ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Modified AODV Routing Protocol to Detect and Avoid the Black Hole Attack in MANET

K. Shobina[1], N. Mohan Prabhu[2]

M.E. Computer Science and Engineering, Mount Zion College of Engineering and Technology, Lena Vilakku, Thirumayam Tk, Pudukkottai, Tamil Nadu 622507, India.

Assistant Professor, Department of Computer Science and Engineering, Mount Zion College of Engineering and Technology, Lena Vilakku, Thirumayam Tk, Pudukkottai, Tamil Nadu 622507, India.

ABSTRACT: The focus is on trustworthy and fault- tolerant communications and behaviors of wireless networking scenario to detect and isolate the malicious node in AODV routing protocol that cause black hole attack in MANET. Traffic and security are the two main causes, which affects the performance of wireless communications in Mobile Ad-hoc Networks. This kind of wireless communications are most admirable by the attackers due to the dynamic changes of the network topology. Black hole attack is an attack which affects the network scenario more crucially. For all these attacks and traffic problems, we require a new methodology called Modified AODV Routing Protocol. Modified AODV provides RREQ and RREP facility to carry over the data transmission successfully between Source and Destination along with A* and Floyd-Warshall's algorithm.

KEYWORDS: Modified AODV, MANET, Black Hole Attack Performance, Security, Trust mechanism.

I. INTRODUCTION

A Mobile Ad Hoc network is a self-configuring networks consisting of mobile nodes without any fixed infrastructure. These wireless devices communicate with each other directly if they are in the same network coverage area. If they are out of the coverage range, the communication will require the formation with the help of cooperatives. Consequently, each node operate as a host and router as well. Due to these characteristics they are used in many critical applications such as disaster relief, emergency operations, vehicular computing, situational information in the battlefield, mobile offices and many more. In MANETs, one of the most challenging tasks is the security.

Open medium, dynamic topology, distributed cooperation, and constrained capability, MANETs are liable to suffer from security attacks. Hence, various attacks of different layers may affect the network. One of the most prominent attacks in MANETs is the Black hole attack, which can be easily instigated on reactive routing protocols like AODV or Dynamic Source Routing (DSR). In this attack, a malicious node can magnetize all data packets by falsely claiming a fresh route or shortest route to the destination, without having any active route to the specified destination, and then absorbs them without forwarding it to the destination node.

The aim of this paper is to overcome the black hole attack. Therefore, the proposed new approach is to eradicate one or more black hole attack on AODV routing protocol. In our approach, the intermediate node forwards the valid route reply to the next node. The invalid routes replies are avoided by intermediate nodes in the overall network.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

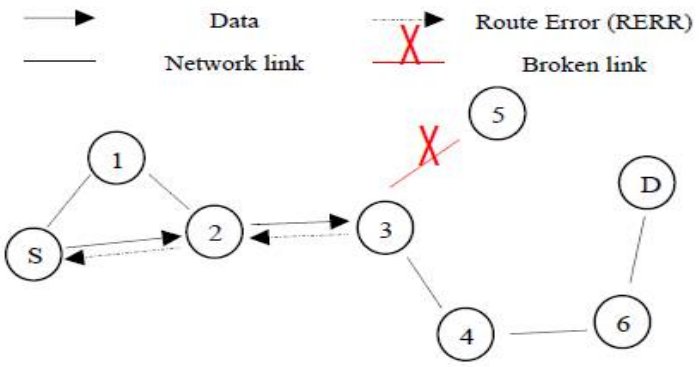


Fig.1 Route Maintenance Process of AODV

II. AODV ROUTING PROTOCOL

Ad-hoc On-Demand Distance Vector (AODV) protocol establishes routes only between nodes that need to communicate each other. The routing message does not contain any information about the whole route path, but only about the source and the destination information. In fact, the routing message does not have an increasing size. It uses Source Sequence Number (SSN) or the Destination Sequence Number (DSN) to specify how the route is newer.

