# Protecting Against Alliance Attacks By Malicious Nodes In MANETs Using CBDS Technique With Originating Message

R.Arun[1], Mr.M.Suresh Anand[2]
[1]P.G student, Sri SaiRam Engineering College, Chennai.
[2] Associate Professor, Sri SaiRam Engineering College, Chennai.

***Abstract- In mobile ad hoc networks (MANETs) are designed based on the assumption that all participating nodes are fully cooperative. Any nodes, in wireless ad hoc network, always uses on intermediate nodes to send the packets to the required destination node. In case of the presence of malevolent nodes, this setup may lead to severe security concerns; for example, such nodes may interrupt this routing process.The malicious nodes are try to launch the grayhole or collaborative blackhole attacks in a network. Collaborative bait detection Scheme (CBDS) with Orginating message is used to resolve this drawback and to protect MANETs against miscreants.CBDS based on Dynamic Source Routing Protocol that integrate the advantage of both proactive and reactive defense architectures is used to detect the malicious nodes.***

***Index Terms-*** **Cooperative Bait Detection Scheme (CBDS), Collaborative Blackhole Attacks, Detection Mechanism, Dynamic Source Routing (DSR) Protocol, Grayhole Attacks, Malicious Node, Mobile Ad Hoc Network(MANET).**

## I. INTRODUCTION

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies.

Ad hoc networks are self-organizing also self-configuring multihop wireless networks where, their structure changes dynamically. This is because of their mobility nature. The nodes in the network act as a router not only as a host to route the data in the network.

MANETs form a peer-to-peer,self-forming,self-healing usually has a routable networking environment on top of a Link Layer ad hoc network in contrast to a mesh network.

A collection of mobile hosts with wireless network interfaces may form a lacking continuity without the help of any established infrastructure or centralized administration. This type of wireless network is known as an *ad hoc network*.

In ad hoc networks devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it.

In Figure 1, mobile host *C* is not within the range of host *A*'s (denotes as a ciicle A) and host *A* is not within the range of host *C*'s wireless transmitter. If *A* and *C* wish to exchange packets, they may in this case enlist the services of host *B* to forward packets for them, since *B* is within the overlap between *A*'s range and *C*'s range.

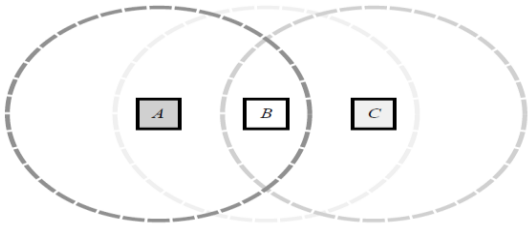


**Figure 1 : A Simple Ad hoc network of three wireless mobile hosts**

There are two sources of menace to routing protocols. The external attackers are the one by injecting wrong

routing information or reply a old routing information could successfully divide a network or set up a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures. The applications of MANETs is distinctly dissimilar, ranging from small, static networks that are forced by power sources, to large-scale dynamic networks. The design for this network is a complex issue.To determine network organization, link scheduling, and routing in MANETs by using efficient distributed algorithms

1.1 CHARACTERISTICS

Mobile Adhoc Network (MANET) is a collection of independent mobile nodes that can transmit an information to each other via radio waves. The nodes with in an radio range can directly transmit an information whereas others need the aid of intermediate nodes to route their packets. These networks are It is a fully distributed network and can work at any place without the help of any infrastructure.These networks is highly exile and robust.

1.2 APPLICATIONS OF MANETS

There are many applications to ad hoc networks.In our day-to-day application such as electronic email and file transfer can be considered to be easily deployable with in an ad hoc network environment.Some well known mobile adhoc network applications are:

Collaborative Work – For some business environments, the need for collaborative computing might be more important outside office environments than inside.In some cases the people do need to have the outside meetings to cooperate and exchange information on a given project.

