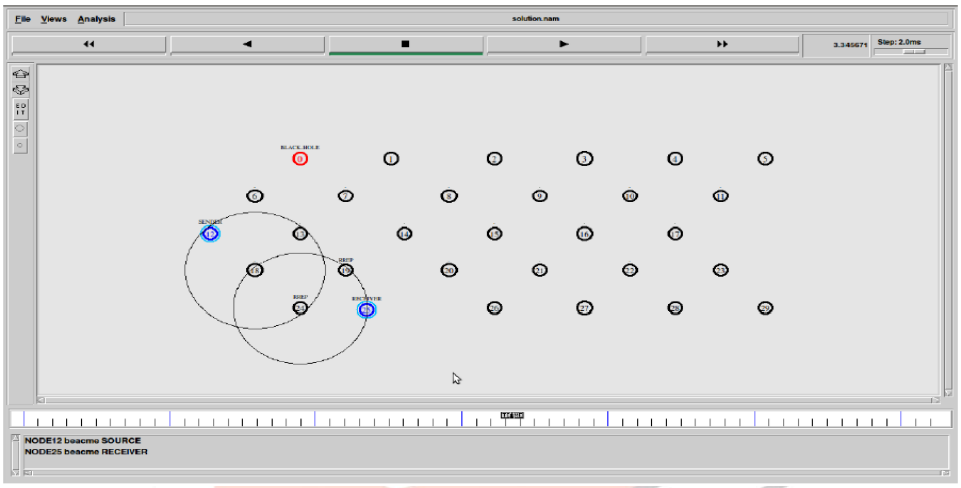

Figure 2.2.3: Sending Route Reply

Figure 2.2.3 shows the route reply send by the other nodes to the source node.

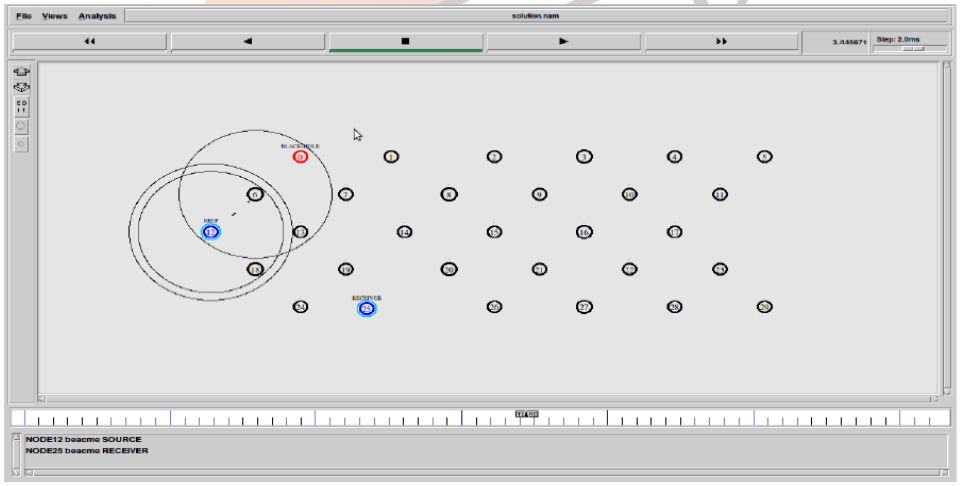

Figure 2.2.4: Route Reply by Black Node

Figure 2.2.4 shows the route reply sent by the black hole node. Now in our purposed solution after finding the shortest route than source node matches the z value.