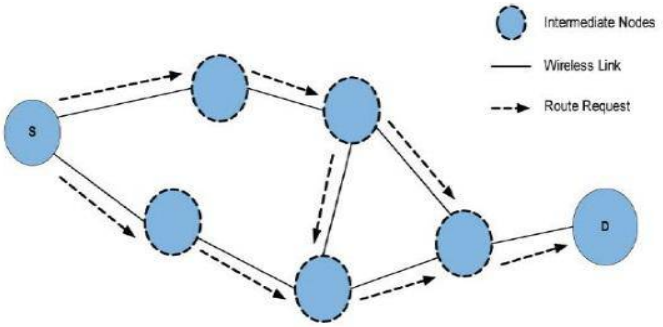


Fig.2 (a) RREQ Message

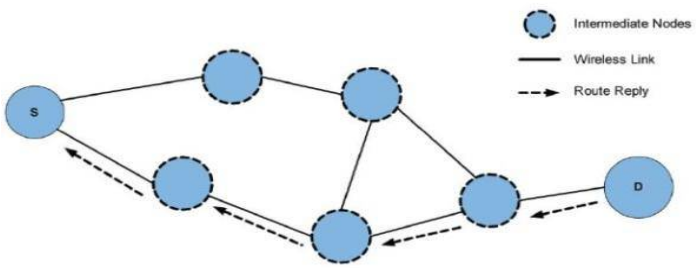


Fig.2 (b) RREP Message

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

The following subsections describe how routes are established and maintained in MANETs. Neighbor connectivity is established with periodic Hello Messages. Routes are found by flooding of Route Request (RREQ) messages as shown in Figure 2(a). Each node receives and retransmits the RREQ and it enters the previous hop count value in its routing table. In AODV, when a source node S is in need to send a data packet to a destination node D and does not have any route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors.

A timer call RREP_WAIT_TIME get started when the RREQ is been sent. The immediate neighbors who receive RREQ message it rebroadcast the same RREQ to neighbors. This process is repeated until the RREQ reaches the destination node. On receiving the first arrived RREQ, the destination node sends a route reply (RREP), as shown in Figure 1 (b), to the source node through which RREQ arrived. The destination node will ignore the RREQ that arrives after the timer expires. In addition, AODV enables intermediate nodes that have sufficiently fresh routes to generate and send an RREP to the source node. Once the source receives the first RREP message, it starts the data transmission along the path traced by the RREP packet.

Table 1. RREQ message format

Type	Flags	Reserved	Hop count
RREQ (Broadcast) ID			
Destination IP address			
Destination sequence number (DSN)			
Source IP address			
Source sequence number (SSN)			

AODV provides a rapid, dynamic network connection, featuring low processing loads and low memory consumption. AODV uses a node sequence number to clarify whether the routing message is fresh or not. Node sequence numbers serve as time stamps. However when a node sends any type of routing control message such as RREQ and RREP it increases sequence number.

Maximum sequence number indicates that the fresh route to the destination can be established over this node by other nodes. Routing messages in a network is divided into

- Path discovery and
- Path maintenance messages.

Path discovery is done using RREQ and RREP, while path maintenance is done using Route error (RERR) and

Table 2. RREP message format

Type	Flags	Reserved	Hop count
Destination IP address			
Destination sequence number (DSN)			
Source IP address			
Source sequence number (SSN)			

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Hello messages. Since the RREQ and RREP have significant involvement in the modified routing protocol, their formats are shown in Table 1 and Table 2, respectively.

When a new route is available, the routing table is updated only if route possess larger destination sequence number or same destination sequence number with smaller hop count to destination node.