Crisis-management Applications – At the time of natural disasters the entire infrastructure is in disarray so the Restoring of communications quickly is essential. By using ad hoc networks, an infrastructure could be set up in hours instead of days/weeks required for wire-line communications.

Personal Area Networking and Bluetooth – A personal area network (PAN) is a short-range, localized network the nodes are attached with the someone's pulse watch, belt, and so on. Bluetooth is a technology aimed at, among other things, supporting PANs by eliminating the need of wires between devices such as printers, PDAs, notebook.

1.3 ADVANTAGES

The advantages of MANETs are : To provide the easy way of access the information and services inspite of geographic position.It is a dynamic in nature so it can be establish at any place and time.It works without any pre-existing infrastructure.

1.4 TYPES OF ROUTING PROTOCOLS

Three main routing protocols for a MANET are Destination-Sequenced Distance Vector routing protocol (DSDV),Ad hoc On-Demand Distance Vector routing protocol (AODV), and Dynamic Source Routing protocol (DSR).

DSDV is a table-driven routing protocol based on the classical Bellman-Ford routing mechanism. In this routing protocol, each mobile node in the system maintains a routing table in which all the possible destinations and the number of hops to them in the network are recorded.

AODV Routing Protocol uses an on-demand approach for finding routes is established only it is required by a source node for transmitting data packets.The most recent path is identified by using the destination sequence numbers.

Dynamic Source Routing Protocol is simple and efficient and is specially designed for use in multihop wireless adhoc network of mobile nodes.Our CBDS Method based on Dynamic Source Routing Protocol.It is similar to AODV in that forms route on-demand when a transmitting node requests. However it uses source routing instead of relying on the routing table ata each intermediate device.

## II. DYNAMIC SOURCE ROUTING PROTOCOL

DSR is an on-demand routing protocol and it maintains a route cache, which leads to memory overhead. DSR does not have any detection mechanism,but the source node can get all route information concerning the nodes on the route.DSR has a higher overhead as each packet carries the complete route, and does not support multicast.

Dynamic source routing protocol offers a number of potential advantages over conventional routing protocols such as distance vector in an adhoc network.First,unlike conventional routing protocols,our protocol uses no periodic routing

advertisement messages.It reducing the network bandwidth overhead and it will useful during little or no significant host movement is taking place.

DSR has two main process : Route Discovery and Route Maintenance.

2.1 ROUTE DISCOVERY

Route Discovery allows any host in the ad hoc network to dynamically discover a route to any other host in the ad hoc network, whether directly reachable within wireless transmission range or reachable through one or more intermediate network hops through other hosts.

A host initiating a route discovery broadcasts a *route request* packet which may be received by those hosts within wireless transmission range of it. The route request packet identifies the host, referred to as the *target* of the route discovery, for which the route is requested. If the route discovery is successful the initiating host receives a *route reply* packet listing a sequence of path through which it may attain the point.

2.2 ROUTE MAINTENANCE

It monitors the operation of the route and informs the sender if there is any routing errors. If the status of a link or router changes, the changes are update in entire routers participate in the network.Route maintenance can also be performed using end-to-end acknowledgements rather than the hop-byhop acknowledgements.

Route Maintenance is possible.In hop-by-hop acknowledgements, the particular hop in error is indicated in the route error packet, but with end-to-end acknowledgements, the sender may only assume that the last hop of the route to this destination is in error.

III. COOPERATIVE BAIT DETECTION SCHEME

Cooperative bait detection scheme (CBDS)] is based on Dynamic Source Routing Protocol is used to detect the malicious node in the network.The malicious nodes can attract all the packets or some of the packets without forwarding it to the destination.The malicious nodes can loss the packets by using the Gray hole/Collaborative Black hole attacks.In Collaborative Bait Detection Scheme,the address of an near by node is used as bait destination address to send a RREQ to all of its nodes.But the bait malicious nodes to send a reply RREP message and it will update the details in the route cache and the exact malicious nodes are detected using a reverse tracing technique.

The detected malicious nodes is update in the black hole list to help the other nodes to avoid the malicious path to send the packets.

