SIMULATION BASED STUDY OF COOPERATIVE BLACK HOLE ATTACK RESOLUTION USING CROSS-CHECKING ALGORITHM

Garima Gupta[1] and Atul Mishra[2]

[1]Department of Computer Engineering, YMCA University of Science & Technology, Haryana, India
[2]Department of Computer Engineering, YMCA University of Science & Technology, Haryana, India

ABSTRACT

An Ad hoc Network is a pool of wireless mobile nodes energetically forming a network without the use of any pre-accessible network infrastructure or centralized administrator. These nodes communicate with each other by hop-to-hop communication. This dynamic topology of mobile ad-hoc networks (MANETs) allows nodes to get attached and leave the network at any second of time. Thus MANET can be used in a variety of fields. Current MANETs are designed primary for military utility. This generic characteristic of MANET has rendered its vulnerability to security attacks. Due to which unprotected attacks of the malicious nodes can occur at any time. This paper focuses on one such attack known as "Black hole attack" and the routing protocol being used here is AODV.

KEYWORDS

MANET, Black Hole Attack, AODV, Cross-Checking, Mobile Node.

1. INTRODUCTION

Irrespective to the infrastructure wireless networks [1], a mobile ad hoc network is a type of wireless ad hoc network which is a self organizing network of mobile devices linked by wireless links with no base station in between. Every mobile node in a network is autonomous. The mobile devices are free to move and organize themselves. In other words, ad hoc network do not rely on any fixed infrastructure. The Communication in MANET is take place by using multi-hop paths. Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, breaking of communication link is very frequent, as nodes are free to move to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET.

However, due to their inbuilt feature of vibrant topology and lack of centralized management security, MANET is open to various kinds of attacks. These include grey hole attack, warm hole attack, black hole attack and the denial-of-service attack. The main protocols in MANETs include the following ones.

a) Proactive or Table Driven like DSDV (Destination Sequence Distance Vector Routing)
b) Reactive or On Demand like AODV (Ad hoc On Demand Vector Routing)
c) Hybrid like ZRP (Zone Routing Protocol)

The packet dropping attack thus described in this paper is Black Hole node attack in which a malicious node absorbs the data packet in itself, similar to the black hole in the universe which absorbs everything that comes to it. In this way, the packets in the network are either dropped or absorbed. A malicious node that drops all the traffic in the network makes use of all the liabilities of all the route discovery packets of the on demand protocol such as AODV [2].

A black hole node is a node that always replies affirmatively with a RREP message to every RREQ, even though it does not have a genuine route to the destination node [2].When the data packet reaches the black hole node, it drops them rather on forwarding them. It was quiet easy and well simulated to work on a single black hole node but a method is needed to be finding out to identify, avoid and drop the cooperative black hole nodes.

The rest of the paper is organized as follows. In section 2 the literature review related to black hole attack has been presented. Section 3 comprises of the cooperative black hole attack with the cross check algorithm to implement it and all the simulation scenarios. Section 4 consists of the result having graphical outputs that shows the throughput and delay. Conclusion is then provided in section 5.

2. LITERATURE SURVEY

There certainly have been several attempts available in the literature that aims at removing the black hole attacks. We review them as follows.

Vipan et al. [3] discuss the problem of improving the security as in existing AODV there is no provision against well known black hole attack. And the network degradation problem is also discussed here. Solution so proposed here is the modification in working of source node by a method called Prior Receive reply. Malicious node is identified by using two methods: 1. Route table 2. Waiting Time. So a simple and efficient approach for defending against black hole attack has been used. This method can be used to find out the secure routes and preventing the black hole nodes in MANETs by identifying their sequence number. Check is done on the difference between the sequence number of source or intermediate node who has sent the RREP back.

Sanjay Ramaswamy et al. [4] proposed the problem of coordinated black holes acting in group. It proposed a solution by discovering the safe route avoiding these black holes. Modification is done by using data routing information table (DRI) and cross checking. It thus identifies the multiple black hole nodes acting in group, discovers secure path from Source to destination by avoiding these. As a future work they need simulation technique for this.

Rajib Dasi et.al [5] thus addresses the problem of addressing and removing the black hole nodes in beginning such that no packet is lost or retransmitted. An additional route to intermediate node is discovered that replies the RREQ message to check whether the route from intermediate node to Destination node exists or not is maintained. When source node receives FRp from next hop node it extracts to check results from reply packet. If result is yes then a route is established else discarded.

