Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9, August 2021: 537-549

an approach based on secure mobile ad-hoc network

Amit Kumar, Vatsal Kejriwal, Rakesh Ranjan

Department of Engineering Himgiri Zee University Dehradun,India

Abstract - In coming future, Mobile Ad Hoc Network (MANET) is going to lead the world in Wireless Technology. MANET consists of group of communication devices or nodes. These nodes desire to communicate without the help of any fixed arrangement and predefined association/structure of available links. In a MANET if mobile node keeps on increasing and moving simultaneously then it will attract the intruders in a form of malicious nodes, This is the biggest security challenge in any Mobile Ad Hoc network. Black Hole attack is one of them, here in this paper we are discussing about this threat and the security concern to overcome this problem with the help of routing protocol used in MANET.

Keywords - Mobile ad hoc network (MANET); Black hole; routing security; NS2 simulation.

I. INTRODUCTION

A group of mobile unit referred as nodes. These nodes form the Mobile ad-hoc networks (MANET). Every node in MANET plays a role of either **host** or **router**. These are wireless hosts that communicate with each other. The communication takes place without the existence of fixed infrastructure and a central control.

The MANET is user friendly as in the network nodes can freely move in any direction. Also within a short span of time it can be turn upside down. In this technology the existing mobile nodes are interconnected through the wireless link. The interconnections are among the nodes that agree to unite and forward packet among each other. In the mobile Ad-Hoc network, these nodes create routes dynamically among themselves.

In this way they form their own wireless network on the fly. The Figure 1 shows a simple Ad-Hoc network model. There are three nodes.

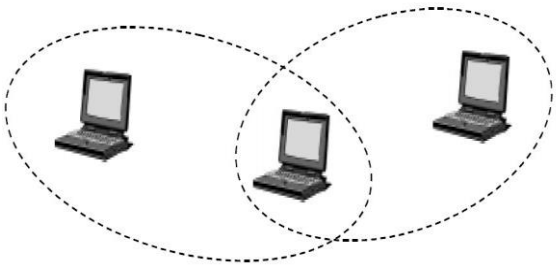

Fig1. A Simple Ad-Hoc network with three participating nodes.

All these nodes form an Ad-Hoc network. The outermost nodes are not inside transmitter range of each other. The central node can be used to onward packets between the both outermost nodes. Thus the middle node behaves like a router. No centralized administration or control is required by an Ad-Hoc network.

Since one of the mobile node moves from the transmitter range, as a result the network never fails. Nodes can be able to arrive or leave the network. Due to inadequate transmitter range of nodes, several hops are required to reach from one node to another. In this way every node acts both host and router. A node can be considered as an abstract entity enclosing a router and a set of associated mobile hosts as depicted in figure 2. A router is an object or device. The routing protocol is executed at this device. In the old logic, a mobile host is just supposed to be an IP-addressable host.

In order to handle topological changes and faults in nodes Ad-Hoc network are also accomplished. This can be fixed through network reconfiguration. Link damage may occur because of moving of a node from one network to another. Unfortunately if such damage occurs then the affected node requests for new route and thus the problem will be resolved. Off course due to this the delay will faintly increase. But the best thing is that the network will still be operative.

MANET also takes the benefit of the properties of the wireless communication medium. Wired network is made of physical medium. This is established thru priori curbing the connection topology of the nodes. This type of restrictions never occurs in the wireless communication. Two nodes are provided within the same transmitter range of each other [17-18]. Thus a rapid link may get form between them.

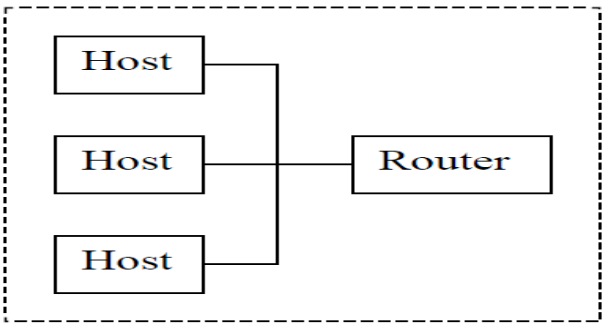

Fig. 2. Block diagram of mobile node acting both as hosts and a router [16].