3.1 COOPERATIVE BLACK HOLE ATTACKS

A black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack.

3.2 GRAY HOLE ATTACKS

A gray hole attack is a variation of the black hole attack,where the malicious node is not initially malicious, it turns malicious sometime later.The Grayhole attack is drop the some of packets to send to the destination.

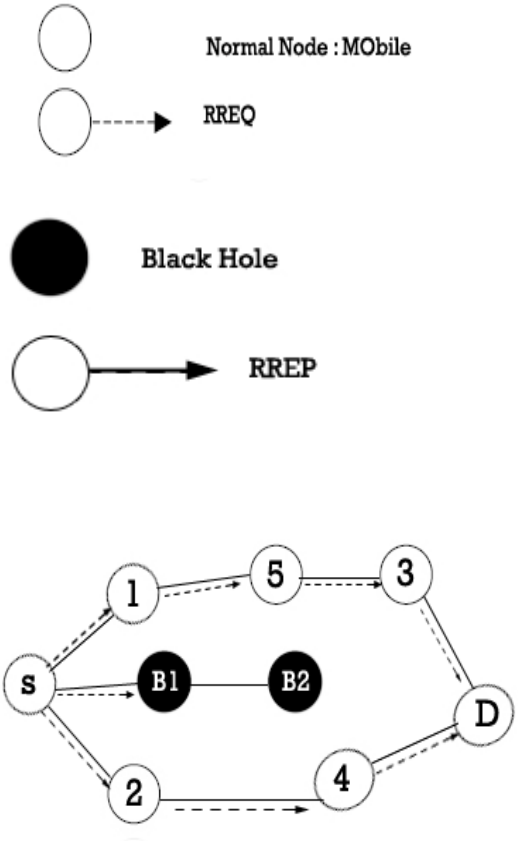


**Figure 2 : Propagation of RREQ Message.**

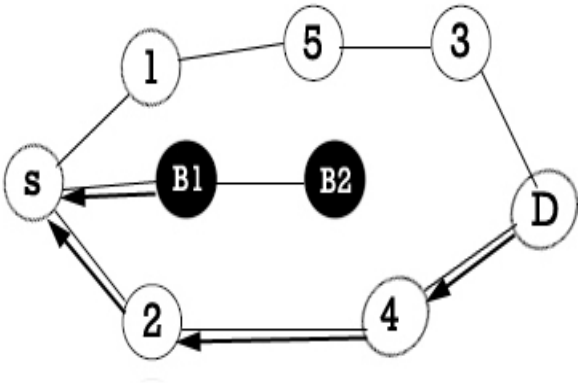


**Figure 3 : Propagation of RREP Message.**

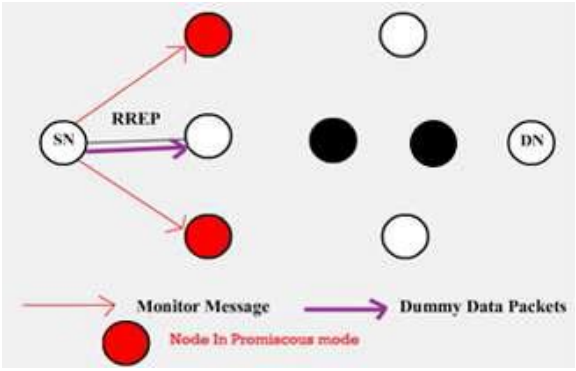


**Figure 4 : Propagation of Monitor message & dummy data packets.**

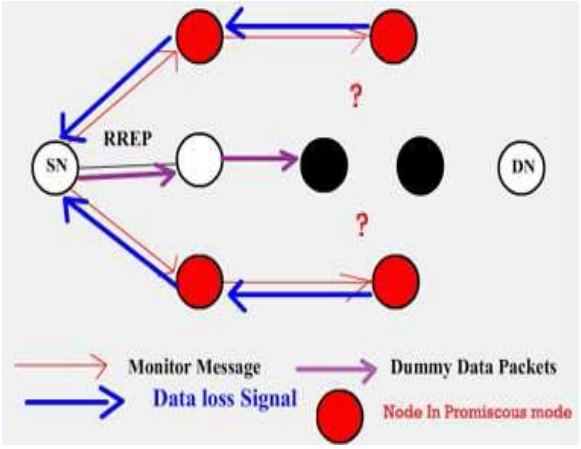


**Figure 5 : Identification of the Black Hole by promiscous nodes.**

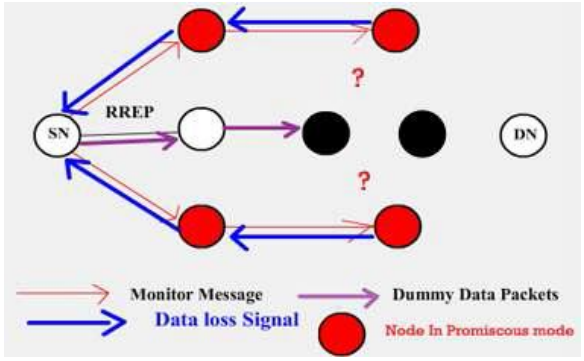


**Figure 6 : Propagation of Data loss Signal back to the Source Node.**

3.3 : GRAY/BLACK HOLE REMOVAL PROCESS

Actions by Source node on receiving the RREP

Step 1: If the RREP is received only to the Destination & not to the Restricted IP(RIP), the node carries out the normal functioning by transmitting the data through the route.

Step 2: If the RREP is received for the RIP, it initiates the process of black hole detection, by sending a request to enter into promiscous mode, to the nodes in an alternate path(i.e. neighbours of next hop for RIP).

Step 3: The feedback sent by the alternate paths are analyzed to detect the black hole & this information is propagated throughout the network, leading to the revocation of the Black Holes certificates.

In general, detection mechanisms that have been proposed in to

1) Proactive detection schemes that reguraly detect the nearby nodes to check if the node is malicious node or normal node.It detect the malicious node reguraly so its resources are wasted.The main advantage is to prevent or detect the attack in its initial stages.

2) Reactive detection schemes are used to detect the malicious node during the significant drop in the packet delivery ratio.The resource wastage is reduced because it can monitor the route during the packet loss.