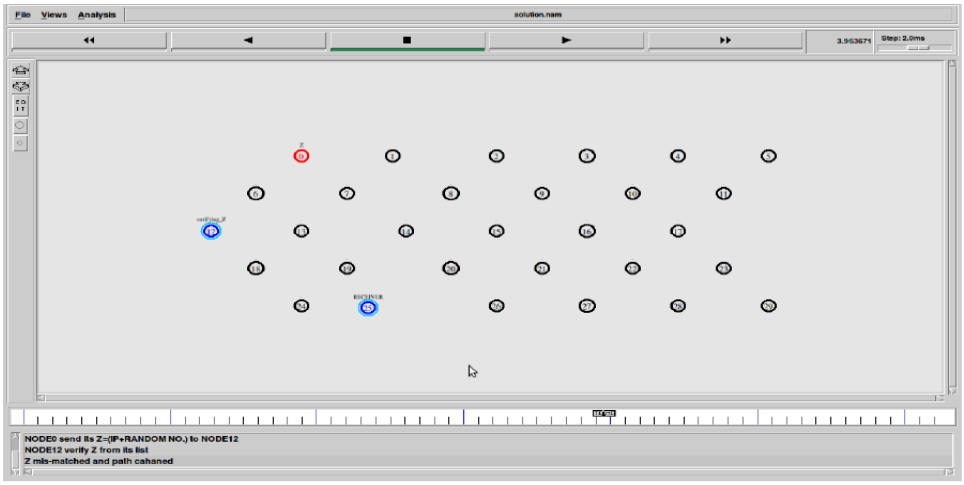

Figure 2.2.5: Verifying the z value with Black Node

Figure 2.2.5 shows verifying of the z value.

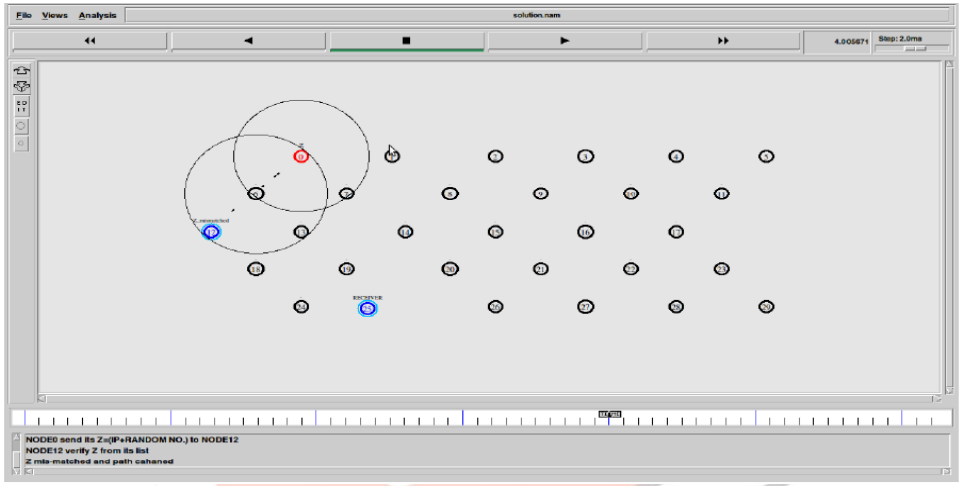

Figure 2.2.6: Mismatch of z Value in Black Node

Figure 2.2.6 shows the mismatch the z value with black node and go to the next path

