International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

DRI-Based Implementation for Detecting and Eliminating Cooperative Black Hole Nodes in MANET

Deepak Sharma

Abstract: ***Mobile Ad hoc Networks is configured by itself using the Mobile nodes in the Network, the maintenance also done by the wireless nodes itself. Dynamic topology, hop-to-hop communication and open-to-all are the features of MANETS, but these features made security of network highly challengeable. From security concern, routing protocols are highly vulnerable to many security threats like black hole attack. In black hole attack malicious node generates false routing information to the path requests about the route it asked for, which results all data packets forward toward it-self by the source and the black hole node manipulate its data. The cooperative black hole nodes in the other hand cooperate within the malicious nodes to fool the single black hole attack prevention algorithms. Here an approach is proposed to detecting the cooperative black holes nodes and eliminate them by broad casting there information into the network.***

Keywords: Mobile Adhoc Network (MANET), AODV Protocol, Black Hole, cooperative black hole.

I. INTRODUCTION

This section is focusing on the basic introduction of MANET, black hole attack and cooperative Black hole attacks. Wireless mobile ad hoc network (or simply MANET) is a type of network which configures itself by using pro-active routing algorithms, and they are wholly depends on the node joined the network, the nodes joins the network are not authenticated because there is no centralized system to do so. The mobile nodes in the network communicate with each other without any infrastructure, also, all of the transmission links are established through wireless medium. MANETs are widely used in Defence purpose, disaster affected areas, personal network areas and many more. However, there are still many open problems in MANETs, such as security problem, finite transmission bandwidth, abusive broadcasting messages, reliable data delivery, dynamic link establishment and restricted hardware caused processing capabilities.

The security hazards have been widely discussed in the wired and wireless networks and many of them are investigated with respect to their severity, like some attacks might be less severe than the other, the severity is depends on what parameters we are considering, the parameters can be anything like loss of packets, network delays, throughput decrement, etc. There are numerous security issues which have been considered in the recent years. For example, snooping attacks, wormhole attacks, black hole attacks, packet replication, poisoning attacks, routing table overflow, denial of service (DoS) attacks, distributed DoS (DDoS) attacks, and so on. Particularly, the misbehavior routing issue is a standout amongst the most promoted security issues, for example, black hole attack, cooperative black hole nodes. A few researchers propose their safe routing algorithms thought to understand this issue, yet the security issue is still an open problem.

Cooperative Black hole nodes are the group of malicious nodes which are configured in such a way that they accept the control packet and generate the fake RREP message of the received RREQ packet, after the route is established, the malicious nodes cooperate with each other and discard the data packets. The discard of data packets can be in any pattern to avoid the security algorithm to detect them as malicious node, like the group of nodes can just drop the packet after receiving it, some pattern might be like the received data packet is only forwarded to the cooperative black hole node till the TTL is expired. In this approach the cooperative black hole nodes receives the data packets and forward it to the next cooperative node and this will continue till the TTL is expired, this is done to make some of the security mechanism fail to detect the malicious activity.

Because of the absence of dynamic topology, centralized administration, limited resources, limited bandwidth, MANET prompts some critical issues like security, bandwidth constraints, Quality of Service, IP addressing, radio interference, routing protocols, control Constraints, versatility administration. Among all these research issues, security has been a prime concern for researchers. One of the vital classifications of attacks to the specially appointed systems is the Denial of Service attack. The most common attacks that belong to this classification are the Black hole and the Gray hole attacks.

As there is no centralized element in MANET, the routing in the MANET is completed by the nodes partaking in the MANET. Each node in MANET carries on as a router. Sender can send information to the receiver only on the off chance that they are both in the communication scope of each other, if it is not possible at that point the sender needs to send information through intermediate hubs. AODV is a reactive routing protocol. AODV is the most generally used routing protocol in MANET. It sets up a route on-demand toward the beginning of the communication session and utilizations it till it breaks, after which another route set up is started.

Manuscript published on 30 September 2019
* Correspondence Author
Deepak Sharma*, Research scholar, MD University, Rohtak, India. Email: erdeepaksharmabwn@gmail.com

To discover a route 13 to the destination, the source node communicates the RREQ (Route Request) packet to its neighbouring nodes and every one of the nodes accepting the RREQ transmit a similar packet to its neighbours until the point that it has a new route to the destination.

