# *Reliable Protection Scheme against Cooperative Black Hole Attack in MANET*

Pranav Tripathi
M. Tech Scholar O.I.S.T
Bhopal, India
pranavtripathi1708@gmail.com

Sanjay Sharma
Asst. Prof. O.I.S.T
Bhopal, India
sanjaysharmaemail@gmail.com

Mahendra Singh Sisodia
Asst. Prof. O.I.S.T
Bhopal, India
mahendra14783@gmail.com

***Abstract*— Mobile Ad-hoc networks are a collection of mobile hosts that communicate with each other without any infrastructure. Due to security vulnerabilities of the routing protocols, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. The damage will be serious if malicious nodes work together as a group. This type of attack is called multiple or cooperative black hole attack. In this paper are doing simulation study of network under multiple black hole nodes and identifying the results after applying defense scheme in multiple Black Hole nodes. We simulated black hole attacks in network simulator 2 (ns-2) and measured the packet loss in the network with and without a black hole. We also proposed a simple solution against black hole nodes attack. Our IDS scheme improved the 90% network performance in the presence of cooperative black hole attack.**

*Keywords*— **MANET, AODV, Cooperative Black Hole, TCP, UDP, ns-2.**

## I. INTRODUCTION

This Mobile ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. They usually have a dynamic topology such that nodes can easily join or leave the network at any time and they move around freely which gives them the name Mobile Ad hoc Networks or MANETs. They have many potential applications, especially in military and rescue operations such as connecting soldiers in the battle field or establishing a temporary network in place of one which collapsed after a disaster like an earthquake. In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. To support this connectivity nodes use routing protocols such as AODV [1] (Ad hoc On-Demand Distance Vector). Mobile ad-hoc networks are usually susceptible to different security threats and black hole attack is one of these. In cooperative Black Hole attack, a multiple malicious nodes which absorbs and drops all data packets makes use of the vulnerabilities of the on demand route discovery protocols, such as AODV. In the route discovery process of AODV protocol, intermediate nodes are responsible to connect a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes abuse this process and they immediately respond to the source node with false information as though they have a fresh enough path to the destination. Therefore source node sends its data packets via this malicious node assuming it is a true path.

Black hole [2] behavior may also be due to damaged nodes dropping packets unintentionally. In any case, the end result of the presence of a black hole in the network is lost packets. In our study, we simulated black hole attacks in wireless ad hoc networks and evaluated their effects on the network performance. We made our simulations using ns-2 (network simulator version 2.31). Having implemented a new routing protocol which simulates the black hole behavior in ns-2, we performed tests on different topologies to compare the network performance with and without black holes in the network. As expected, the throughput in the network deteriorated considerably in the presence of a black hole. We also proposed a solution based on ignoring the request established route to disable the adverse effects of the black hole node in an ad-hoc network using AODV as a routing protocol.

We implemented the solution in ns-2 and evaluated the results in case of multiple or cooperative black hole implementation. We presented the improvement due to our proposed solution in the proceeding sections.

The paper organization is as follows: section 2 describes the cooperative Black Hole attacks and related work is

described in section 3. AODV routing is described in section 4 and the proposed solution is described in section 5. Network simulation results are presented in section 6 followed by conclusions and future work in section 7.

## II. Multiple or Cooperative Black Hole Attack

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack in which a malicious nodes makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [3]. This attacks aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attackers. During the route discovery process, the source node sends route request (RREQ) packets to the intermediate nodes to find fresh path to the intended destination. When the source node *S* (Fig. 1) wants to communicate with the destination node *D*, the source node *S* broadcasts the *Route Request* (RREQ) packet. Each neighboring active node updates its routing table with an entry for the source node *S*, and checks if it is the destination node or whether it has the current route to the destination node. If an intermediate node does not have the current route to the destination node, it updates the RREQ packet by increasing the hop count, and floods the network with the RREQ to the destination node *D* until it reaches node *D* or any other intermediate node that has the current route to *D*, as depicted in Fig.1. After connection establishment malicious nodes respond immediately to the source node as these nodes do not refer the routing table shown in fig.2