Marti et al. [6] proposed a scheme named Watchdog. It aims to improve the throughput when malicious node is present in the ad hoc network. It mainly consists of two parts -Watchdog and Path rater. Watchdog detects the misbehavior in the network while the Pathrater finds a new route to the destination excluding that malicious node by cooperating with the routing protocol. It listens to its next node transmission; it maintains a buffer which stores the packet in it and a failure counter. If a node forwards the packet to its neighbor then that packet is deleted from its buffer else it increases the value of its failure counter. If the value of the counter exceeds the pre

defined threshold then that node is declared as malicious and now Pathrater finds the new route to the destination. It detects the malicious node in the network instead of malicious links. There are six weaknesses that are mentioned by Marti [6]. They are:

1) Receiver Collision problem
2) Ambiguous collision
3) Limited Transmission power
4) False misbehavior
5) Collusion
6) Partial Dropping.

Liu et al [7] proposed the TWO ACK scheme. This scheme aims to resolve the limited transmission power and receiver collision problem of the Watchdog. But it is not an improvement or enhancement of the Watchdog scheme proposed by Marti. It detects the misbehaving links by making the nodes send an acknowledgment packet to every third node down the route, which means upon receiving the data packet every third node in the route from source to destination is required to send an acknowledgment packet to the node two hops away down the reverse route.

Elhadi M. Shashuki et al [8] [9] proposed a new approach called EAACK that solves three weaknesses out of six weaknesses of the Watchdog scheme. It solves false misbehavior problem, limited transmission power and receiver collision problem. It makes use of the digital signature to ensure the legitimacy of all the acknowledgment packets. By using the digital signature it prevents the attacker from forging the acknowledgments.

Songbai Lu et at [10] [11] proposed SAODV that resolves the problem of security measures that arises in AODV protocol. Here in it, a random number is generated by the source node and is send in every RREQ message. If the same random number is received by destination from more than two different paths than it sends a RREP message to source node that contains another random number. Same process is followed by source node for verification. If the random number is same as the previous one than the path is secure and data can be transmitted over that path.

Ms. Nidhi Sharma et al [12] proposed two possible solutions for prevention of black hole attack in MANET. First solution suggests finding more than one route to destination node by finding the authenticity of the node that initiates the RREP message. In it RREP packet has to be received from at least more than two nodes. During this time the source node than buffer its packets until the safe route is discovered. Main drawback in this approach is time delay.

The second approach suggests that every packet has a unique sequence number having the value always greater than the precedence node. In it, every node has to maintain two small sized tables. These tables are updated whenever any packet is arrived or transmitted. Packet authenticity is checked by the higher sequence number and its comparison from the precedence one. It has benefit of having more reliability and no overhead.

Shambhu Upadhyaya et al[13] addresses the problem of colluding and coordinating black hole attack which then leads to the loss of all the necessary and critical information transmitted all over the network. It thus provides a solution to overcome this problem by introducing multipath routing schema. It uses the ACK (acknowledgement) packets being transmitted first to check for the validity of the path. These packets thus establish the secure path and data can then be transmitted successfully over that path. Furthermore, this approach is implemented on network simulator with the graphs showing the data packets their mobility, control packets and the packets lost and the packets routed to another node.

Kishor jyoti Sharma et al [14] presents a survey of various attempts and techniques that are established till date for identification and removal of black hole and cooperative black hole nodes. Such attempts are listed as:

1) DRI table and Cross Checking scheme
2) Time-based threshold detection scheme[15]
3) Detection, Prevention and Reactive AODV scheme[16]
4) Nital Mistry et al.'s method[17]
5) Hash based scheme[18]
6) Neighborhood-based and routing recovery scheme[19]
7) Trust table Method[20]
8) Secure AODV[13]
9) Optimized Black hole Detection and Prevention Algorithm[21]

3. SIMULATED STUDY OF COOPERATIVE BLACK HOLE ATTACK RESOLUTION

3.1 BLACK HOLE ATTACK

A kind of denial of service where a **malicious node** can attract all packets by untruely claiming a new route to the destination and then absorb them without forwarding them to the destination is a black hole attack.

In **fig. 1** the node 1 and the node 4 are source and destination nodes resp. while the **node 3 is the black hole** node that absorbs the data packets. Here node 3 first of all sends the RREP (route reply) so that all the data packets can be transmitted over that.