III. BLACK HOLE ATTACK IN AODV

A black hole attack is one of the active DoS attacks in MANETs [6]. In this attack, a malicious node may advertise a fresh path to a destination during routing process. The intention of the node is to disturb the path thereby posing itself as a destination node or interpret the packet being sent to destination. For instance, the attacker can send a fake RREP to the source node, claiming that it has found a fresh route to the destination node. This makes the source node to select the route that lead to the attacker.

Therefore, all traffic routes towards the attacker, and therefore, the attacker can misuse or break the traffic. Since AODV treats RREP messages having higher value of destination sequence number to be fresher ever, the malicious node will always send the RREP with highest possible value of destination sequence number. Such RREP message, when received by source node is treated a fresh route. An example of black hole attack is shown in Figures 3(a) and 3(b) in which nodes S and D represent the source and the destination nodes respectively.

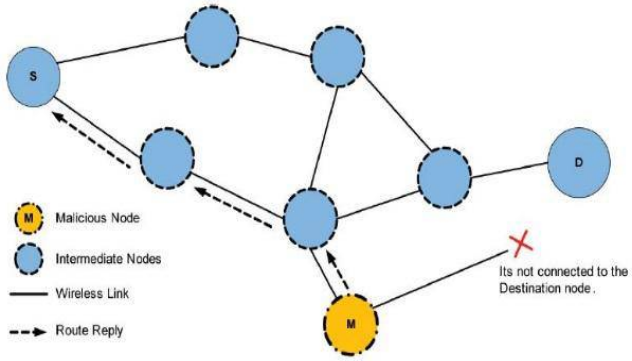


Fig.3(a) A malicious node sending false RREP to the ource node

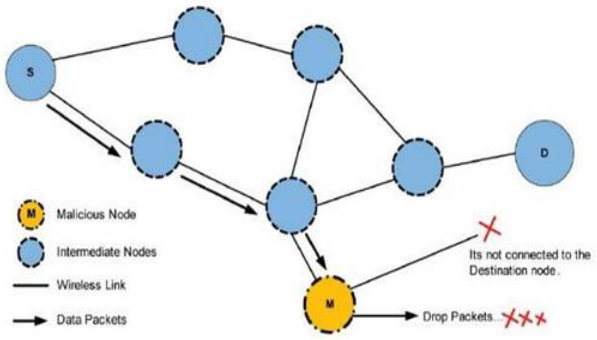


Fig. 3(b) A malicious node dropping data packets as the source node is unaware

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

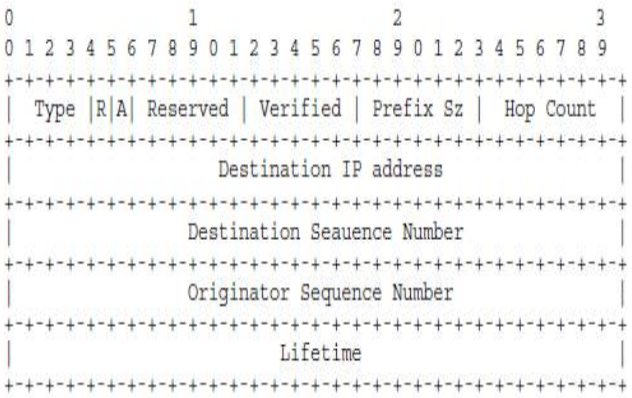
Node M is a malicious node which replies RREQ, a false response shows a shortest route to the destination node. Therefore, source node S erroneously judges the route discovery process when completion, and starts sending data packets to malicious node M. As mentioned above, a malicious node probably drops or magnetizes the packets. This malicious node can be regarded as a Black Hole problem in MANETs.

IV. ATTACK PREVENTION

We describe in detail of our proposed solution to prevent the black hole attack which we have encounter in AODV routing protocol. Therefore, we made a significant modification in recvReply(Packet *p), recvRequest(Packet *p) procedures and the Route Reply (RREP) message as shown in the following.