The node having a definite fresh route to the destination in the wake of accepting the RREQ message creates the RREP (Route Reply) message and forward that parcel to node from which it got the RREQ bundle. At that point the RREP bundle is sent in the turnaround direction until the point that it achieves the source. At the point when the source node gets the RREP message, it refreshes its routing table with the entry of the destination node and the neighbouring node which has sent the RREP. In this way the source node begins routing the information packets through the way the RREP was crossed.

Black hole and Gray hole attacks are the most common attacks in the Denial of Service attack class. In Black hole attack, the vindictive node tries to trick the sender node that it is the real destination node by sending false reply messages to the sender. The black hole node may reply with the high sequence number so the sender node would surmise that the black hole node is a destination node or it has new route to the destination.

II. LITERATURE REVIEW

In this section we are focusing on the existing work and some basic overview about MANET. Mobile Ad hoc networks (MANET) is a network in which a group of mobile nodes meet up in order to encourage communication between them through wireless connections. Since there is no need of any pre-defined organization, MANET can be effectively set up in situations where it isn't conceivable to set up any infrastructure. Besides MANET have dynamic topology, any hub can enter or leave the network whenever it want. Because of these attributes, MANET's have a wide area of uses in different fields like Defence operations, emergency situations, natural calamities, weather forecasting and so forth.

Ali Dorri [1] proposed An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. The objective of this work is to detect the Cooperative black hole nodes and eliminate them by broadcasting there information. The complete process is divided in three corresponding steps. First Step is to find the fresh path for the Data packet, if the path is available with the routing table then send the data normally otherwise make a RREQ packet and broadcast it throughout the network to get the path from the intermediate node or destination node.

In Second step check the path by checking the RREP generator, in fig below if M1 sends the RREP then the SN will check for the trust of next node and then check the further node till it find the destination or the trustful node.

In the third step the new data structure called DRI table is used to find the correlation between the nodes using the entries in them, the entries of the DRI table is updated with the new information it receives at the time when there is some transfer of data.

The cooperative black hole nodes are decreased and the throughput of the network is improved as compared to the network which is with cooperative black hole nodes. Also it decreases the delay in the network.

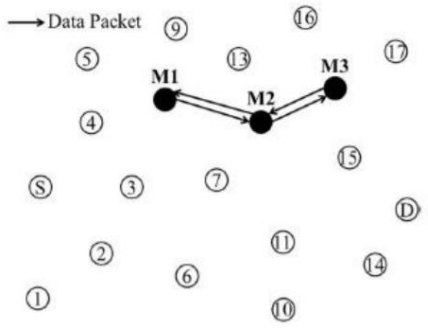

Fig. 1. Prevention using hash function [1]

A. Dorri and H. Nikdel [2] proposed a new approach for detecting and eliminating cooperative black hole nodes in MANET. The objective of the work Detecting Cooperative black hole nodes as soon as possible to reduce the further loss to the network. In this work some metrics are used such as packet overhead, processing time.

Packet overhead refers to the quantity of created RREQ packets in the source node for producing secure way. RREQ packets communicated in the system; in this way, they increment the congestion and collision likelihood which prompts packet lost.

Processing time refers to time required for producing a protected way between the source and the destination. In this investigation, the source node would not send information packets until the point that it finds a safe way to the destination. Because of dynamic topology of MANET, preparing time of security approach is exceedingly challengeable, since high handling time may prompts route break and rerouting process.

The exactness of detection scheme can be assessed by Detected malicious nodes in each run. In cooperative attacks spurious nodes work with each other to cover their tracks; subsequently, security approach must have the capacity to recognize all helpful spurious nodes in each run. False Positive refers to true nodes which detected as malicious nodes by security algorithm.

The Detection of Black hole nodes is faster than the base approach taken by the author and PDR ratio also increased.

Gayatri Wahane and Savita Lonare [3] proposed a Technique for Detection of Cooperative Black Hole Attack in MANET. The RIT Table is used in this approach which check the reliability of the nodes present in the network. In the proposed scheme, the steps for recognizing and also protecting against a cooperative black hole attack is distinguished and displayed by a calculation. The modification of Ad Hoc on Demand Distance Vector Routing Protocol takes with the introduction of two sorts of concepts one is addition of Routing Information Table (RIT) and the other is by Checking Reliability of each node.