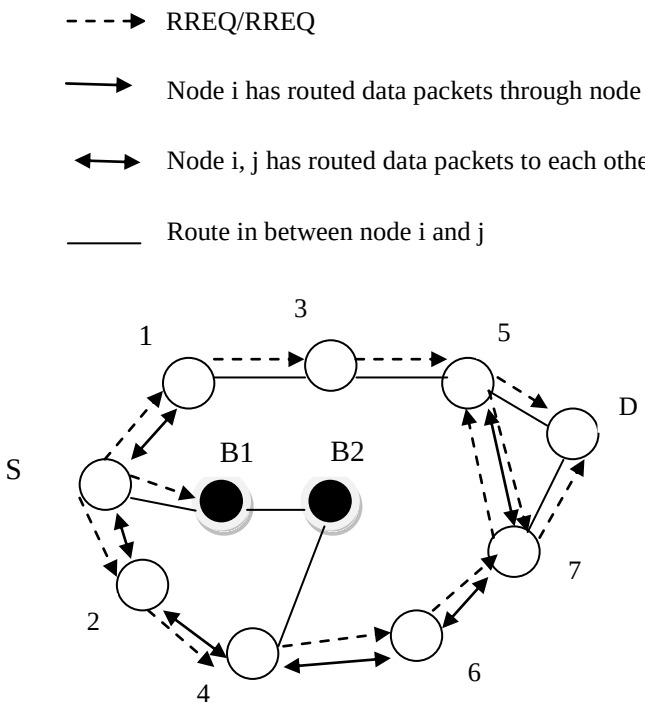


Fig.1 Generate RREQ Message

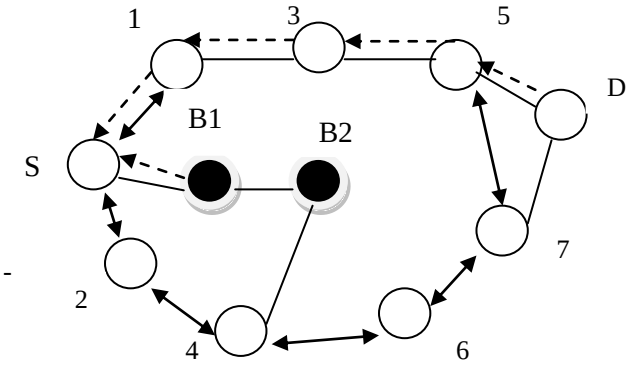


Fig.2 Respond RREP Message

The source node assumes that the RREQ process is complete, ignores (other route reply) RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious nodes do this by assigning a high sequence number to the reply packet. The attackers now drop the received messages instead of relaying them as the protocol requires. Malicious nodes take over all routes by attacking all route request messages. Therefore the quantity of routing information available to other nodes is reduced. The malicious nodes are called black hole nodes. The attack can be accomplished either selectively or in bulk. Selective dropping means dropping packets for a specified destination or a packet every seconds or a packet every packets or a randomly selected portion of packets. Bulk attack results in dropping all packets. Both result in degradation in the performance of the network. Attacker nodes receive a RREQ message, and send RREP message to the source node. So that the source node considers the message has arrived and the communication has been successfully performed. In fact, the message did not reach the destination node.

## III. Related Work

Several researchers have studied the vulnerabilities of ad hoc networks against black hole attacks. Deng et al [4] propose a solution to black hole problem by using one more route to the intermediate node that replays RREQ messages to check whether the route from intermediate node to destination node exists or not. This method avoids the black hole problem and prevents the network from further malicious behavior but the routing overhead is greatly increased. Also, this solution cannot prevent cooperative black hole attacks on MANETs.

Al Shurman et al [5] have proposed two different solutions for black hole. The first solution suggests unicasting a ping packet from source to destination through multiple routes and then chooses a safe route based on the acknowledgement received. The second solution is based on keeping track of sequence numbers so that the black hole nodes which usually modify these sequence numbers can be detected. But these solutions have a longer delay and lower number of verified routes.

Marti et al [6] have proposed a Watchdog and Pathrater approach against black hole attack which is implemented on top of Dynamic Source Routing protocol. The Watchdog module cannot detect misbehaving nodes in the presence of

ambiguous collisions, receiver collisions, limited transmission power, directional antennas, false misbehavior and partial dropping. Since the system avoids the use of cryptographic methods for securing exchanged messages, it suffers from the possibility of black hole attacks.

CONFIDANT (Cooperative of Nodes, Fairness In Dynamic Ad hoc Networks) [7] proposed by Buchegger and Le Boudec is an extended version of Watchdog and Pathrater which uses a mechanism similar to Pretty Good Privacy for expressing various levels of trust, key validation and certification. CONFIDANT allows negative ratings from other nodes resulting in false accusation. Moreover CONFIDANT does not address partial packet dropping.