II. LITERATURE REVIEW

Soufine Djahel, Farid Nait-Abdesselam and Ashfaq Khokhar proposed solution [3] to deals with the cooperative black hole attack an acknowledgement based on the alleviate the damage of topology evidence due to the releasing of topology control (TC) message by aggressors. In accumulation to the unique control message of OLSR are Hello and TC messages. They had introduced two different types of control packets. They are named as **3hop_ACK** and **HELLO rep**.

The “HELLO” rep message is used by a node to advertise its two hop neighbors to an entreating multi point relay (MPR) node. The 3hop_ACK message is used to acknowledge its reaction of a TC message by a node from the neighbor three hops away. For the request, they utilize one of the vacant

bits in the HELLO message. This is to verify whether the sender's MPR nodes had produced the "HELLO" packet or not.

In RIT algorithm every node maintains three bit information. Out of the three bit the first two bit is discuss earlier but the last one bit is represented by "through any trustful node". This last bit is set only if any trustful node has routed the data packet through the node.

But the reliability checking of node is based on intermediate nodes. These nodes generate the RREP. The RREP provides the information about Next hopping node (NHN) and RIT entry for the NHN. Source node will check its own RIT to see whether IN is unreliable. The source node send Additional request (ARq) message to next hop node.

Ankur Mishra et.al had suggested the solution of this problem. The check bit was used to find the trusted source node as well as one trusted destination node (CN) with their respective demand routing information table (DRI). The source node sends prob. packet 2 through remaining suspected node to that trusted node. Then it receives the TTL value OF FIRST PROB PACKET. Once it is received, the source node SN enquires the trust node (CN) whether it has received prob. packet 2 or not. If packets were not received then the source node has to send another PROB PACKET 2 to CN. If any one of two PROB PACKET is received, then we consider this as another trusted source node and mark an entry under check bit as '1'for this node. Eventually if the packet is not received, then the source treats them as "black hole node" and maintains the identity of such node as **MALI_** node. Thus in future it can discard any control messages coming from such node. The intermediate node echoes the RREQ message. RREQ is used to check whether routes between the intermediate node and the destination node exist or not.

```
IF (route exists between the intermediate nodes) THEN
{
    Trust the intermediate node;
    Send the data packet;
}
ELSE
{
    Source node just discards the reply message;
    Send out alarm message to the network;
    Isolate such node from the network.
}
```

Suparna biswas et.al suggested a solution for the prevention of black hole. The suggestion was to use the average value for parameters like- rank, velocity, and battery power. Then select a higher trust value among all the available routes. These trust values are compared. The route having highest

average trust is selected for packet transmission. After completion of packet transmission, the destination node sends an acknowledgement to source the node. Which in turn increments the rank and also

decrements the battery power of each node in that route.

Tamilselvan L et.al has suggested a Time-based Detection system. This is based on the original AODV routing protocol. In this system a timer is set in the Timer Expired Table (TET). It collects the further request send from nodes. Once it gets the first request, it will store the packet's sequence number and the packet receiving time in Collect Route Reply Table (CRRT). Timeout value is computed with respect to the incoming time. The selection of the appropriate route is absolutely based on the above threshold value.

Jaydip Sen et.al. suggested another solution. Their algorithm for defending against a cooperation black hole by introducing two concepts: data routing information (DRI) table and cross checking.

In their first algorithm, each node maintains a DRI table assigning two bit 1 or 0. 1 stands for true and 0 for false. First bit "from" stand for the information on routing data packet from the node. Second bit "through" stand for information on routing data packet through the node. While in cross checking it further uses request (FREQ) and reply (FREP). If there is no route entry for the source node, a RREQ message is broadcasted. This is done to find a secure route between the source and destination node. Once the route is establish, the destination node replies all intermediate nodes. In turn these intermediate nodes update and insert routing entry for that destination node as a trust destination. Source node also trusts on destination and they will start transporting data packets through the designated route. The source node updates the DRI table for this path.

III. PROBLEM STATEMENT

A. Black hole attack

Routing protocol has bare variety of attack. Black hole attack [1] [6] is denial of services (DOS) attack in MANET. Black hole attack is a type of active attack in which the malicious node takes the benefits of the liabilities of routing protocol. During the route detection and maintenance progression, a malicious node misleadingly broadcasts a fake RREP packet through the shortest path. When the source node receives this RREP packet, it starts sending a data packet to the malicious node. This malicious node engages these entire data packet and drops them fully or sometimes partially. When another RREP packet reaches from another route to the source node then they discard that RREP packet. So that source and destination node will not be able to communicate with each other.