Table 1 illustrates the fields of RREP message. According to the original AODV routing protocol, the source node will broadcast the RREQ packet to check for fresh path to reach the destination node. The destination node, or any intermediate node on the path, can send reply to the source node. By default, the source node accepts the pretty fresh enough RREP coming to it.

In this approach, in standard AODV routing protocol, the destination node or intermediate node generates the RREP, but it generates another RREP too. It is an event of confirmation of the first reply with a sequence number incremented by one.



Format of the modified Route Reply (RREP) Message

V. EXISTING SYSTEM

Wireless Network Area has been threatened by a lot of security attacks such as denial of service attack, modification, IP spoofing, fabrication attack, etc. The black hole attack has a serious impact over reactive routing protocols. In Black hole attacks, a node sends a malicious broadcast informing that it has the shortest path to the destination. In this case, a malicious node (so-called Black hole node) attract all packets by using forged Route Reply (RREP) packet to falsely claim that “fake” shortest route to the destination and then discard or obtain those packets without forwarding them to the destination. For all of this the entire network's Security is poor and Performance is low.

Mobile Ad hoc Network is threatened by a number of security attacks such as denial of service attack, modification, IP spoofing, fabrication attacks, etc. As a result, a lot of research has been gone through this area. Many of researches have been conducted to design techniques for intrusion detection systems to identify the black hole attack. However, there are methods that are used to mitigate and resolve the black hole attack.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

TABLE I. FIELDS OF RREP MESSAGE

Type	Forced to 2.
R	Repair flag; used for multicast.
A	Acknowledgment required.
Reserved	Sent as 0; ignored on reception.
Verified	One bit specifies the packet Route Reply if it is valid or not as illustrated below: 0 refer to the invalid RREP 1 refer to the valid RREP
Prefix Sz	If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination.
Hop Count	The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP.
Destination IP address	The IP address of the destination for which a route is supplied.
Destination Sequence Number	The destination sequence number associated to the route.
Originator Sequence Number	The IP address of the node which originated the RREQ for which the route is supplied.
Lifetime	The time in milliseconds for which nodes receiving the RREP consider the route to be valid.

TABLE II. SIMULATION PARAMETERS

Parameter	Value
Coverage Area	500x500 m
Number of nodes	25
Simulation time	200s
Transmission range	50m
Mobility model	Random way point
Data Rate	0.25
Packet Size	512 Bytes
Routing Protocol	AODV / Modified-AODV
Mobility speed	0-30 m/s
No of black hole nodes	1 and 5
Connections	5
Traffic type	UDP–CBR
Pause time	10s

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

VI. PROPOSED METHODOLOGY

The proposed approach focuses on attack free wireless communication medium with the help of Modified AODV Protocol. The proposed protocol determines two main functionalities:

- Route Discovery
- Route Maintenance.

In proposed approach, the Source Node sends Route REQuest (RREQ) to nearby node. The nearby node checks it and forward Route REPly (RREP) to Source Node. Neighbor node sequence Number will incremented by count 1. If only the node is valid the count will be incremented otherwise it is considered to be an attack. Selecting Neighbors is based on Shortest Path, so the performance is good as well.

The proposed project mitigates the black hole attack thereby blocking the malicious node intrusions as well as fake destination. Fake destination works for malicious node, it is a cooperating node. Routing table is maintained to update the nodes details like hop count, sequence number etc.

Each routing table entry has:

- Destination IP address
- Next hop
- Number of hops
- Destination sequence number
- Active neighbors for this route
- Expiration time for the route table entry

The data transmission is done in secured manner so data security and data integrity is maintained. To maintain data integrity we include the powerful and efficient data cipher algorithm called Advanced Encryption Standard (AES) is implemented. It provides the safe secure successful communication between source and destination which is done in second phase of work and we have intended to provide the multicast communication between source and multiple destinations.

Algorithm 1: Attack Finding Algorithm

Step 1: (Initialization Process)

Start the route discovery phase with the source node S.