CORE (Collaborative Reputation) [8] is a reputation based system proposed by Michiardi et al similar to CONFIDANT. CORE consists of a set of reputation tables and a watchdog module. Each function that is monitored has a reputation table and a global RT combines the reputations calculated for different functions. The limitation with CORE is that the most reputed nodes may become congested as most of the routes are likely to pass through them. Also the limitations of the monitoring system in networks with limited transmission power and directional antennas have not been addressed in CORE. Patcha et al [9] have proposed a collaborative architecture for black hole prevention as an extension to the watchdog method.

Bansal et al [10] have proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks), which is the enhanced version of DSR protocol. OCEAN uses a monitoring system and a reputation system to identify malicious nodes. But OCEAN fails to deal with misbehaving nodes properly. These papers have addressed the black hole problem on unicast routing protocols such as AODV or DSR. This scheme in Black Hole Secure-ODMRP (BHS-ODMRP) is implemented on top of the route discovery process of ODMRP where in the security service is distributed over multiple nodes and nodes authenticate each other in a self organized manner.

## IV. AODV Routing Protocol

Ad Hoc On-Demand Vector Routing (AODV) [1] protocol is a reactive routing protocol for ad hoc and mobile networks that maintain routes only between nodes which need to communicate. The AODV routing protocol builds on the DSDV [11] algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, as nodes that are not on a selected path do not maintain routing information. That means, the routing messages do not contain information about the whole route path, but only about the source and the destination. Therefore, routing messages do not have an increasing size. It uses destination sequence numbers to specify how fresh a route is (in relation to another), which is used to grant loop freedom. Whenever a node needs to send a packet to a destination for which it has no route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ (unless it has a 'fresher' one).When the intended destination (or an intermediate node that has a route to the destination) receives the RREQ, it replies by sending a Route Reply (RREP). It is important to note that the only mutable information in a RREQ and in a RREP is the hop count (which is being monotonically increased at each hop). The RREP travels back to the originator of the RREQ (this time as a unicast). At each intermediate node, a route to the destination is set (again, unless the node has a 'fresher' route than the one specified in the RREP). In the case that the RREQ is replied to by an intermediate node (and if the RREQ had set this option), the intermediate node also sends a RREP to the destination. In this way, it can be granted that the route path is being set up bi-directionally. In the case that a node receives a new route (by a RREQ or by a RREP) and the node already has a route 'as fresh' as the received one, the shortest one will be up dated. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP. The AODV protocol is vulnerable to the well-known black hole attack [12].

## V. Proposed solution Against Multiple Black Hole Attack

The proposed scheme uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. Here we analyze the result in three cases i) in Case of normal AODV routing. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP) [13]. Here they are not work out on TCP analysis and other performance parameters. But in this paper we work out on UDP, TCP and other performance parameters.

### A. *Data Routing Information Table*

Each node maintains a data routing information (DRI) table. This table keeps track of whether or not the node did data transfers with its neighbors. This table contains one entry for each neighbor and indicates whether the node has sent data through this neighbor and whether the node has received data from this neighbor. Table entry contains *node id*, *from* and *through* as shown in Table 1. The field *from* stands for information on routing data packets from the node (in the node id field) whiles the field *through* stands for information on routing data packets through the node (in the node id field). Values of *from* and *through* fields will be 0 or 1 to represent false and true respectively. Table 1 shows the sample DRI table for a node 6. The entry 10 for node 5 implies that this node has routed data packets from node 5 but has not routed any data packet through node 5. The entry 11 for node 6 implies that this node has successfully routed data packets

from and through node 4. The entry 00 for node B2 implies that node has not routed any data packets from or through node B 2.

This DRI table is updated when any node received data packet from one of its neighbors or any node that sent data packets through one of its neighbors. In addition, if any node finds out the reliable path to destination which it needs to send the data, DRI table is updated with entries for all intermediate nodes through the path. This reliable route discovery process will be described in details in the following section. From DRI routing we analyze the routing information and behavior of each node.