There are two types of Black hole attack:-

1. Single Black Hole
2. Cooperative Black Hole attack

a. *Single Black Hole attack*

It is the simplest form of black hole attack. In this attack only one malicious node is used to perform attack. The malicious node advertises itself as a node of shortest path from the source to the destination. When the packet reaches at it this node, it simply discards the all packets. The fig. 3 depicts the concept of Single Black Hole attack.

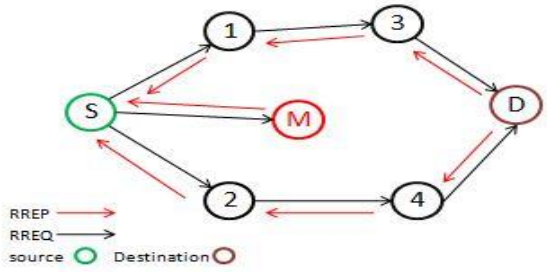

Fig. 3. Single Black hole attack.

b. *Cooperative Black hole attack*

In *Cooperative* black hole attack there is more than one malicious node. These malicious nodes send a false RREP packet to the source node that has started route detection. It does so to spectacle itself as a destination node/ intermediate node. This malicious node absorbs or drops packets. In this way entire packets are lost that was sent from the source node. Often these malicious nodes cooperate with each. Their aim remains the same of dropping packets. This why these nodes are known as cooperative black hole nodes [13] and this phenomena of attack is known as **Cooperative Black Hole Attack**.

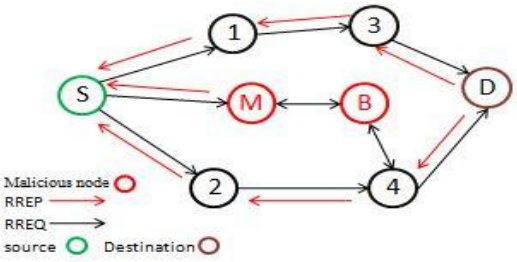

Fig. 4. Cooperative Black Hole Attack.

In the fig 4 source node S desires to transmit a data packet to the destination. In this progression it first broadcast the RREQ packet to the neighboring nodes. Unfortunately this RREQ packet is also fetched by the (Black hole node) malicious nodes since this is also a part of the network. The RREP packet from the malicious node ‘M’ reaches to the source node. It starts sending data to this malicious node ‘M’ and another RREP packet. These packets reach later from different route they discard it. The malicious node ‘M’ drops or absorbs all data packets which were transported to the destination ‘D’ by the source node ‘S’. This situation arises only when single malicious node had occurred in the network.

This problem becomes more critical when multiple black hole nodes are active in cooperation with each other. ‘M’ the first black hole refers to its partner ‘B’ as next hop. The source node ‘S’ sends further request to ‘B’ through a different route (S, 2, 4, B) other than via ‘M’. Node ‘S’ asks ‘B’ whether is there any other route between ‘M’ and destination node ‘D’. Because ‘B’ is cooperating

with ‘M’ its further reply is ‘yes ‘for both questions. Source node ‘S’ start sending packet assuming route (S,M,B) is secure but the packet are dropped by node ‘M’.

B. MANET routing protocol

In order to find shortest path in the network (route), MANET routing protocols is used. Due to the random and rapid motions of nodes, MANET helps to find new route. The new route can be found with the help of several protocols.

These routing protocols are:- Proactive, Reactive and Hybrid [12]

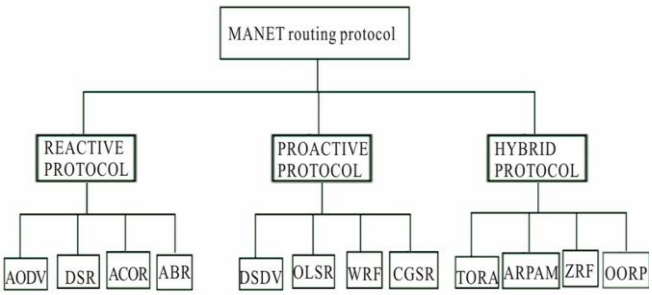

Fig. 5. Routing Protocol [15]