Step 2: (Generation of RREPs)

The destination node or the intermediate node generates two route reply with two different destination sequence number, the second one must be incremented by one.

```
sendReply( seqno, // Dest Sequence Num
VERIFIED = 0, ); // Appended field
sendReply( seqno+1, // Dest Sequence Num
VERIFIED = 0, ); // Appended field
```

Step 3: (Verification of RREPs)

```
if ( intermediate node receives RREP ){
if ( the first time the node receives RREP ){
Store the IP address and seqno of the node;
if ( RREP is valid){
Forward RREP; }
} else if (the node receives more than one RREP ){
Store the IP address and seqno of the node;
if ( RREP is invalid){
if ( new RREP's seqno == old RREP's seqno + 1){
VERIFIED = 1; //( Mark RREP as valid)
Forward RREP;
```

Step 4: (Continue default process)

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

VII. LITERATURE SURVEY

In the year of 2007, the authors J., Wu, J., & Cardei, M proposed a paper titled "A survey of attacks and counter measures in mobile ad hoc networks" is discussing the importance of Security, is an essential service for wired and wireless network communications. The success of mobile ad hoc network (MANET) will depend on people's confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation.

First, we made an overview of attacks according to the protocol layers, and security attributes and mechanisms. We also put forward an overview of MANET intrusion detection systems (IDS), a reactive approaches to thwart attacks and used as a second line of defense.

In the year of 2012, the authors Jhaveri, R. H., Patel, S. J., & Jinwala, D. C, proposed a paper titled "DoS attacks in mobile ad hoc networks: A survey", has a description such as MANETs have unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration, as a result, they are vulnerable to various attacks in different layers of protocol stack.

Each node in a MANET is capable of acting as a router. Routing is one of the aspects having various security concerns. In this paper, we made a survey of common Denial-of-Service (DoS) attacks on network layer namely Wormhole attack, Black hole attack and Gray hole attack are serious threats for MANETs. We will also discuss some proposed solutions to detect and prevent these attacks. As MANETs are widely used in many vital applications, lots of research work has to be done to find efficient solutions against these DoS attacks that can work for different routing protocols.

In the year of 2015, the authors Khatri, S., Sharma, P., Chaudhary, P., & Bijalwan, A, proposed a paper titled "A Taxonomy of Physical Layer Attacks in MANET", described Mobile ad-hoc networks (MANETs) are a key enabler of pervasive computing. Constrained resources in mobile stations make it critical for nodes to be able to cooperate, enhance communication computation capabilities.

However, the wireless and dynamic nature of the links is easy attack vectors for adversaries. The ability to securely discover and identify neighboring nodes (secure ND) is a fundamental building block for such networks. Even a relatively weak adversarial relay has the capability of distorting the network view and diverting significant amount of traffic. This can cause significant performance degradation. In this paper, we utilize the physical layer authentication scheme introduced by Yu, Baras and Sadler to secure neighborhood discovery against adversarial relays.