TABLE I
DRI TABLE OF NODE 6

| Node id | Data Routing Information | |
|---|---|---|
| | From | Through |
| 5 | 1 | 0 |
| 6 | 1 | 1 |
| B2 | 0 | 0 |
| 2 | 0 | 1 |

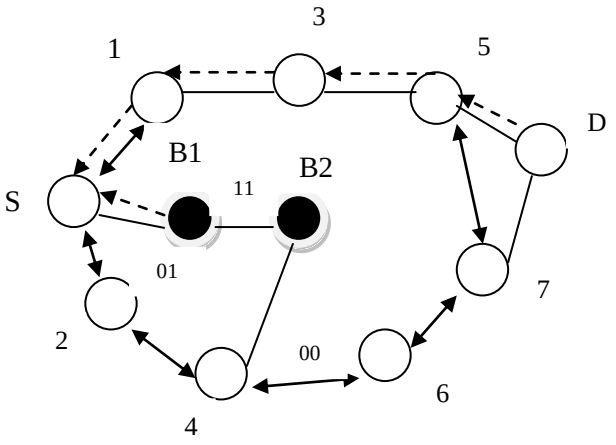


Fig.3 Multiple Black Hole detection

B. *Proposed Algorithm.*

The modified AODV routing protocol and the algorithm for our proposed methodology are described below:

- **Algorithm to prevent cooperative black hole attack in MANETs**

Notations :
SN: Source Node IN: Intermediate Node
DN: Destination Node NHN: Next Hop Node
FRq: Further Request FRp: Further Reply
Reliable Node: The node through which the SN has routed data
DRI: Data Routing Information
ID: Identity of the node
1 SN broadcasts RREQ
2 SN receivesRREP
3 IF (RREP is from DN or a reliable node) {
4 Route data packets (Secure Route)
5 }
6 ELSE {
7 Do {
8 Send FRq and ID of IN to NHN
9 Receive FRp, 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 }

In this protocol, if the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (Route Request) message to discover a secure route to the destination node same as in the AODV. Any node received this RREQ either replies for the request or again broadcasts it to the network depending on the availability of fresh route to the destination. If the destination replies, all intermediate nodes update or insert routing entry for that destination since we always trust destination. Source node also trusts on destination node and will start to send data along the path that reply comes back. Also source node will update the DRI table with all intermediate nodes between source and the destination.

If the intermediate node (IN) generates the Route Reply (RREP), it has to provide its next hop node (NHN) and its DRI entry for the next hop node. When the reply comes back, it collects the IP addresses of all nodes between source and the intermediate node but no intermediate node updates the route entry for the destination. Upon receiving RREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node or not. If the source node has used IN before to route data, then IN is a reliable node and source will first send a route establishment message to IN node along the path that RREP comes according to the information contains in the RREP message. Upon receiving this message all nodes between the source and the intermediate node will update or insert route entry for the destination. Then source node starts sending data through the IN and updates the DRI table with nodes between source and IN node. If the source has not routed data through IN before, IN is not a reliable node. Then source first stores the information about IN and the nodes between the source and IN, and sends Further Request (FREQ) message to NHN of the IN to verify the reliability of the IN and ask NHN:

1) Whether the IN has routed data packet through NHN.
2) Who is the current NHN's next hop to the destination?
3) Has the current NHN routed data through its own next hop?

Then NHN in turn responds with Further Reply (FREP) message which includes:

1) DRI entry for IN.
2) The next hop node (NHN) of current NHN, and
3) The DRI entry for the current NHN's next hop.

If the current NHN is the destination, then the next hop entry and the DRI entry for the next hop fields of FREP contain zeros and all intermediate nodes will either update or insert route entry for the destination. When the source receives FREP from destination, it starts routing data and updates its DRI table with all nodes between the source and the destination. If NHN is not the destination, based on the FREP message from NHN, the source node checks whether NHN is a reliable node or not. If the source node has routed data through NHN before, NHN is reliable; otherwise NHN is unreliable. Also the source node will check whether IN is a black hole or not. If the second bit of the DRI entry from IN is equal to 1 (i.e. IN has routed data through NHN) and the first bit of the DRI from NHN for IN is equal to 0 (i.e. NHN has not routed data from IN) then IN is a black hole node. Also, if the current NHN's next hop is an already visited node (node between current NHN and the IN that reply for the RREQ) then current NHN is a black hole node. If the current IN or NHN is a black hole node then source node identifies all the nodes in the reverse path from current IN or NHN to the node that generate RREP as black hole nodes. Then source node starts the secure route discovery process from beginning and sends the RREQ again. Source node ignores any other RREP messages from any black hole nodes and broadcasts the list of cooperative black holes to notify others. If IN is not a black hole node and the NHN is a reliable node, then route to destination is secure. Source node will update its DRI table with entries for all nodes from source to IN with 01 and start routing data via IN. If the NHN is an unreliable node, the source node treats the current NHN as IN and send FREQ to the updated IN's next hop node and goes into the steps described above.