In this, an Algorithm to recognize cooperative Black Hole Attack has been proposed and examination has been done by considering three distinct cases. In the primary case there were no spurious node display in the system and the reply for route request was from the trustful node so in light of this past information of quality of node the route is confirmed to be secured.

In the second case there were two black hole nodes in the system commonly collaborating with each different as there was no past information for these two nodes so they are checked for dependability and discovered malignant toward the end and this information of malicious conduct was spread all through the system.

In the third case a node is observed to be solid and this information is communicated all through the system and third piece regarding that node is set to genuine which demonstrates that the node in question is trustful node.

At last it has been concluded that this calculation functions admirably in all the three cases with the point of distinguishing Cooperating Black Hole Attack and guaranteeing a protected and also dependable route from source to destination. Attacker found but delay increased because the control packets flow in the network increased.

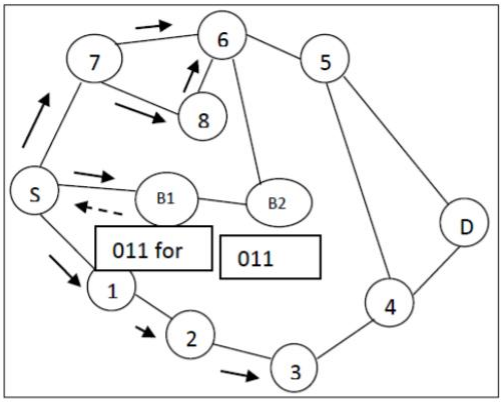

Fig. 2. Cooperative black hole node attack [3]

Kundan Munjal et al. [4] proposes a different approach for Cooperative Black Hole Node Detection by Modifying AODV. The objective of this work is to modify the AODV protocol to detect the cooperative black hole nodes.
The proposed scheme have RIT table in which the extra data of the nodes are updated, the working principal of the proposed is described by the example below: The node B1 quickly answers deceptively with RREP packet demonstrating that it is having the briefest and in addition sufficiently new route to the destination.
The SN as indicated by the calculation first checks whether the RREP is from the destination node or from the trustful node i.e. it checks the RIT section for that node yet it finds the node B1 temperamental and after that it checks it for dependability. It approaches B1 for its next jump and furthermore the RIT passage for the following bounces.
It gives its next jump B2 and it lies with the RIT section with esteem 0 1. Since no node in the system has sent information through B1 previously, B1 isn't a trustful node to S. Subsequently S sends additional request (ARq) to B2 by means of elective way S-10-9-B2 and get some information about three things: 1. Regardless of whether B2 had routed any information from B1. 2. Who is B2‟s next jump to the destination? 3. Regardless of whether B2 had routed information packets through B2's next jump.
Since B2 is maliciously working together with B1 it answers emphatically to all the three questions and gives node 3 with its next jump. Since node 3 has neither a route to node B2 nor it has gotten information packets from B2 the RIT section an incentive as for B2 as in routing information table of node 3 is 0. In light of this information node S gathers that B2 is a black hole and source node S additionally derives that node B1 is maliciously participating with node B2.
Consequently the two nodes B1 and B2 are set apart as Black Hole nodes and this information is spread all through the system. Malicious nodes present in the network avoided by the help of manipulating the data routing information table.

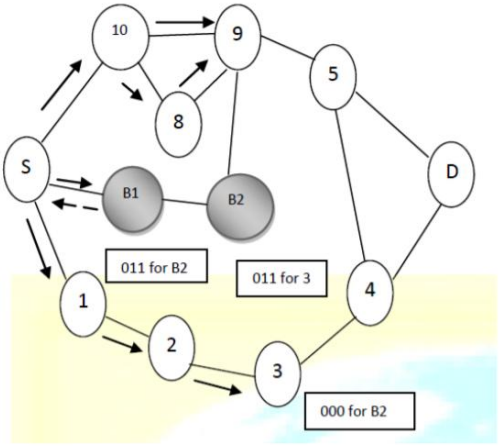

Fig. 3. Attack prevention on given scenario [4]

III. PROPOSED APPROACH

In this section an approach is proposed for eradicating the Cooperative black hole nodes by updating the DRI table entries and using them at the time of route lookup. The DRI table is attached with routing table and have two column FROM and THROUGH which are initialize to 0 initially and updated to 1 or 0 representing ‘True’ or ‘False’ respectively. If there is a node identified as Black hole node then both the values will be updated with ‘NULL’, so next time when the Black hole node replies to the route request then it can be avoid by looking the DRI table entries at the source node.