VIII. EXPERIMENTAL RESULTS

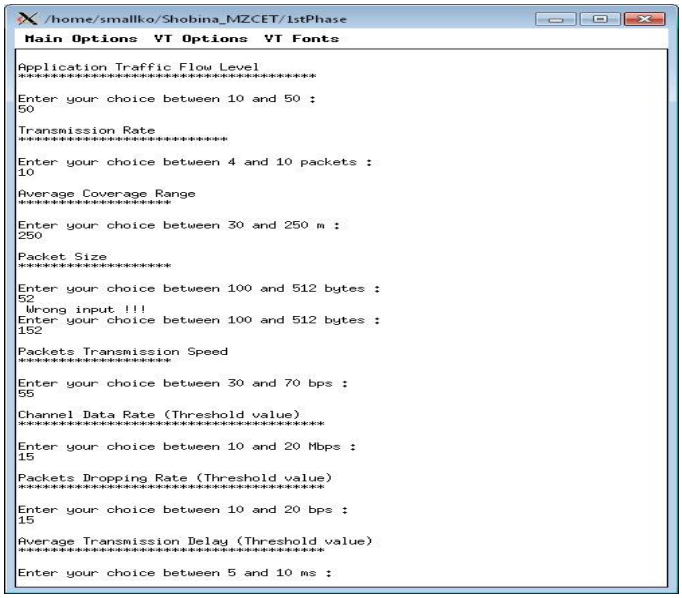


Fig.6 Input Parameters

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

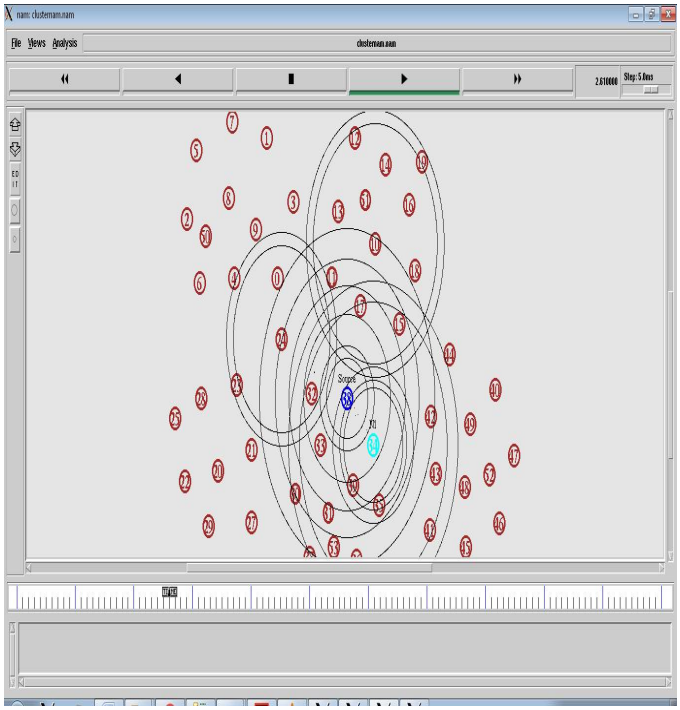


Fig.7 Nodes Establishment

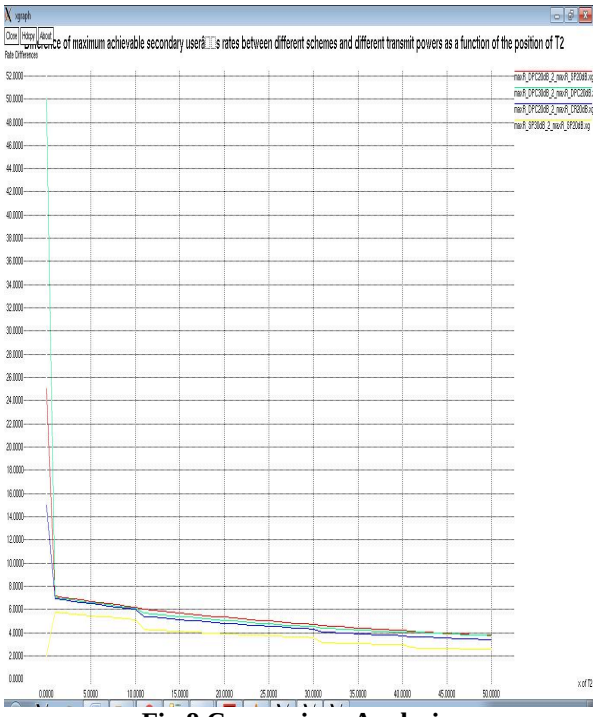


Fig.8 Comparison Analysis.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

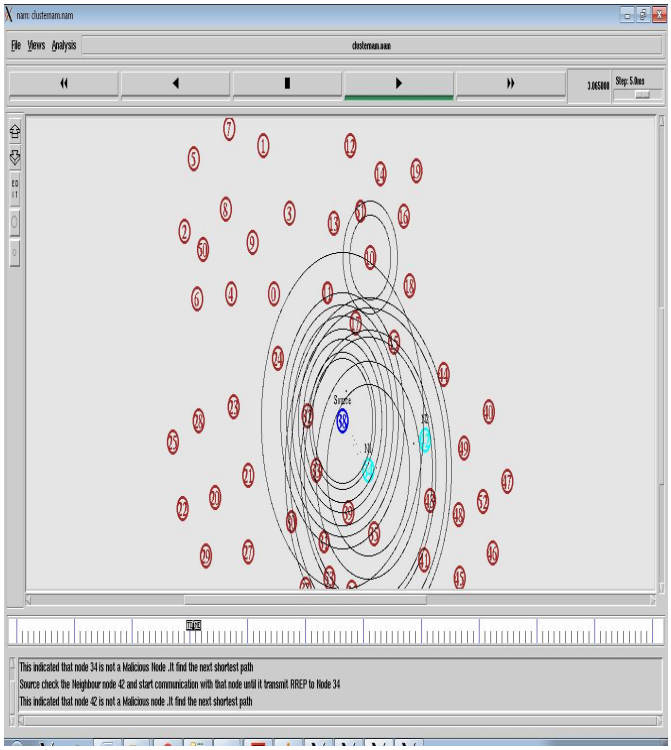


Fig.9 Communication

IX. CONCLUSION AND FUTURE SCOPE

Ad hoc routing protocols are prone to various attacks because of their ignorance in security aspect during their designs. A black hole attack disrupts normal network functionality by sending bogus routing information during route discovery phase. In this paper, we proposed a solution to avoid the black hole and the multiple black hole attackers on the AODV routing protocol in MANETs. According to the simulation results, the modified AODV gives significant improvement in packet delivery ratio with acceptable average end-to-end delay and normalized routing overhead when the mobility of nodes increases. Consequently, we concluded that our proposed approach shows superior performance than the AODV in the presence of one or multiple black hole nodes.

REFERENCES

[1] Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security (pp. 103-135). Springer US.
[2] Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012, January). DoS attacks in mobile ad hoc networks: A survey. In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on (pp. 535-541). IEEE.