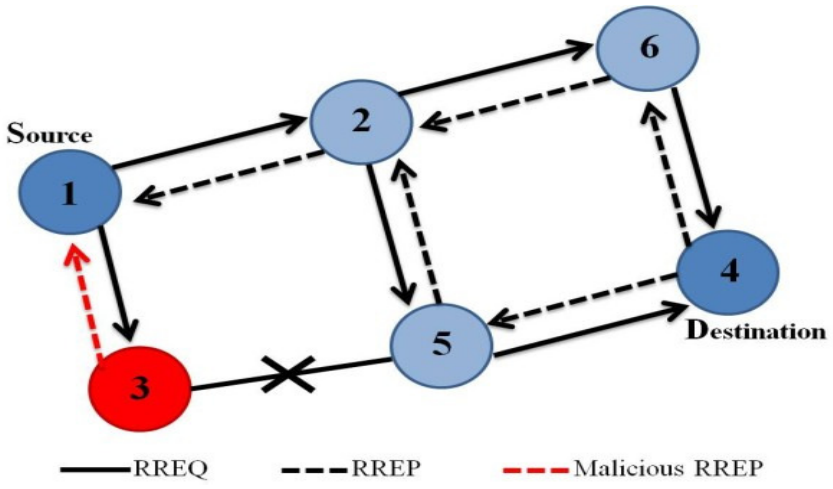

Fig. 1 Black Hole Attack in MANET

3.2 COOPERATIVE BLACK HOLE ATTACK

Researchers have given many solutions to identify and eliminate a single black hole node. However, in case of multiple cooperative black hole nodes no efficient and reliable solution has been provided.

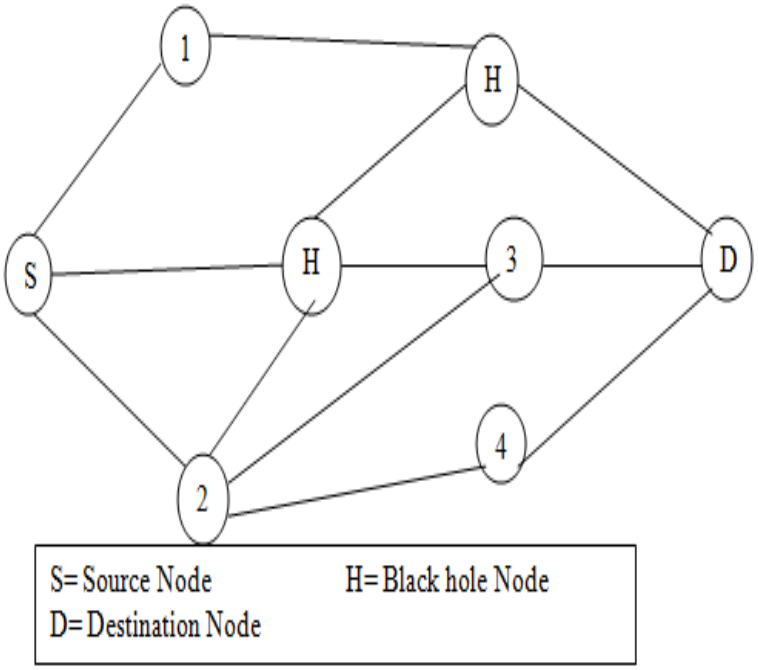

Fig. 2 Cooperative Black hole node attack problem

For example, [4] as shown in fig. 2, source node S wants to transmit data packets to destination node D. It first broadcasts a RREQ to intermediate node IN. IN being a black hole H replies first with the RREP message and always refers to other black hole H having the shortest path to destination. Source node then checks for the reliability of that black hole node H via. Sending further request Freq. to coordinated black hole via. Different route. As H is in coordination with another black hole it will always reply with a Further reply FRp. With that confirmation S starts sending the data packets to H. However, in reality, the packets are consumed by node B1 and the security of the network is on conciliation.

3.3 CROSS- CHECKING ALGORITHM

The following task is being carried on [4] as shown in fig. 3.

1. The source node (SN) broadcasts a RREQ message in conquest to discover a safe route to the destination node.(DN)
2. The Intermediate Node (IN) generates the RREP which has to provide its Next Hop Node (NHN) and its DRI entry for the NHN.
3. Now, the source node will check its DRI table for the reliability of IN.
4. If the result is yes, then the source node sends Freq message to NHN. Based on the Frep message from NHN, source node checks whether NHN is a reliable node or not.

5. If IN is not a black-hole and NHN is a reliable node, the route is secure, and source node will update its DRI entry for IN with 01, and starts routing data via IN.
6. If IN is a black-hole, the source node identifies all the nodes along the reverse path from IN to the node that generated the RREP as black hole nodes. Source node ignores any other RREP from the black holes and broadcasts the list of cooperative black holes.