## VI. Simulation Environment

The detailed simulation model is based on network simulator-2 (ver-2.31) [14], is used in the evaluation. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver to create the statistical data track file and so on.

### A. *Simulation Parameters for Case Study.*

In our scenario we take 30 nodes in which 0 to 27 nodes are simple nodes, and node 28 and 29 are malicious nodes or Cooperative Black Hole nodes. The simulation is done using ns-2, to analyze the performance of the network by varying the nodes mobility. The evaluated performances are given below. We are taking the following parameters for case study shown in table 2. The given simulation parameters are selected after numbers of simulations because if we generate the results and calculate the values in all three cases are never conflict with other.

TABLE III
Simulation Parameters for Case Study

| | |
|---|---|
| Number of nodes | 30 |
| Black hole nodes | 2 |
| Dimension of simulated area | 800×600 |
| Routing Protocol | AODV |
| Simulation time (seconds) | 100 |
| Transmission Range | 250m |
| Traffic type (UDP,TCP) | CBR |
| Packet size (bytes) | 512 |
| Number of traffic connections | 20 |
| Maximum Speed (m/s) | 30 |

### A. *Performance Metrics*

In this paper we focus on evaluating the protocols under Black hole or malicious nodes attack with following criteria [15, 16]:

- *Delivery Ratio (PDR:* The ratio of data delivered to the destination to the data sends out by source. The greater value of packet delivery ratio means the better performance of the protocol.
- *Throughput:* The total amount of data a receiver actually receives from sender divided by the time taken by the receiver to obtain the last packet.
- *End to End Delay*: The difference in the time it takes for a sent packet to reach the destination. It includes all the delays, in the source and each intermediate host, caused by the routing discovery, queuing at the interface queue etc.
- *Normalized routing overhead:* This is the ratio of routing-related transmissions (RREQ, RREP, RERR etc) to data transmissions in a simulation. A transmission is one node either sending or forwarding a packet. Either way, the routing load per unit data successfully delivered to the destination.
- *Packet lost:* Total number of packets dropped during simulation. The lower value of packet lost means the better performance of the protocol.

### B. *Results*

In this section we present a set of simulation experiments to evaluate this protocol by comparing with the original AODV [1] routing protocol.

1) *Scenario of Multiple Black Hole Nodes:* In this figure we represent the nam scenario of thirty nodes in which node 28 and 29 are malicious nodes and rest of them are normal nodes. All the nodes are mobile nodes first they sense the neighbour then transmit data according to protocol.

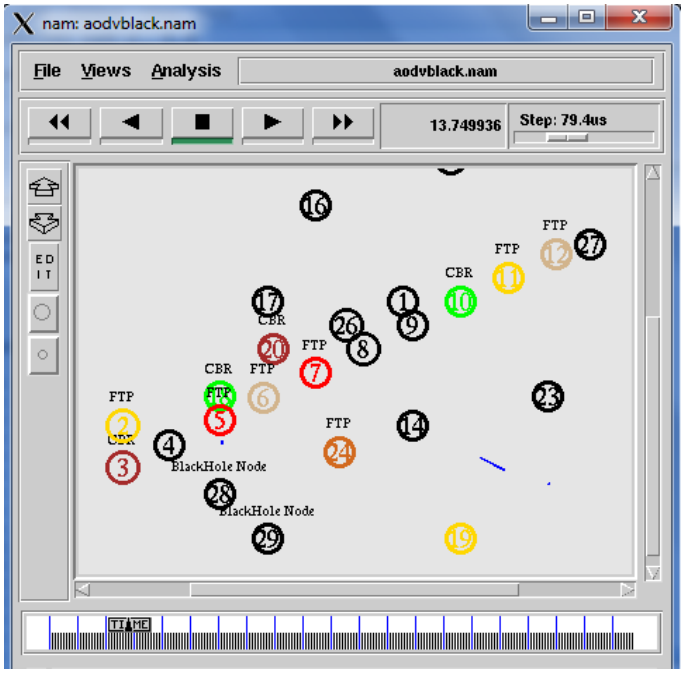


Fig.4 A nam scenario of Cooperative Black Hole nodes.