A. Idea behind the Approach

The idea behind the proposed approach is that single black hole node detection schemes will not work in finding the Cooperative black hole node detection because of the pre-defined cooperation between multiple nodes, so it is required to make a scheme to find the cooperative black hole nodes.
So, If the RREP packet is received from the trustful node, then there is no need to check the node if it is malicious or not because it already transferred data in past. Trustful Node – In DRI table of a node if there is entry for some node indicating FROM as ‘1’ as well as THROUGH is ‘1’ then this node is trustful for the node.
If the RREP generating node is not trustful, then the proposed control packet will check the Next hop Node (NHN) and asks its DRI table entries for the Previous Hop Node (PHN) and the Next hop node (NHN).
The checking is done at the Source Node (SN) on the basis of comparing the current node FROM column and Previous Node THROUGH column which tells the data is transferred previously from the current node.

If somewhere there is No Match of FROM of current node the THROUGH of Previous node then the node from RREP generator to Previous node of current node will be marked as the Black hole nodes and further RREP messages will not be entertained from these node.
They are marked black hole by Source node (SN) by giving NULL at FROM and THROUGH.
Comparison between the previous approach and proposed approach:

Table- I: Comparison Between different approaches

DRI Table in the proposed approach	Normal DRI Table
1. The DRI Table in this approach is implemented in the Routing table itself by defining the variables. 2. Routing table lookup increased to two from one for servicing a single RREP and FREQ request. 3. The comparison of FROM and THROUGH can done in one lookup of routing table	1. DRI table is implemented in different Data Structure which increase the space complexity. 2. Only one lookup is required to service a RREQ and FREQ request.

B. Working principle

Work Flow of the proposed approach is as follows. Once the SN needs to transfer the Data to some Destination node then it checks for the Path in its routing table if the route is available then the SN will transfer the data. If there is no route available at the SN for the Destination then the SN will make the RREQ packet to get the fresh route to the Destination.
The nodes with the route to destination node will make RREP packet and send it to the SN with the DRI table entries.
The SN will check for the Black hole node by checking if the RREP packet generator's THROUGH column and NHN's FROM column, if both are '1' for each other then check for the further nodes till we get the Destination node or the node where the FROM and THROUGH of each other are not matched.
If the FROM and THROUGH of the current node and the previous hope not matched, then the from RREP generator to previous nodes are marked as the black hole nodes by making NULL at the DRI table of the SN, so further RREP can be discarded from those nodes.
If the NHN is destination itself, then the SN will start the data transfer, and update its DRI table entries.

C. Flow charts

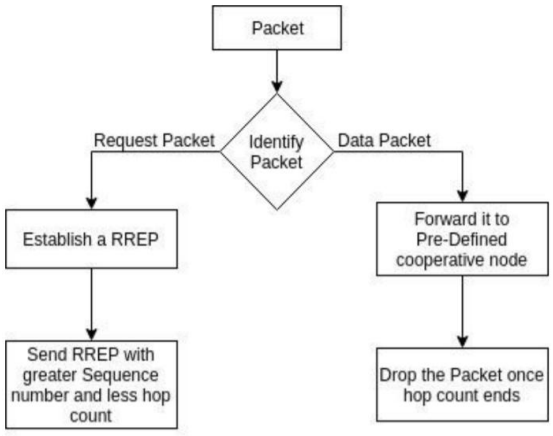

Fig. 4. Implementation of Cooperative Black Hole node

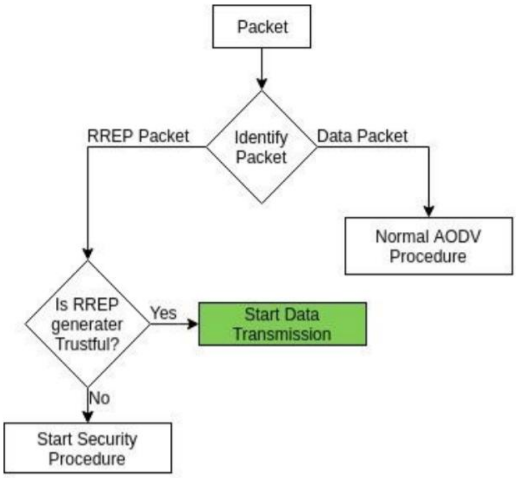

Fig. 5. Route Request Generator (Source)

IV. IMPLEMENTATION AND RESULTS

This section explains how the new proposed approach has been implemented in the NS-2 and the results of that implementation.