[3] Khatri, S., Sharma, P., Chaudhary, P., & Bijalwan, A. (2015). A Taxonomy of Physical Layer Attacks in MANET. International Journal of Computer Applications, 117(22).
[4] Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual Southeast regional conference (pp. 96-97). ACM.
[5] Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).
[6] Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In Mobile computing (pp. 153-181). Springer US.
[7] Patel, A. D., Jhaveri, R. H., & Shah, S. N. (2015). I-EDRI Scheme to Mitigate Grayhole Attack in MANETs. In Intelligent Computing, Communication and Devices (pp. 39-43). Springer India.
[8] Marttinen, A., Wyglinski, A. M., & Jantti, R. (2014, October). Movingtarget defense mechanisms against source-selective jamming attacks in tactical cognitive radio MANETs. In Communications and Network Security (CNS), 2014 IEEE Conference on (pp. 14-20). IEEE.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

[9] Gharehkoolchian, M., Hemmatyar, A. A., & Izadi, M. (2015). Improving Security Issues in MANET AODV Routing Protocol. In Ad Hoc Networks (pp. 237-250). Springer International Publishing.
[10] Dorri, A., & Nikdel, H. (2015, May). A new approach for detecting and eliminating
cooperative black hole nodes in MANET. In Information and Knowledge Technology (IKT), 2015 7th Conference on (pp. 1-6). IEEE.

BIOGRAPHY

Mrs. Shobina. K. Studying M.E. Computer Science and Engineering in Mount Zion College of Engineering and Technology, which is located in Lena Vilakku, Pudukkottai, Tamil Nadu, India.