a. Proactive routing protocols

Proactive routing are the table-driven routing protocols. In this protocol each of the nodes maintains a routing table (RT). The RT contains record of adjacent nodes as well as reachable node. RT also contains the number of hops. The overhead increases in contrast with the increase in size of the network. There are many types of Proactive routing Protocol. They are mentioned in below:

i. DSDV

ii. OLSR

iii. WRF

iv. CGSR

b. Reactive routing protocol

Reactive routing protocol is also called On-demand routing protocols. In this protocol the correct routing information are not maintained on all nodes at all time. Rather the routing information is collected only depending on the needed. To resolve the route, the route queries are sent throughout the network. This routing protocol is categorized into following way which is mention below:

i. AODV

ii. DSR

iii. ACOR

iv. ABR

c. Hybrid routing protocol

In Hybrid routing protocol, there is tradeoff between proactive and reactive protocol. Proactive protocols have a large overhead and less latency. On the hand reactive protocols have less overhead and more latency. Thus a hybrid protocol is presented to overcome the shortcoming of both proactive and reactive routing protocols. Hybrid routing protocol is the combination of both proactive and reactive protocol. It is classified into:

i. ZRP

ii. TORA

iii. ARPAM

iv. OORP

MANET technology is a dynamic topology. At any time any node can easily join or leave the network. Many security issues also arise if the mobile Ad-Hoc networks used in critical operations. So the ultimate goal is to protect communication between mobile nodes in an argumentative environment. There are a few protocols to tackle this situation in order to establish proper communication. These are mentioned below.

AODV, DSR, DSDV and ZRP.

d. Ad-Hoc on demand distance vector (AODV)

AODV (Ad-hoc on demand distance vector) [13] routing protocol is a reactive routing protocol. It is the most widespread used routing protocol. It is intended for Ad-Hoc mobile network. It is an on-demand algorithm. Whenever any source node desires to transmit a packet, the route is established. It means routes are established on-demand. AODV is suitable for both unicast as well as multicast routing. This process is accomplished with route discovery mechanism which source node S sees its routing table if a valid route entries is found toward the destination D then source node S send the data to a given destination node D , else it initiate a route discovery procedure which source node broadcasting a Route Request(RREQ) message to the neighbor. When a RREQ is receiving by any intermediate node they finally see its routing table to find a fresh route toward the requested destination in RREQ. If such a route is obtain a route reply (RREP) is unicast toward a source via intermediate node. If intermediate node doesn't obtain a fresh route its update its routing table and send RREQ to these neighbor. This process is repeated until RREQ accomplish the destination node D and they all have successful route from source to destination.

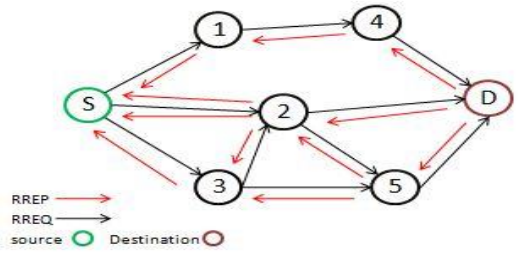

Fig. 6. Route discovery process under AODV.

e. Dynamic source routing (dsr)

Dynamic source routing (DSR) is a reactive routing protocol. This is based on a method known as source routing. This is also called on-demand protocol. No routing information is maintained by these protocols. Hence there is no requirement of maintaining or updating routing table. Mostly DSR is designed for the use of Multi-hop Ad-Hoc network of mobile node. This is suitable for the small diameter network in which route discovery is initiated by the sources only on-demand basis. The sender determines the route from source to destination and it includes the address of intermediate node to route record in the packet. This process is done with the use of the cache technology to maintain the routing table. There are two phase in DSR:

A. Route discovery

B. Route maintenance.

The node first checks its route cache. Then source node sends the packet through the route to the destination node. Otherwise route discovery process are initiated the by broadcasting route. This is done to know the route dynamically in the network.

f. Zone routing protocol (ZRP)

ZRP is a type of hybrid routing protocol [10]. This protocol distributes the whole network into several routing zones. It then postulates them into two separate protocols that work inside and between the routing zones. There are two types: Intrazone (IARP) and Interzone (IERP). The IARP operates inside the routing zone. It provides route to all the nodes within the zone. It also acquires the smallest space for them.