A. Simulation environment

Table- II: simulation environment

Simulator	Network Simulator 2.35
Simulation duration	150 s
Data rate	1Mbps
Number of nodes	30
Data packet size	1 KB
Simulation Area	1000 m X 1000 m
Routing Protocol Modified	AODV
Transport Agent	UDP

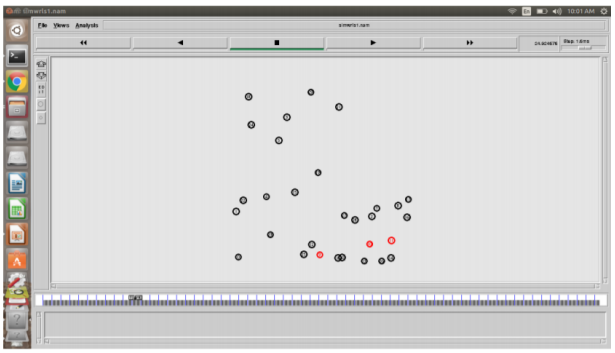

Fig. 6. Simulation result in NAM

The overall simulation events like sending, receiving, forwarding, drop of packets in the network is recorded in the trace file with respect to the time the event is happened. The events are recorded with the corresponding time, the other attributes are also there like to see if from where the packet is originating, where the packet is destined, the next hop node for the packet, etc. The trace files are saved in the .tr format and they are analysed through any of the scripting language like AWK, perl, python etc. AWK is the commonly used scripting language in the NS2 new trace file format.

B. Scenario 1: Cooperative Black hole attack

In this Scenario the Data connection is defined between Node 0 and Node 17.

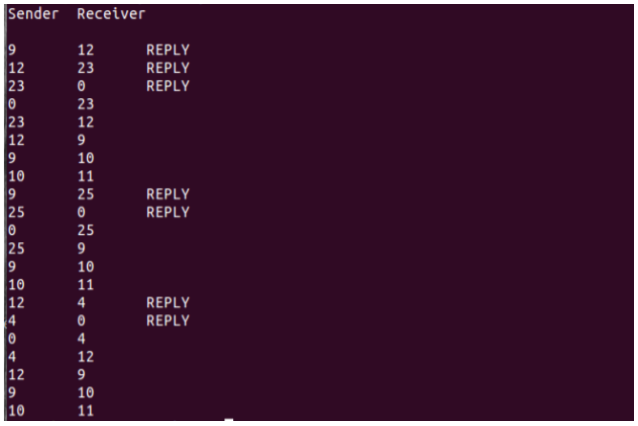

Fig. 7. Sender – Receiver information

Analysis of above Result when there is Black hole attack in the network. AODV RREQ is broadcasted by the Node 0 for finding out the route to the destination. In response to that RREQ packet an AODV RREP packet flow: 9→12→23→0. Node 0 routing table after receiving reply from Node 9 upadte the information.

Table- III: Node 0 Routing table

Node id	Next hop	Hop count
17	23	5

Node ID, Next hop, Hop count 17 23 5. Data packet flow using the path: 0→23→12→9→10→11. The packet which is bound to Node 17 didn't reach the destination which is showing black hole attack. After some time connection breaks due to mobility. AODV RREQ is again broadcasted by the Node 0. In response to the second RREQ packet an AODV RREP packet flow from path: 9→25→0. Node 0 updated routing table after receiving reply from Node 9.

Table- IV: Node 0 Routing table

Node id	Next hop	Hop count
17	25	4

Data packet flow using the path: 0→25→9→10→11. The packet which is bound to Node 17 didn't reach the destination which shows the black hole attack. Connection breaks due to mobility. AODV RREQ is again broadcasted by the Node 0. In response an AODV RREP packet flow using path: 12→4→0. Node 0 routing table after receiving reply from Node 12 as Node ID, Next hop, Hop count 17 4 5.

Table- V: Node 0 Routing table

Node id	Next hop	Hop count
17	4	5

Data packet flow using path: 0→25→9→10→11. The packet which is bound to Node 17 didn't reach the destination which shows the black hole attack. Here it is clear that the data is terminated at the 11 node which is also a black hole node because the hop count is 0 at this node.