Algorithm to prevent cooperative black hole attack in MANETs

Notations:
SN: Source Node IN: Intermediate Node
DN: Destination Node NHN: Next Hop Node
Freq: Further Request Frep: Further Reply
Reliable Node: The node through which the SN has routed data
DRI: Data Routing Information
ID: Identification of node

```
1    SN broadcasts RREQ
2   SN receives RREP
3    IF (RREP is from DN or a reliable node) {
4    Route data packets (Secure Route)
5    }
6    ELSE  {
7              Do {
8              Send Freq and ID of IN to NHN
9               Receive Frep, NHN of current NHN, DRI entry for
10              NHN's next hop, DRI entry for current IN
11              IF (NHN is a reliable node) {
12              Check IN for black hole using DRI entry
13              IF (IN is not a black hole)
14              Route data packets (Secure Route)
15              ELSE {
16              Insecure Route
17              IN is a black hole
18                        All the nodes along the reverse path from IN to the node
19                        that generated RREP are black holes
20                        }
21                       }
22              ELSE
23              Current IN = NHN
24              } While (IN is NOT a reliable node)
25  }
```

Fig. 3 Cross-Checking Algorithm

3.4 SIMULATION SCENARIO

In the simulation scenario, the following design issues are considered.

a) Simulation Environment
b) Simulation Metrics
c) Simulation Scenarios

3.4.1 SIMULATION ENVIRONMENT

The simulator used here is NS2 i.e. the working environment is NS2. Protocol used here is AODV. Rest of the parameters are shown in tabular form as in Table 1.

Table 1: Simulation Parameters

S.No.	Parameters	Value
1.	No. Of nodes	20
2.	Simulation area	900X900 meter
3.	Simulation Time	30 sec
4.	Mobility Model	Random waypoint 0
5.	Packet size	1000 byte
6.	Traffic Type	CBR
7.	Packet rate	4/sec
8.	Protocol used	AODV

The simulation here is conducted on NS2 platform with number of nodes being used is 20(variable). Simulation area is 900X900 meter with the core of Ubuntu 10.4.

3.4.2 SIMULATION MATRICES

The simulation here is done on the basis of the following parameters:

1) **Throughput**: It basically describes the ratio of total packets sent to the total packets received in prescribed simulation time depending on the no. of malicious nodes present here.
2) **Delay:** Here, in this parameter the delay factor is taken under consideration in which the total time is calculated. Total extra time the packet takes to reach to the destination is termed as delay.
3) **Overhead:** It provides all the information that tells about the routing just like the route reply and route request.
4) **Packet Delivery Ratio**: PDR tells the ratio of total number of packets sent from the source node to the destination node via. Intermediate node.

3.4.3 SIMULATION SCENARIOS

The simulation of following scenarios has been done.

1) Network Simulation with No Black hole

In this case no black hole has been taken. So maximum packets send are received by the destination. Thus no packet is dropped or lost in the midway. This then leads to maximum throughput and almost zero delay.

2) Network Simulation with Single Black hole

In this scenario a single black hole is introduced. Keeping the other parameters same. Now due to the single black hole some packets are lost and dropped. This then leads to packet retransmission. Here in this case the threshold is reduced to some extent and so the delay is increased.

3) Network Simulation with Cooperative Black hole

In this scenario a cooperative black holes are introduced. Keeping the other parameters same. Now due to the single black hole some packets are lost and dropped. But due to cooperative black

holes more packets are dropped and lost. They thus can't reach the destination. This then leads to the energy lost and packet retransmission. In this case the threshold is further more reduced and so the delay is increased.

4) Cross Checking Algorithm Implementation

Now to improve the throughput and lessen the delay cross checking algorithm as provided in [4] is implemented in NS2.

In this the simulator continuously checks for the black hole node and when satisfied by the route sends the data packets else discards the route. This algorithm thereby, increased the throughput value and lessens the delay furthermore.

4. RESULTS

The graphical representation and simulation scenario is shown below:

SCENARIO 1: NETWORK SIMULATION WITH NO BLACK HOLE

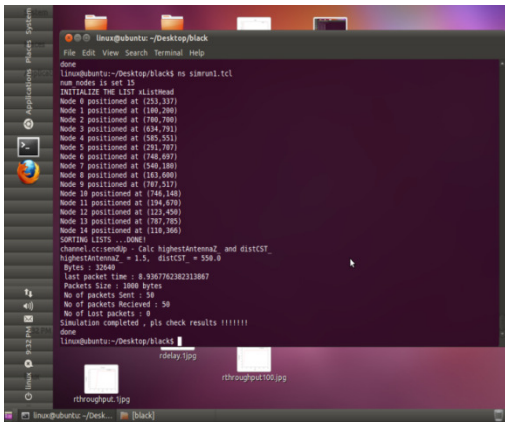

Fig. 4 Simulation Screen

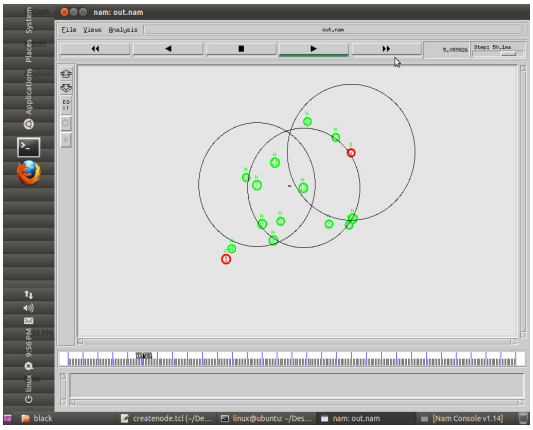

Fig.5 Nam Window

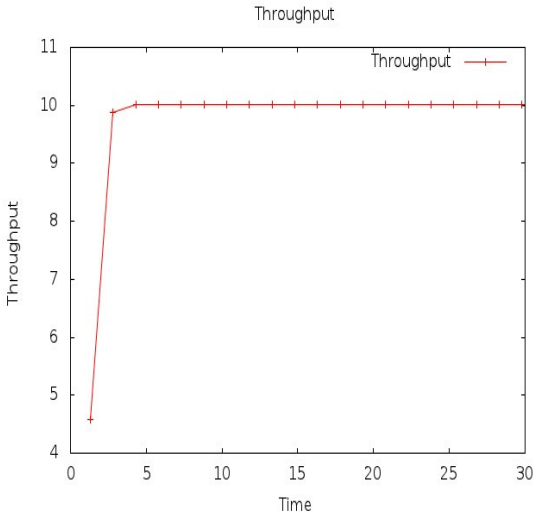

Fig.6 Throughput graph

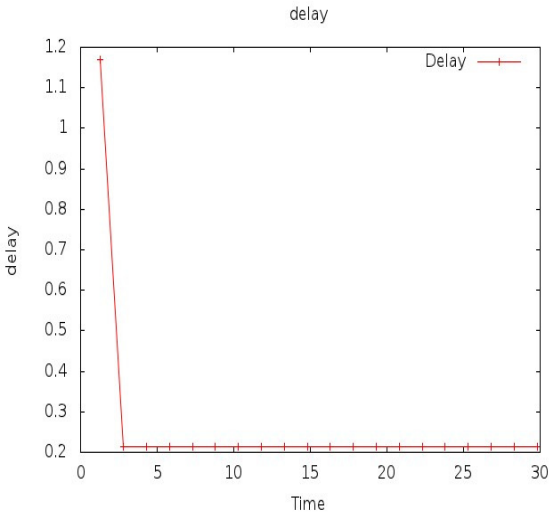

Fig.7 Delay graph

The graphs show that with no black hole we get a maximum value of throughput and almost no delay. In this case all the packets send by the sender reaches the destination accurately i.e. there is no packet loss.

Fig. 4 shows the simulation screen in which 50 packets are sent and received properly. Here, in this the packets are transmitted between the source and destination with no malicious node. Fig. 5 shows the NAM window for the above simulation showing the absence of any malicious node i.e. black hole. Fig. 6 shows the variance between the throughput and time. As there are no black holes present so the throughput value reaches to 100% in this scenario. Thus, all the packets reach the destination properly and fig. 7 shows variance between the delay and time. With little environmental factors such as noise or distortion the delay variance is approx. 0.2%.