IV. PROPOSED METHODOLOGY

The proposed solution is- The requesting node do not sent the DATA packets to the reply node at once. The node has to wait till other replies with next hop details from the other neighboring nodes. Then following actions are performed.

I. The timer is set (“Timer Table” of the node) after the first request is received from the neighbors. This is done in order to collect the further requests from different nodes.

II. It stores the ‘sequence number’, of RREP.

III. It also preserves the packet arrival time. The time for which every node will wait is proportional to its distance from the source.

IV. The ‘timeout’ value is computed based on arrival time of the first route request.

V. After the timeout is computer, it checks in Route Reply Cache Table (RRCT), whether there is any repeated next hop node or not.

IF(Repeated next hop is present in the reply paths)THEN

{

It accepts the path that is correct;

Any one of the path is selected with the repeated node to transmit the DATA packets;

}

ELSE

{

Random route is selected from RRCT (The chance of selection of malicious route is reduced);

}

The proposed solution is illustrated in the below figure 7.

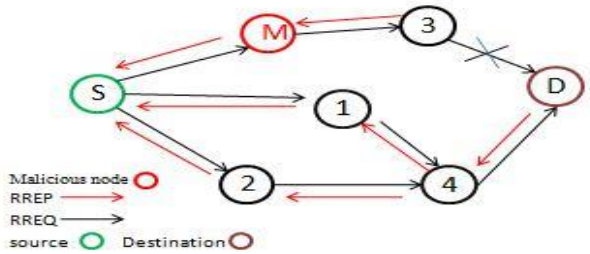

Fig. 7. Black hole attack solution.

A. Working principle

In the above figure 7, the source node ‘S’ requires to transmit to destination node ‘D’. First of all It first the route requested is broadcasted to all our neighboring nodes. Here node ‘1’, node ‘M’ and node ‘2’ get this broadcast request. The malicious node ‘M’ has no intent to transmit the DATA packets to the destination node ‘D’. In reality it desires to intercept/collect the DATA from the source node ‘S’. Hence it immediately replies to the request as (M – 3). Instead of transmitting the DATA packets instantly through ‘M’, ‘S’ has to wait for the reply from the other nodes. After some time it will receive the reply from node ‘1’ as (1 – 4), and node ‘2’ as (2 – 4).

According to this proposed solution it first checks the path that contains repeated next hop node to the destination.

If there is no repeated node, it select random path and transmits the data through that path. The routing table from ‘S’ to ‘D’ is given in Table 1.

TABLE 1. ROUTING DETAIL

Source	Intermediate	Destination
S	M-3	D
S	1-4 2-4	D

B. Proposed Algorithm

Step 1:- Source node broadcast the route request (RREQ) to our neighbor's node to transfer data from source to destination.

Step 2:- The route reply (RREP) message is sent back by malicious node to the requested node. This is to articulate that I have shortest path towards the destination. (they have no information for destination).

Step 3:- source node check our routing table

IF (*Information occurs towards the destination through this intermediate node*) THEN
{
I. Transfer the data through this intermediate node.
II. This route is considered as a trustful route.
}
ELSE
{
I. They set a timer in timer table with "current time";
II. Set "sequence number";
III. Receive another RREP from different route;
}
IF (*RREP packet received a from different node*) THEN
{
I. Update our timer table to by updating a
"sequence number receiving time";
II. Find the highest sequence number;
III. Transfer data based on this sequence number;
}
ELSE
{
I. Set this timer as expired;
II. Maintain the routing table;
}

V. SIMULATION EVALUATION

Network simulator 2 (NS2) is an open–source event-driven simulator. This has been designed specifically for research in the field of computer communication networks. This is one of the most widely used network simulators. Since its interception in 1989, NS2 has continuously gained tremendous interest from industry, academia, and government. NS2 have been enhancement with constant and minute exploration for years. Presently NS2 comprises several modules for abundant network machineries such as routing, transport layer protocol, application, etc. NS2 has a special feature called an easy-to-use scripting language. This is very effectively used by the researchers. They can effortlessly configure the network. Thus it becomes very easy to inspect network

performance by examining the results generated by NS2. Undoubtedly, today NS2 has become the utmost extensively used open source network simulator.

In this solution we implement the black hole attack based on the secure AODV routing protocol (SAODV) with timer table and RRCT using this tool. The scenario is show in the below table 2.