This analysis shows that the Node 0 is transmitting the Data packets after one of the cooperative black hole nodes is replied to the RREQ packet and the route is formed between the source and the RREP generator black hole node.

In the Fig.7 the Node numbers in second column against the Node number in first column shows the packet received for example In first Column Node 0 is transferring data to the nodes present in the second column.

Node 0 is transferring data to Node number 9, 10, 11 which are Cooperative black hole nodes, so from the information in Node 9, 10, 11 it is clearly showing that these nodes are not forwarding the data towards the destination but they are just forwarding the data to the fellow black hole nodes.

C. Scenario 2: On applying DRI table based Security Approach

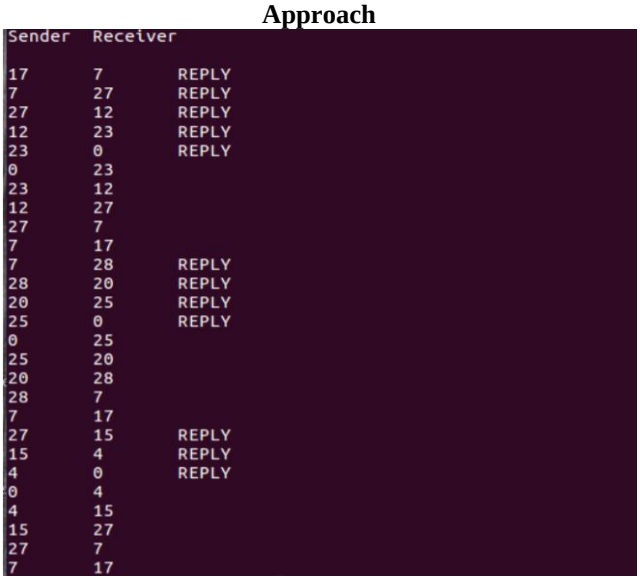

Fig.8: Sender-Receiver information

The Simulation of the approach is also done in the same environment and the Data connection is between the Node 0 and Node 17.

Here the Fig.8 is showing that after applying the proposed security mechanism the cooperative black hole nodes 9, 10, 11 are eliminated and they are not considered when they sends RREP to any route request.

Analysis of above Result when there is Black hole attack in the network. AODV RREQ packet is broadcasted by the Node 0 to get the desired route. AODV RREP received from Black hole Node 9 in response to the RREQ packet sent by node 0 previously. Node 0 initiates Security Mechanism by sending FREQ packet to NHN (Next hope node) of Node 9 to compare Node 9 FROM and Node 10 THROUGH by getting the FREQ from NHN Node 10. Node 0 (SN) maintain a data structure of node id on which it is sending the FREQ.

Table- VI: Node 0 Routing table

0	1	2	3
9	10	11	

Node 0 (SN) now update the Routing table, as the newly founded nodes identified as black hole nodes and their corresponding entries are updated with NULL in the routing table. Now to every RREP from Node 9 the Node 0 (SN) first check the trustfulness of Node if it is a black hole node then it drop that request packet and consider the other request packets in buffer. AODV RREP packet flow using the path: 17→7→27→12→23→0. Node 0 routing table after receiving reply from Node 17.

Table- VII: Node 0 Routing table

Node ID	Next hop	Hop count	From	Through
17	23	5	0	1
9	23	5	NULL	NULL

Data packet flow using the selected path which is: 0→23→12→27→7→17. The packet which is bound to Node 17 reached the destination. Connection breaks due to mobility. AODV RREQ packet is broadcasted by the Node 0 to get the desired route. AODV RREP packet flow using path: 7→28→20→25→0. Node 0 routing table after receiving reply from Node 7.

Table- VIII: Node 0 Routing table

Node ID	Next hop	Hop count	From	Through
17	25	5	0	1
9	25	4	NULL	NULL

Data packet flow using the path: 0→25→20→28→7→17. The packet which is bound to Node 17 reached the destination. Connection breaks due to mobility. AODV RREQ packet is broadcasted by Node 0. AODV RREP packet flow using the path: 27→15→4→0. Node 0 routing table after receiving reply from Node 27.

Table- IX: Node 0 Routing table

Node ID	Next hop	Hop count	From	Through
17	4	5	0	1
9	4	5	NULL	NULL

Data packet flow using path: 0→4→15→27→7→17. The packet which is bound to Node 17 reached the destination. The RREP from the Black hole node is dropped by the SN because after the security mechanism the DRI entries of the Node are updated to NULL, so that the black hole nodes cannot taken as the path.