2) *UDP Packets Analysis*: In UDP analysis first we consider the normal routing case. In normal routing case about 2250 UDP packets are received. But In attack case negligible data packets are reached to destination all packets are dropped. But after applying IDS on Black Hole attack we observe that about 90% of data are received. Here we notice that after applying IDS packet receiving increases and dropping of packets decreases.

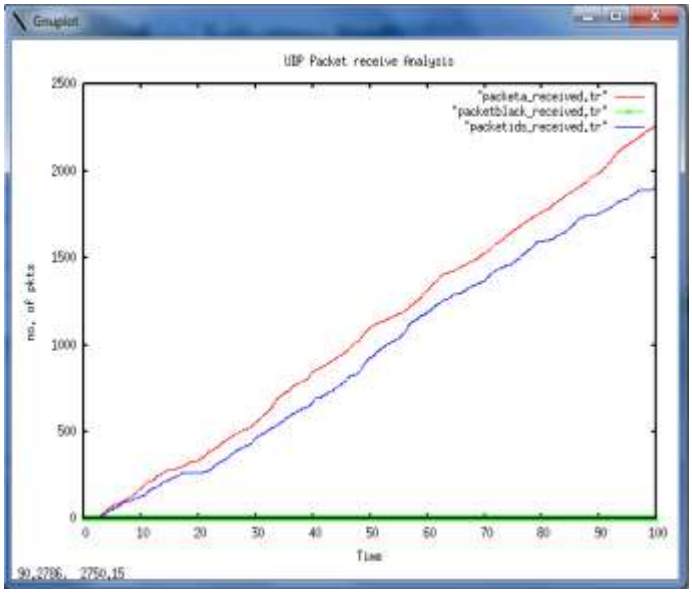


Fig.6 UDP packet receiving analysis in all three cases

3) *Analysis of TCP Congection Window:* Here we represents the analysis of TCP packets in normal AODV routing case, in case of coopereative Black Hole attack and in case of after applying IDS. At the time attack the TCP packets receiving rate decreases about 10% of data received on destination but after applying IDS receiving rate are almost equal to normal AODV routing case.

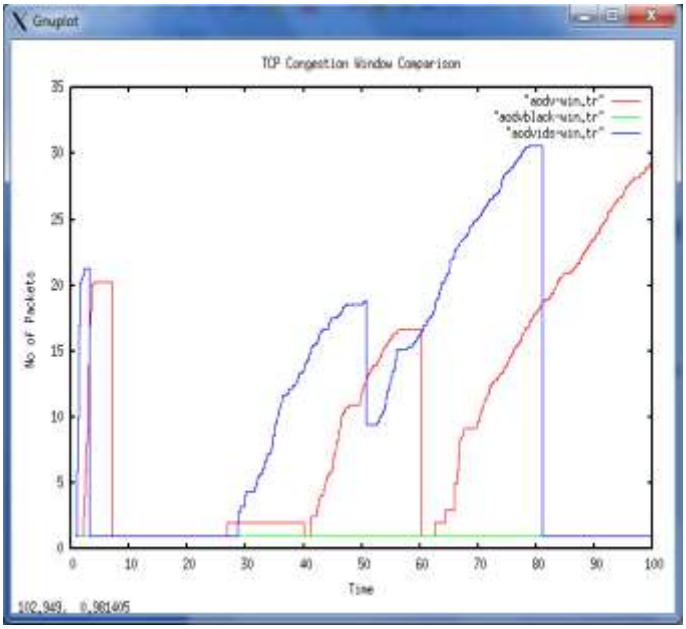


Fig.5 TCP packets receiving analysis

4) *Packet Delivery Fraction (PDF) Analysis:* PDF analysis in normal or attack free case successful data receiving is 94% but at the time of attack data receiving percentage is unpredictable only .2% or nearly equal to zero. Now After applying IDS scheme now again network overcome from attack and provide 88% of data receiving. Only 6% less then from normal case.