TABLE 2. PARAMETERS USED DURING MANET SIMULATION

Parameter	Value
Nodes	20
Simulation Time	5M
Mobility	Random way point model speed – 30 m/s pause time – Node mobility varied between 10 S to 90 S
Load	300 items, Data Pay Load 512 byte, Inter departure Time
Coverage Area	800m*800m

A. Comparison with basic aodv

For the purpose evaluating the packet delivery ratio, 25 nodes have been taken to simulate. The source node transmits 300 packets to the destination node. Each packet is of 512 bytes length. It is transmitted with an interval of 1 second. We can easily observe in the figure 8 that in SAODV the packet delivery ratio is more compared to AODV. The mobility speed of nodes is indicated by Node Mobility. The packet ratio and node mobility are inversely proportional. This means if the packet delivery ratio will be very high only when the node mobility is very low. In other words when the node mobility is increased the packet delivery ratio is slightly decreased. The packet delivery ratio increases by using SAODV compare to

AODV till 70m/s node mobility.

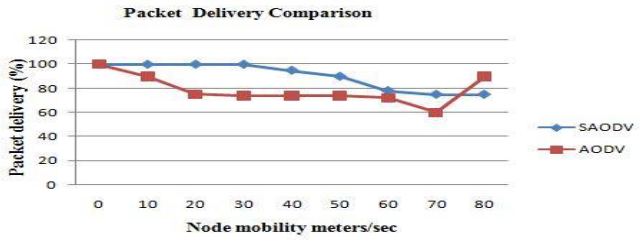

Fig. 8. Packet delivery (%).

Figure 8 shows the packet delivery ratio in the presence of malicious node. Consider Source 0 sends packet to Destination 7. Here assume 1 is the malicious node. In AODV the packet delivery ratio is reduced to 30%. But in SAODV the packet delivery ratio is around 80 to 100%. From this figure 8 it is clear that even when the malicious node is near the source SAODV give a good result.

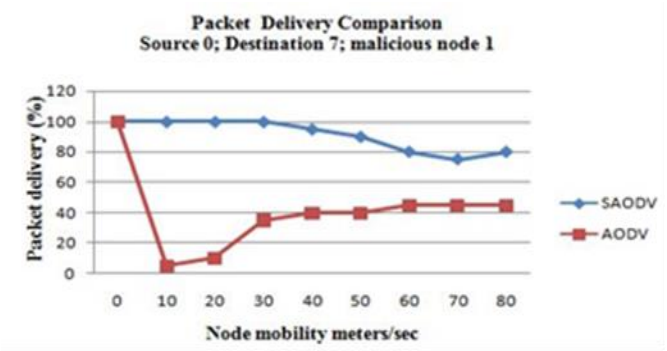

Fig. 9. Packet delivery (%) in the presence of malicious node near the source node

Figure-9 shows the packet delivery ratio in the presence of malicious node away from the source. Consider Source 0 sends packet to Destination 7. Here say 10 is the malicious node. In AODV the packet delivery ratio is increased to around 80%.

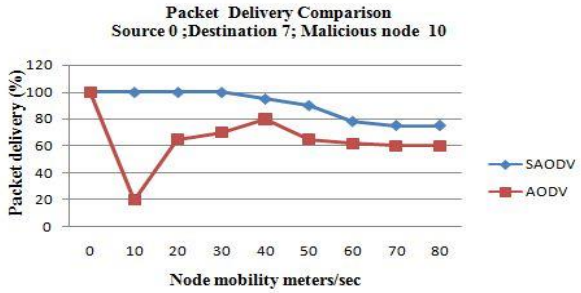

Fig. 10. Packet delivery (%) in presence of malicious node away from source node.

This is because before the reply from the malicious reaches the source, nearby node to the source transmits the reply. Again in SAODV the packet delivery ratio is around 90 to 100%. In the figures 9 & 10 it is clear seen that even thou if the malicious node is near or far from the source, SAODV give a good result compared to AODV.