The CBDS scheme comprises three steps: 1) the initial bait step; 2) the initial reverse tracing step; and 3) the shifted to reactive defense step, i.e., the DSR route discovery start process. The first two steps are initial proactive defense steps,whereas the third step is a reactive defense step.

1.THE INITIAL BAIT STEP

Initial Bait Step is used to identify whether the path has malicious node or not.In bait node,one of the neighbor node of the source chosen as bait node.Source node send the RREQ to all the nodes in order to identify the malicious path in the network.The Bait node should not receive the request and send the reply.Normal nodes receive the route request and match destination address with its own address.If the destination address does not match with its address then forward the RREQ to neighbour node.But in case the malicious node take the destination address as its own and send RREP as similar as bait to the Source.Source node record the path in to the routing table for further reference.Source node recognize the path consists of malicious node.

2.THE INITIAL REVERSE TRACING STEP

Reverse Tracing Program is used to detect the behavior of nodes through the Route Reply Message.In Reverse Tracing Technique applied to find the exact address of the hacker node.Route Reply RREP contains the path from source to the destination which has not presence of the bait node.If the path contains the address of the bait node,then that node is the malicious node.After identifying the malicious node information of the malicious node get from its neighbor node. Source Node send RREQ to all of node in the network.Destination node send RREP to source node checks the nodes in the path with routing table.

3.THE SHIFTED TO REACTIVE DEFENSE STEP

If the selected path has malicious node choose alternate path to send the data.If there is no malicious node in the path,Source node sends the data to destination.Using this method we can avoid the significant packet loss in the network.It is an On Demand network so we can implenment depend on our needs.