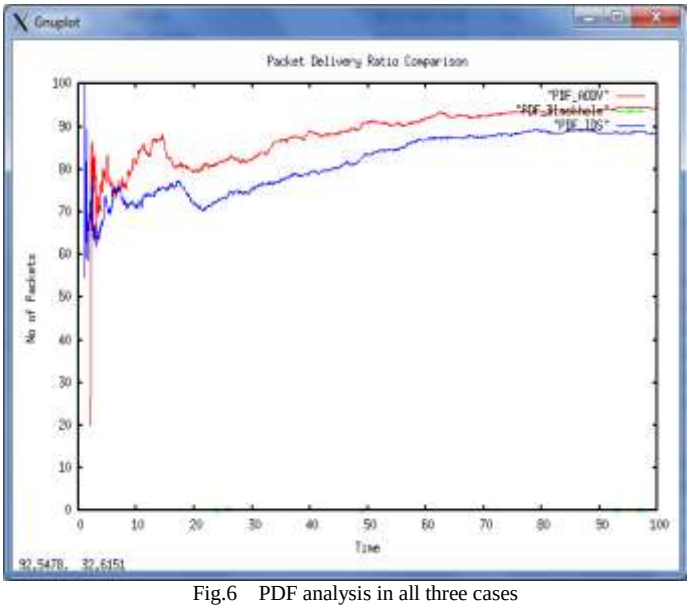


Fig.6 PDF analysis in all three cases

5) *Throughput Analysis:* Throughput analysis in the case of attack reaches to nearly zero level means negligible packets are received at destination as compare to throughput in normal case but after applying IDS data is recovered and throughput increases from time 1sec. to 70sec. and after that nearly equal to normal case. At the

time of attack number of packets are not shown in given fig. due to nedgligible packet delivery.

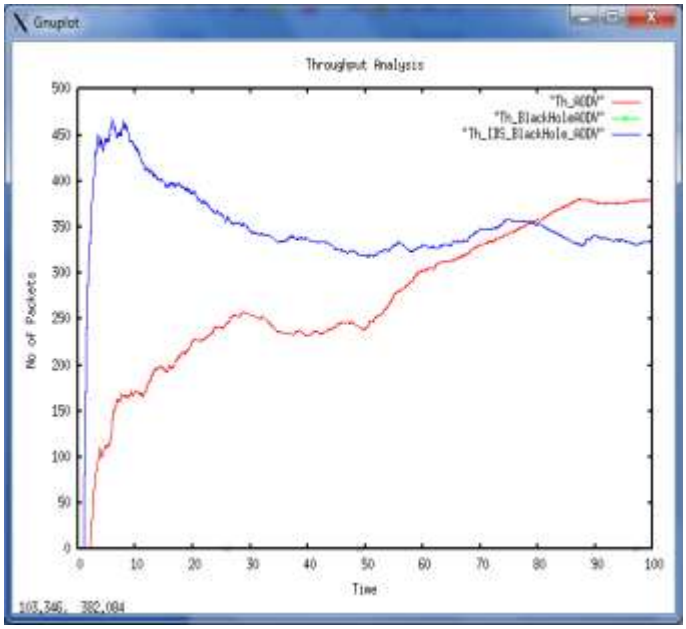


Fig.7 Throughput analysis in all three cases.

6) *Routing Load Analysis:* In routing load analysis we observe that in case of attack about 700 routing packets are delivered but negligible data packets are received. In normal routing case and in case of IDS nearly equal numbers of routing packets are delivered but PDF are excellent in both cases see in fig.6.

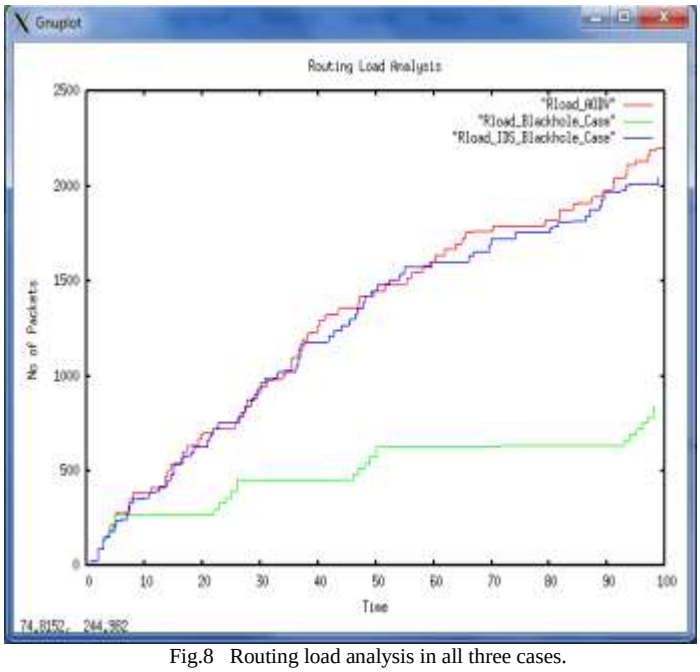


Fig.8 Routing load analysis in all three cases.