VI. CONCLUSION

In MANET, the security threat is the major challenge. This mainly aims for the detection and prevention the malicious node from attacker. So here we can observe that attacker will attack through some malicious node. This attack has come under a black hole attack. This malicious node sends a fake RREP packet with higher sequence number. It then absorbs the entire data packet sent. So we can detect and prevent this black hole attack using various techniques such as route discovery process, cross checking and DRI and many more ways. This can be made possible with the help of AODV routing protocol. But at the same time detection and prevention arises some defect also. Due to this the packet delivery becomes low. Also it consume more time. These issues are solved with the help of timer based and RRCT to SAODV to delivery packet with correct route.

Future work: Future work should be focused on design of an algorithm for minimizing the delay. Also packet dropping ratio should be reduce and packet delivery ratio should be increased in case of

mobility of nodes in mobile Ad-hoc network. And also a great effort should be taken to enhance the efficiency of mobile Ad-hoc network.

References

[1] Yibeltal Fantahun Alem and Zhao Cheng Xuan, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", ",2nd International Conference on Future Computer and Communication , volume 3, 2010.

[2] Jaydip Sen , Sripad Koilakonda and Arijit Ukil, A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks, Second International Conference on Intelligent Systems, Modeling and Simulation, pp 338-343 , Jan 2011Campbell Scientifi c, Inc., April 2008.

[3] Soufine Djahel, Farid Nait-Abdesselam and Ashfaq Khokhar H. Yang, "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol", IEEE Communications Society, 978-1-4244-2075-9/08/ © ICC 2008.

[4] Ms. Gayatri Wahane and Ms. Savita Lonare " Technique for Detction of Cooperative Black Hole Attack in MANET", 4th ICCCNT ,IEEE- 31661 July 4-6, 2013, Tiruchengode, India.

[5] Kishor Jyoti Sarma, Rupam Sharma and Rajdeep Das "A Survey of Black Hole Attack Detection in Manet", 978-1-4799-2900-9/14/ ©2014 IEEE.

[6] Harsh Pratap Singh and Rashmi Singh "A Mechanism for Disco very and Prevention of Cooperative Black hole attack in Mobile Ad hoc Network Using AODV Protocol", Electronics and Communication Systems (ICECS),International Conference on Coimbatore ,IEEE, 13-14 Feb. 2014.

[7] Kriti Chadha and Dr. Sushma Jain "Impact Of Black Hole And Gray Hole Attack In AODV Protocol", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.

[8] Suparna Biswas, Tanumoy Nag and Sarmistha Neogy "Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET",Applications and innovations in mobile computing (AIMoC),IEEE, Feb. 27 2014-March 1 2014, Kolkata, India.

[9] Mangesh kumar S. Shegokar and R. R. Tuteja "Survey on Classified Ad-hoc Routing Protocols in MANET", International Journal of Science and Research (IJSR), Volume 3 Issue 4, April 2014

[10] Ankur mishra, Ranjeet Jaiswal and Sanjay Sharma "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network", 3rd IEEE International Advance Computing Conference (IACC) , 2013.

[11] Khushboo Sawant, Dr. M.K Rawat, "Survey of DOS Flooding Attacks over MANET Environment", Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 5(Version 6), May 2014, pp.110-115.

[12] Sunil J. Soni & Suketu D. Nayak "Enhancing Security Features & Performance of AODV Protocol under Attack for", International Conference on Intelligent Systems and Signal Processing (ISSP) 978-1-4799-0317-7/13/2013 IEEE

[13] Latha Tamilselvan & Dr. V Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol. 3, No. 5, May 2008 Academy Publisher.

[14] Stallings William(2000), network security essentials : applications and standards; Pearson education

[15] Stallings William (2003), cryptography and network security principles and practices; Pearson education 3rd edition.

[16] Sarvesh tanwar, Prema k.v ," threats & security issues in ad hoc network: a survey report", International journal of soft computing and engineering (ijsce) ISSN: 2231-2307, volume-2, issue-6, January 2013.

[17] Verma PR, Singh DP, Goudar RH. Power Efficiency with Localization for Tracking and Scrutinizing the Aquatic Sensory Nodes. InIntelligent Computing, Communication and Devices 2015 Jan 1 (pp. 661-673). Springer India.

[18] Pushpendra R. Verma, D. P. Singh et al., "Localization and Minimization of Power Consumption of Sensory Nodes with DOA Technique Deployed in Hazardous Chemical Plume Area," in Proc. International Conference On Emerging Research In Computing, Information, Communication and Applications, Volume 1, 2014, ISBN-9789351072607.