## IV. SYSTEM DESIGN

### 4.1 DATA UNIT

Data Unit is used to process the data.It is used to Store and retrieve the data.

### 4.2 ROUTE DISCOVERY

It is used to discover the new route to send the data packets. Route Discovery allows any host in the ad hoc network to dynamically discover a route to any other host in the ad hoc network.

### 4.3 ROUTE MAINTENANCE

Route Maintenance is used to maintain and recover in case of failure occur in route.Route Discovery and Route Maintenance are combined to allow nodes to discover and to maintain source routes to arbitrary destinations in the adhoc network.

### 4.4 ROUTING MANAGER

Routing Manager is used to manage all the activities in the network.It is used to transmit and receive the data in the network.

### 4.5 BEHAVIOUR ANALYZER

It is used to analyse the behaviour of the node.To Check whether the node is Good or Bad.

### 4.6 ROUTE CACHE

To update those network are participated in route.It can store the all node details including the hacker node.

### 4.7 TRANSMITTER/RECEIVER

It can transmit or receive the data in the network.

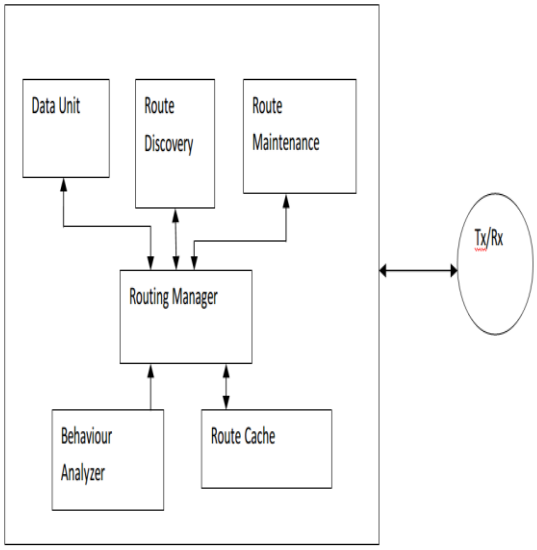


**Figure 7 : Architecture Of CBDS**

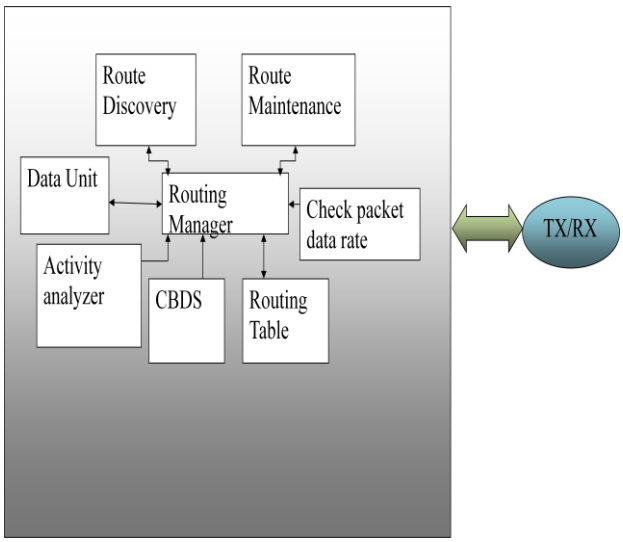


**Figure 8 : Architecture Of CBDS With Originating Message**

4.8 CHECK PACKET DATA RATE

To check whether the entire data packets are reached to the destination or not.If not the Destination node to intimate the source node to recheck the path in the network.

4.9 COOPERATIVE BAIT DETECTION SCHEME

Cooperative bait detection scheme (CBDS)] is based on Dynamic Source Routing Protocol is used to detect the malicious node in the network.The malicious nodes can attract all the packets or some of the packets without forwarding it to the destination.The malicious nodes can loss the packets by using the Gray hole/Collaborative Black hole attacks.In Collaborative Bait Detection Scheme,the address of an neighbor node is used as bait destination address to send a RREQ to all of its nodes.But the bait malicious nodes to send a reply RREP message and it will update the details in the route cache and the exact malicious nodes are detected using a reverse tracing technique.