SCENERIO 2: SINGLE BLACKHOLE

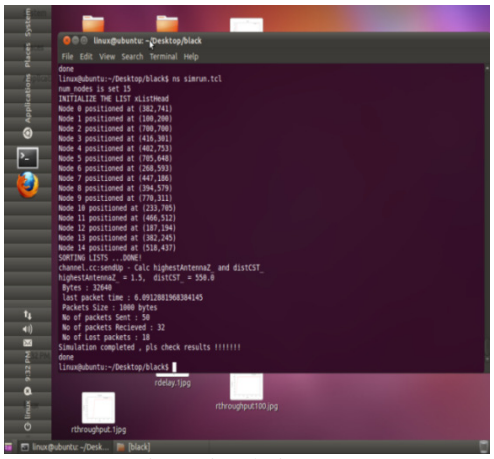

Fig.8.Simulation screen

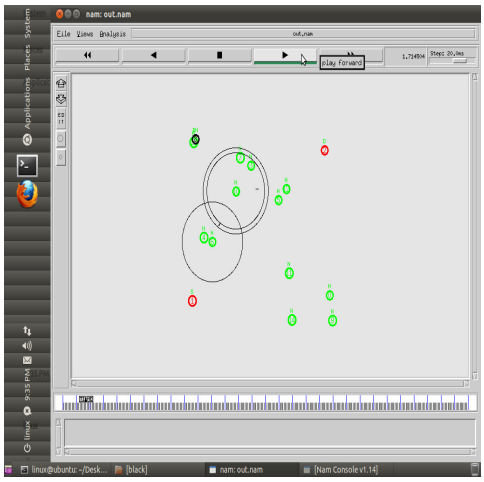

Fig.9 Nam Window

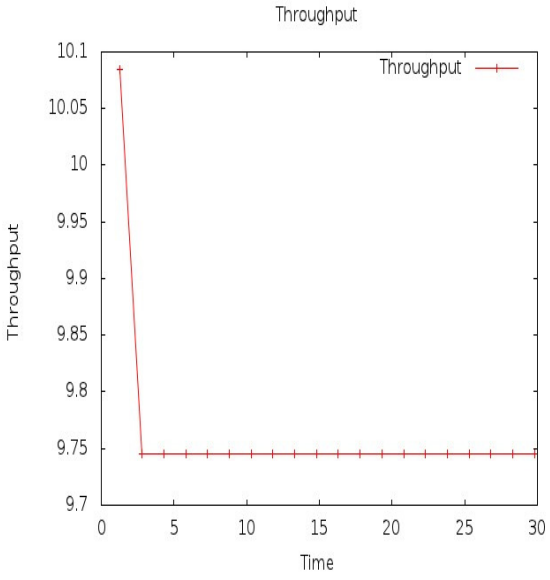

Fig. 10 Throughput graph

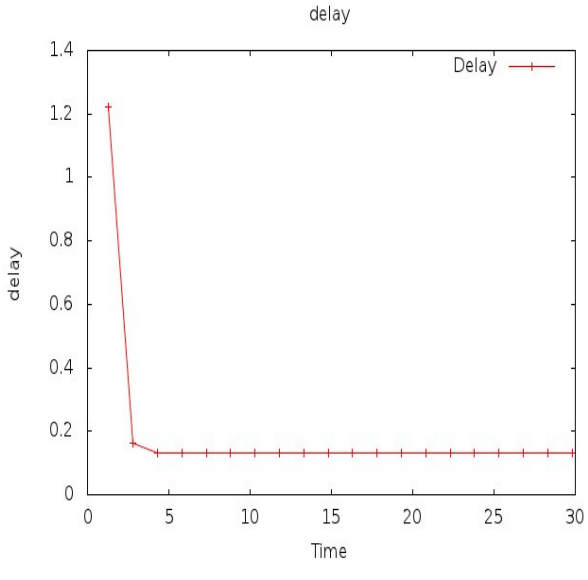

Fig.11 Delay graph

The graphs show that with a single black hole some of the packets reaching the destination are lost. As a result, a variation in value of throughput is seen and delay is somewhat increased also. In this case all the packets send by the sender does not reaches the destination accurately. That leads to dropping of throughput value.

Fig. 8 shows the simulation screen in which 50 packets are sent but, all packets are not received properly. Fig. 9 shows the NAM window for the above simulation showing the presence of single malicious node i.e. black hole. Fig. 10 shows the variance between the throughput and time. As there is single black hole present so the throughput value decreased to 97% in this scenario. Fig. 11 shows variance between the delay and time. With more retransmissions delay is increased upto 2%.