7) *Overall Summery of Analysis:* In overall analysis we represent the summery of all performance parameters shown in table 3. This table shows the network performance according to simulation parameters.

TABLE IIIII
OVERALL SUMMERY

| Performance Parameters | Normal Case | Attack Case | IDS Case |
|---|---|---|---|
| Packets Send | 5621 | 2498 | 5728 |
| Packets Received | 5299 | 5 | 5053 |
| Routing Packets | 2233 | 844 | 2046 |
| NRL | 0.42 | 168.8 | 0.4 |
| PDF | 94.27 | 0.2 | 88.22 |
| End to End delay(ms) | 745.65 | 32.03 | 970.33 |
| Data Drop in Packets | 312 | 2493 | 617 |
| Data Drop in bytes | 249600 | 1994400 | 493600 |

## VII. CONCLUSIONS AND FUTURE WORK

In this paper we have gone through the routing security issues of MANETs, described the cooperative Black Hole attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to a) Identify multiple black hole nodes cooperating with each other in a MANET; and b) Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. Also we showed that the effect of packet delivery ratio and throughput has been detected in case of attack. There is reduction in Packet Delivery Ratio and Throughput. In Black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to network and nodes as shown in the result of the simulation. In Future we also work out on effect of attack on Node Energy, location based routing and Multicast routing protocols.

## REFERENCES


[1]. IETF MANET Working Group AODV Draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-08.txt, Dec 2002.

[2]. Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE communications surveys & tutorials, Vol. 10, no. 4, pp. 78-93, 2008.

[3]. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Blackhole Attack in Wireless Ad Hoc Networks", In Proc. of 2003 Int. Conf. on Wireless Networks, ICWN'03, Las Vegas, Nevada, USA, 2003, pp. 570–575.

[4]. H. Deng, W. Li, and Dharma P. Agrawal, " Routing Security in Ad Hoc Networks", IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, October 2002, pp. 70-75.

[5]. Al-Shurman, M. Yoo, S. Park, "Black hole attack in Mobile Ad Hoc Networks, ACM Southeast Regional Conference", 2004, pp. 96-97.

[6]. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000), "Mitigating routing misbehavior in mobile ad-hoc networks", Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom), ISBN 1-58113- 197-6, pp. 255-265.

[7]. S. Buchegger, C. Tissieres, and J. Y. Le Boudec. "A test bed for misbehavior detection in mobile ad-hoc networks", –how much can watchdogs really do. Technical Report IC/2003/72, EPFL-DI-ICA, November 2003. Available on:citeseer.ist.psu.edu/645200.html.

[8]. P. Michiardi and R. Molva. Core: "A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", In Proceedings of the 6th IFIP Communications and

Multimedia Security Conference, pages 107 121, Portorosz, Slovenia, September 2002.

[9]. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks", Radio and Wireless Conference, 2003. RAWCON '03, Proceedings, pp. 75-78, 10-13 Aug. 2003.

[10]. S. Bansal and M. Baker. "Observation-based cooperation enforcement in ad hoc networks", July 2003. Available on: http://arxiv.org/pdf/cs.NI/0307012.

[11]. Perkins and P. Bhagwat. "Routing over multihop wireless network for mobile computers", SIGCOMM '94 : Computer Communications Review:234-244, Oct. 1994.

[12]. Arshad, J.; Azad, M.A.; , "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks," Sensor and Ad Hoc Communications and Networks, SECON '06. 2006 3rd Annual IEEE Communications Society on , vol.3, no., pp.971-975, 28-28 Sept. 2006.

[13]. N.Bhalaji, Sinchan, Dr.A.Shanmugam **"**A novel routing technique against Packet dropping attack in Adhoc networks**",** in Journal of Computer science, USA Volume 4(7), 2008. pp 538-544.

[14]. Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns.

[15]. AODV Protocol against Blackhole Attacks," Procedings of the international multi conference of engineer and computer science Vol 2, 2010.

[16]. Juwad, M.F.; Al-Raweshidy, H.S.; , "Experimental Performance Comparisons between SAODV & AODV," Modeling & Simulation, AICMS 08. Second Asia International Conference on, vol., no., pp.247-252, 13-15 May 2008.