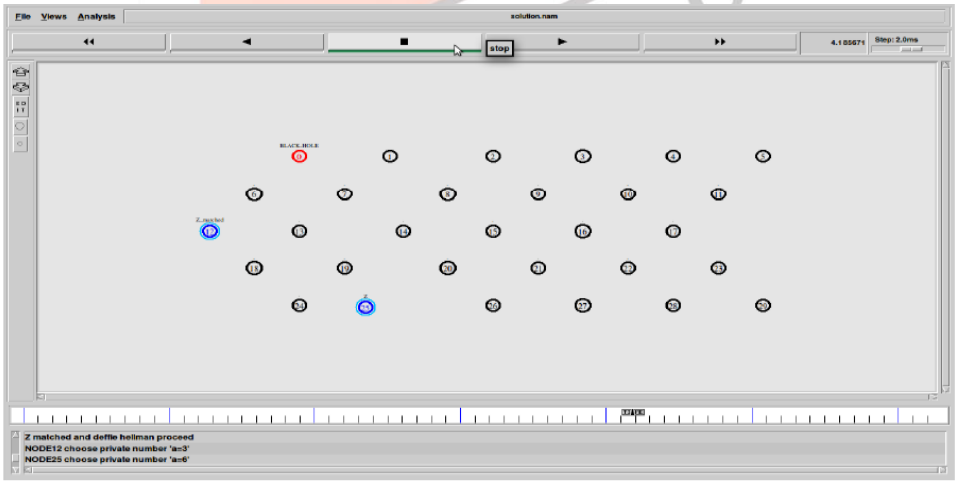

Figure 2.2.7: Matching the z Value with Destination Node

Figure 2.2.7 shows the verifying the z value to destination node

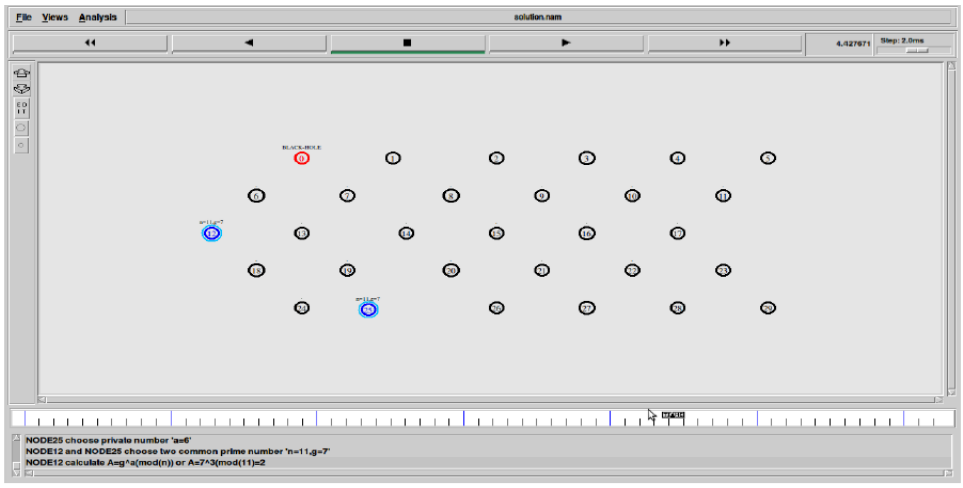

Figure 2.2.8: Secure Channel Setup

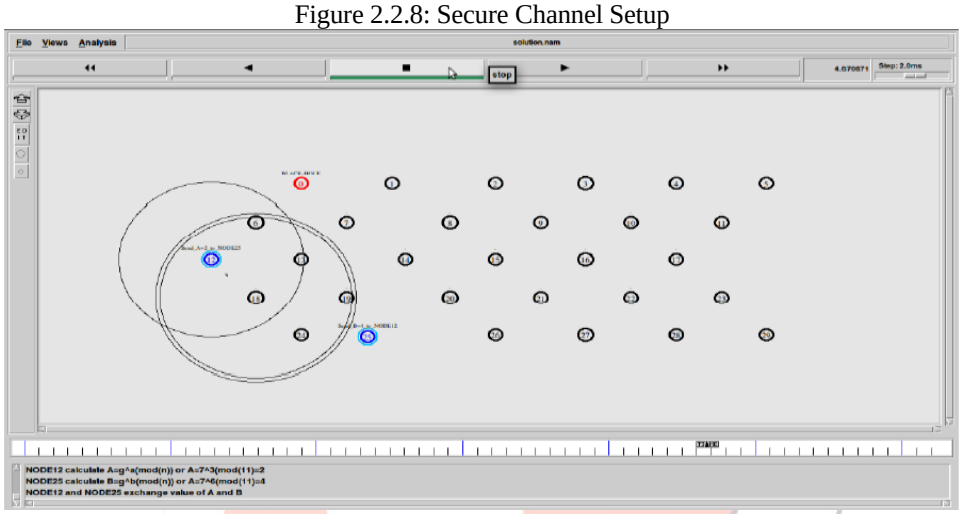

Figure 2.2.9: Sending the Data to Destination Node

Figure 2.2.8 and 2.2.9 show the secure channel establishing between the source node and destination node to sending the data.