SCENERIO 3: COOPERATIVE BLACK HOLE

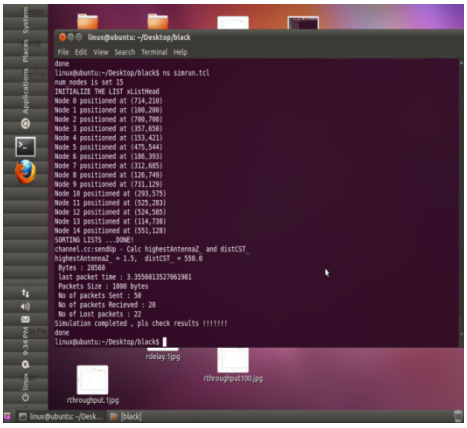

Fig.12 Simulation Screen

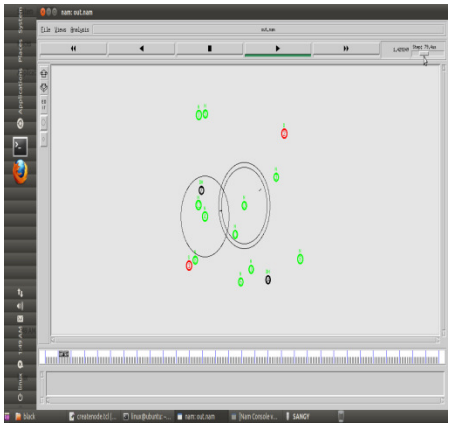

Fig.13 Nam Window

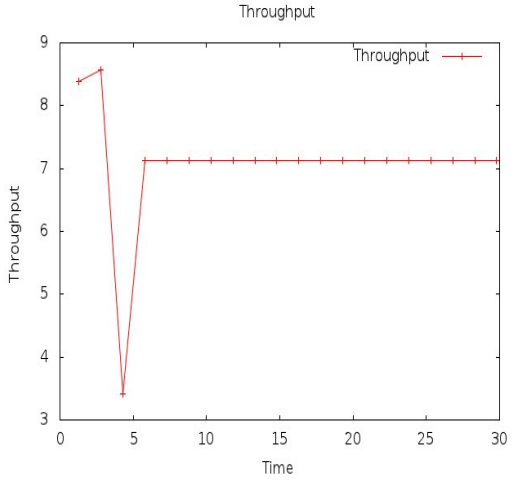

Fig. 14 Throughput graph

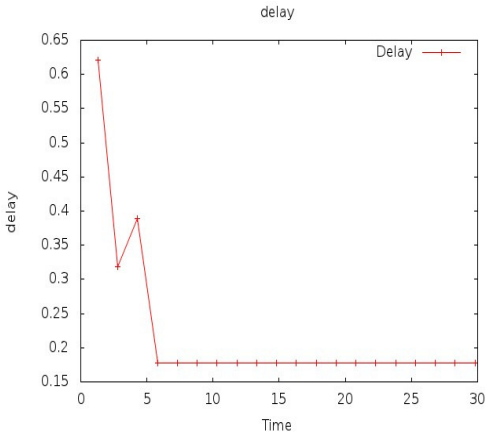

Fig.15 Delay graph

The graphs show that with cooperative black hole more packets reaching the destination are lost. As a result, a variation in value of throughput is seen and delay is somewhat increased also. Here, in this case, all the packets send by the sender does not reaches the destination accurately. That leads to more dropping of throughput value. Value almost decreased to 70%.

Fig. 12 shows the simulation screen in which 50 packets are sent but, all packets are not received properly. Fig. 13 shows the NAM window for the above simulation showing the presence of single malicious node i.e. blackhole. Fig. 14 shows the variance between the throughput and time. As there are cooperative blackholes present so the throughput value decreased to 70% in this scenario i.e. more packets are lost and more retransmissions are required. Fig. 15 shows variance between the delay and time. With more retransmissions delay is increased considerably.

SCENARIO 4: CROSS-CHECKING ALGORITHM IMPLEMENTATION

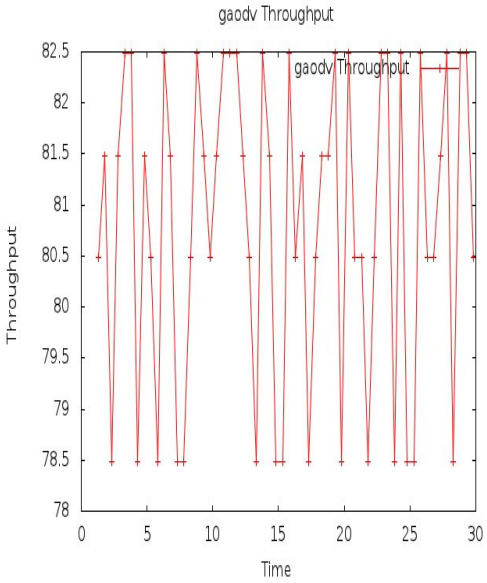

Fig. 16 Throughput graph

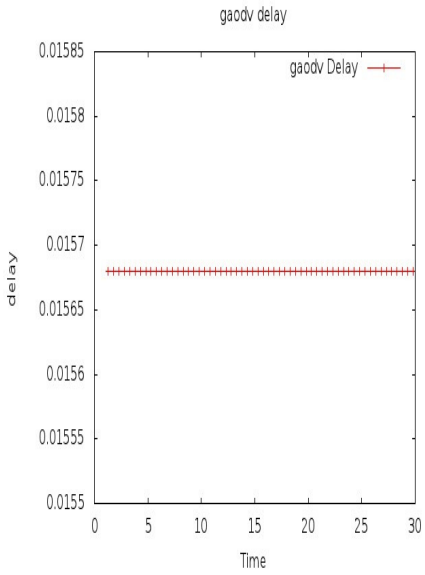

Fig.17 Delay graph

This graph shows that value of the throughput is decreasing and increasing because it searches for the best route avoiding the black holes.

Using the above strategy the delay also lessens and we get less value of delay. Fig. 16 shows the variance between throughput and time. This variance is a bit irregular because this algorithm tries to find the safe route on the basis of DRI entry of each node. So the throughput value is increased upto a considerable amount by using this approach i.e. 80%. Fig. 17 shows the variance between delay and time. Due to this better approach, delay variance comes out to be approx. 0.01565%.