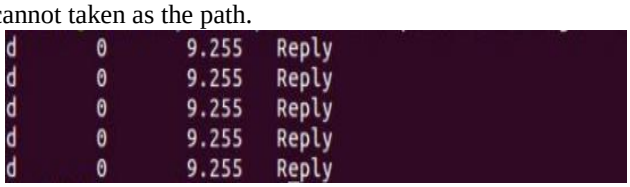

Fig.9: Rejected replies of malicious node

In the Fig.9, it is showing that after the Nodes are found out as malicious node, then there reply to any RREQ is dropped by the source node. This shows how the black holes nodes now do not considered in the network.

V. CONCLUSION AND FUTURE SCOPE

A. Conclusion

In this section we will conclude the overall performance of our work, assumption taken and the scope of project in future. From the analysis we can conclude that the proposed approach is finding the black hole nodes in the system by applying the security mechanism. The complexity of the proposed security mechanism is increased with the increased number of Blackhole nodes present in the network. The Cooperative black hole detection procedure proposed in the approach is able to detect the black holes. After the detection of the black holes there information is broadcast throughout the network, so further RREP are not considered by the nodes in the network.

Some assumptions are taken into consideration while implementing this approach. The Cooperative Black hole nodes are in a chain form and the their routing table contains only the routing information to fellow black hole nodes. The information about their fellow black hole nodes are given initially so there is no need to maintain the collaboration between the black hole nodes. There is no breaking in connection between the black hole nodes.

B. Future Scope:

The assumptions taken can be further includes in the approach to make the security procedure more concrete towards detection of black hole nodes in more varieties of conditions. The proposed approach do not have provision of verify False detection of black hole, this may lead to detect more black hole then they really are, and sometimes the packet of security scheme is lost which also result in false detection of black hole node.

REFERENCES

1. Ali Dorri, “An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET”, Wireless Networks (2016), Springer.
2. A Dorri and H. Nikdel, "A new approach for detecting and eliminating cooperative black hole nodes in MANET”, 2015 7th Conference on Information and Knowledge Technology (IKT), Urmia, 2015, pp. 1-6.
3. Ms. Gayatri Wahane, Ms. Savita Lonare "Technique for Detection of Cooperative Black Hole Attack in MANET”, 4th ICCCNT 2013, Tiruchengode, India, pp. 10-16.
4. Kundan Munjal, Shilpa Verma, Aditya Bakshi, “Cooperative Black Hole Node Detection by Modifying AODV”, International Journal of Management, IT and Engineering, 2014, pp. 485-501.
5. S. Ramaswamy, H. Fu, M. Sreekantaradhya, John Dixon and Kendall Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks” International Conference on System Engineering and Technology, 2012, pp.-1-7.
6. Nidhi Choudhary, Dr.Lokesh Tharani, “Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism” SPACES-2015, Dept. of ECE, K L UNIVERSITY, IEEE, 2015.
7. Al-Shurman M, Yoo S-M, Park S, Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE’42), Huntsville, Alabama, 2-3 April 2004.
8. Anand A. Aware,Kiran Bhandari, “Prevention of Black hole Attack on AODV in MANET using hash function” Published in: Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 3rd International Conference on 8-10 Oct. 2014,IEEE.
9. Apurva Jain, Urmila Prajapati, Piyush Chouhan, “Trust Based Mechanism with AODV Protocol for Prevention of Black-Hole Attack in MANET Scenario”. Published in: Colossal Data Analysis and Networking (CDAN), Symposium on 18-19 March 2016, IEEE.
10. T. Clausen, J. Dean, C Adjih, “Generalized Mobile Adhoc Network Packet/Message Format”, RFC-5444, July 2015.
11. Aarti,Dr. S.S Tyagi “Study of MANET: Characteristics, Challenges, Application and Security Attacks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, ISSN: 2277 128X May 2013.

AUTHORS PROFILE

Deepak Sharma is currently pursuing a Ph.D. in Computer Science at M. D. University, Rohtak. He has completed his M.tech from C-DAC: Centre for Development of Advanced Computing, Ministry of Communications and Information Technology, Government of India affiliated from Guru Gobind Singh Indraprastha University, Delhi. His main research areas include Data mining, Mobile Adhoc Network (MANET), wireless sensor network (WSN) and Internet of things (IoT).