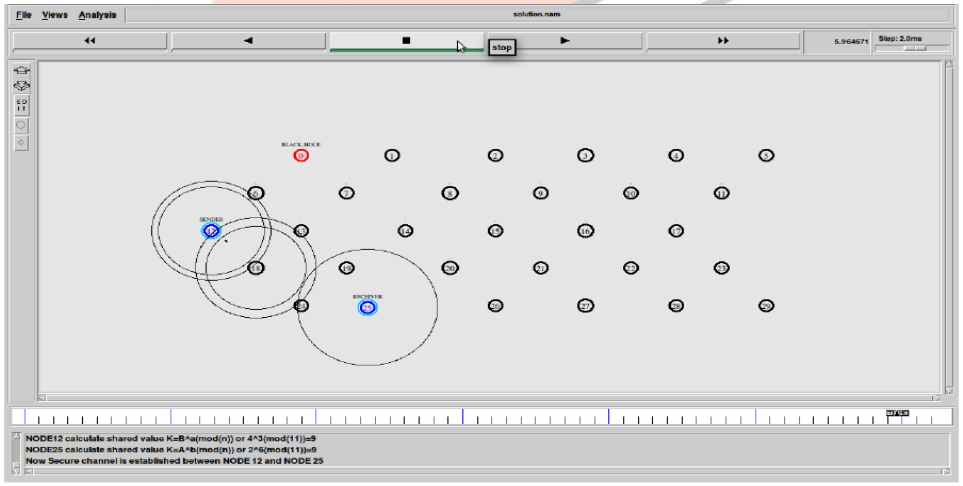

Figure 2.2.10: No Loss of Data

Figure 2.2.10 shows the establishing of secure channel and data is transferred from source node to destination node and there is no loss of data.

V. CONCLUSION

In this paper we have instigated black hole attack in MANET/Ad Hoc network and premeditated its influence on the security issue on the Mobile Ad Hoc Network. For this purpose we implemented a new AODV routing protocol which behaves as black hole. In this study, we analyzed effect of the Black Hole attack, in MANET using of AODV protocol. For this purpose, we use the NS-2.in the simulation We simulated two scenarios first is that when the black hole attack is attacking the network and whole data is lost, Second scenarios is using our purposed technique, having simulated in first scenarios when the black hole attack is attacking

the network in that case whole data is loss and throughput is zero. In the second case when we use the technique we saw that there is no loss of data and throughput is maximum.

VI. FUTURE WORK

Wireless Ad hoc networks are widely used networks due to their flexible nature i.e. easy to deploy regardless of geographic constraints. These networks are exposed to both external and internal attacks as there is no centralized security mechanism. A lot of research work is still needed in this area. We tried to discover and analyzed the impact of Black Hole attack in MANETs using AODV. In future we can analyze Black Hole attack in other MANETs Routing protocols such as DSDV, TORA and GRP and also different techniques can be used for prevention and detection of this attack, also taking more than one black node in the network.

REFERENCES

[1] L Tharani,(2015) " Preventing Black Hole Attack in AODV using timer-based detection mechanism", International Conference on Signal Processing And Communication Engineering Systems (SPACES), VOL.6 ,2015.

[2] Amol A. Bhosle, TusharP,Thosar and SnehalMehatre, (2012) "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012,pp 2012.2105.

[3] Arunima Patel, Sharda Patel, Ashok Verma,(2012) " AReview of perfmance of evaluation of ADOV protocol in MANETwithout black hole attack", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

[4] PoojaJaiswal ,Dr. Rakesh Kumar , "Prevention of Black Hole Attack in MANET ", IRACST – International Journal of Computer Networks andWireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No5, October 2012.

[5] Payal N Raj Prashant B. Swadas (2009**)** "DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET", IJCSNS International Journal ofComputer Science and Network Security, Vol. 2, 2009.

[6] N Vetrivelan, Dr. A V Reddy (2008) "Performance Analysis of Three Routing Protocols for Varying MANET Size ", Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol II ,IMECS, 2008.

[7] Hesiri Weerasinghe,(2008) "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, 2008, pp 362-367.