5. CONCLUSION AND FUTURE WORK

In this paper, the detailed study about the cooperative black hole attack is done. When black holes attack in a group they decrease the throughput value and increase the delay. So for this, certain scenarios are implemented. First of all, a neutral case is taken where there is no black hole , then a single black hole is introduced in the network and lastly multiple black holes are introduced which work in coordination with each other. Simulation of all these cases is taken graphically. As a solution to this problem, cross- checking algorithm is implemented, which in return results in increase throughput and lower delay value. But the major drawback with the above implemented algorithm is that the delay value is always constant whatsoever the case. Moreover, throughput value is not very much increased.

As a future work we intend to develop an algorithm that will enhance the throughput and will be more efficient and feasible than the given algorithm.

REFERENCES

[1] Mohit Kumar, Rashmi mishra (2012)"An Overview of MANET: History, challenges and Applications" Printed and published by IJCSE , Vol. 3 No. 1

[2] Al-Roubaiey, T.Sheltami,A.Mahmoud, H.Mouftah(2010) "AACK: Detection for MANET with Node Detection Enhancement" IEEE, 24th Edition.

[3] Vipan Chand Sharma, Atul Gupta, Vivek Dimri (2013) "Detection of Black Hole Attack in MANET under AODV Routing Protocol". International Journal of Advanced Research in Computer Science and Software Engineering volume 3.

[4] Sanjay Ramaswamy,Huirong Fu., John dixit (2013) "Prevention of cooperative Black hole attack in Wireless Adhoc Network", Printed and published by IJREE,

[5] Rajib Das, Dr. Bipul Syam, Dr. Pradipto Das "Security attacks of black hole attack in MANET: An approach, Printed and published in IJARCSSI.

[6] S. Marti, T.J.Giuli, K.Lai, and M.Baker (2000)"Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6Th Annu.Int. Conf. Mobile Computing Networking., Boston, MA, pp.255-265.

[7] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan (2007) "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, pp. 536–550.

[8] Elhadi M.Shakshuki, Nan Kang, Tarek R. Sheltami (2013) "A secure Intrusion Detection system for Manets", IEEE, Vol. 60, No. 3.

[9] Elhadi M. Shashuki, Nan Kang and Tarek R. Sheltami (2013) "EAACK- A Secure Intrusion-Detection System for MANET's", in Proc. IEEE Transactions on Industrial Electronics, Vol 60, pp 1089-1098.

[10] Songbai Lu, Longxuan Li (2009) "SAODV-A MANET Routing protocol that can withstand Black hole attack" International Conference on computational Intelligence and Security.

[11] Kwok-Yan Lam, Lingyan Jia (2009) "SAODV" International Conference on computational Intelligence and Security

[12] Ms. Nidhi Sharma, Mr. Alok Sharma (2012) "The Black hole node attack in MANET" Second International Conference on Advance Computing and Communication Technologies.

[13] Shambhu Upadhyaya, Satish Salem Ramaswami (2006)" Smart Handling of colluding Black hole attack in MANETs and Wireless Sensor Networks using Multipath Routing" Proc. IEEE Workshop on Information Assurance US Military Academy, West Point, NY.

[14] Kishor Jyoti Sharma, Rupam Sharma, Rajdeep Das (2014)"A Survey of Black hole Detection in MANET" IEEE, International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).

[15] Latha Tamilselvan, Dr. V Shankaranarayanan (2007)"Prevention of black hole attack in MANET" 2nd International Conference on wireless Broadband and Ultra Wideband Communications.

[16] Raj PN, Swadas PB (2009) "DPRAODV: A Dynamic Learning System against Black hole Attack in AODV based MANET', International Journal of Computer Science Issue, Vol. 2, pp 54-59.

[17] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) "Improving AODV Protocol against Black hole Attacks", International MultiConference of Engineers and Computer Scientists IMECS Hong Kong, Vol. 2, pp 1-6, 17-19.

[18] Wang W, Bhargava B, Linderman M (2009) "Defending against Collaborative Packet Drop Attacks on MANETs". 2nd International Workshop on Dependable Network Computing and Mobile Systems, New York.

[19] Sun B, Guan Y, Chen J, Pooch UW (2003)" Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom.

[20] Yaser khamayseh, Abdulraheem Bader, Wail Mardini, Muneer BaniYasein (2011) "A New Protocol for Detecting Black Hole Nodes in Adhoc Network", International Journal of Computer Networks and Information Security (IJCNlS), Vol. 3, No. I.

[21] Tanu Preet Singh, Prof. R.K Singh, Jayanl Vats, Manmeel Kaur (2011) "International Conference on Computer Science and Information Technology (lCCSIT'2011)" Pattaya.