The detected malicious nodes is update in the black hole list to help the other nodes to avoid the malicious path to send the packets.

## V. PERFORMANCE METRICS

We have compared the CBDS against the DSR 2ACK and BFTR schemes, chosen as benchmarks, on the basis of the following performance metrics.

1) PACKET DELIVERY RATIO

This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source.

we study the packet delivery ratio of the CBDS and DSR for different thresholds when the percentage of malicious nodes in the network varies from 0% to 40%.The maximum speed of nodes is set to 20m/s. Here, the threshold value is set to 85%, 95%, and the dynamic threshold, respectively. The results are captured in Figure 9. It can be observed that DSR drastically suffers from blackhole attacks when the percentage of malicious nodes increases. This is attributed to the fact that DSR has no secure method for detecting/preventing blackhole attacks. Our CBDS scheme shows a higher packet delivery ratio compared with that of DSR.

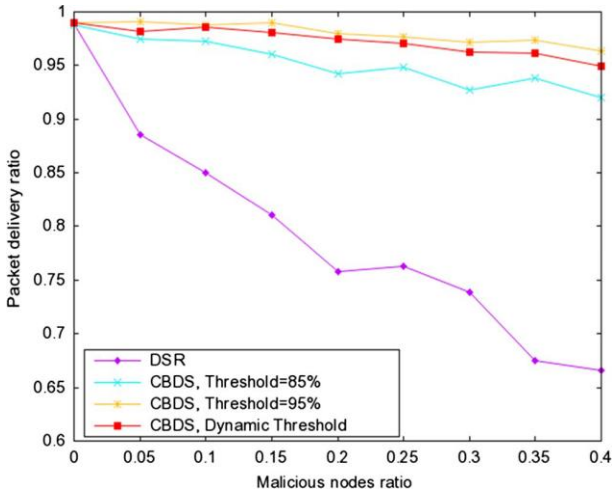


**Figure 9 : Packet delivery ratio of DSR and the CBDS for different thresholds.**

2) ROUTING OVERHEAD

This metric represents the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions.

we study the routing overhead of the CBDS and DSR for different thresholds. The results are captured in Figure 10.It can be observed that when the number of malicious nodes increases, DSR produces the lowest routing overhead compared with the CBDS.
This is attributed to the fact that DSR no intrinsic security method or defensive mechanism.

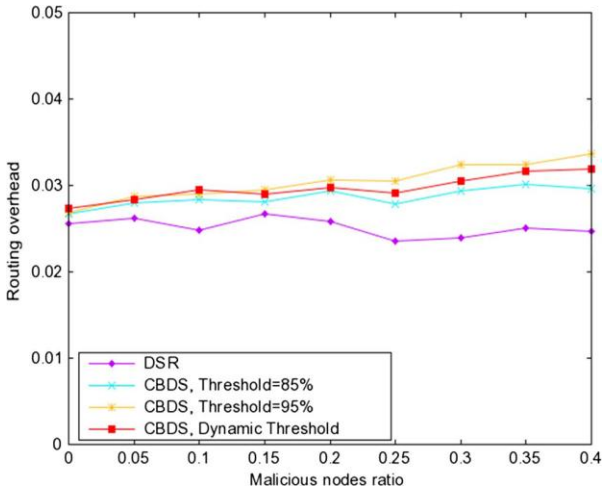


**Figure 10 : Routing overhead of DSR and the CBDS for different thresholds.**

3) AVERAGE END-TO-END DELAY

This is defined as the average time taken for a packet to be transmitted from the source to the destination.

In Figure 11, it can be observed that the CBDS incurs a little bit more end-to-end delay compared with that of DSR. This is attributed to the fact that the CBDS necessitated more time to bait and detect malicious nodes. Therefore, a tradeoff must be made between end-to-end delay and packet delivery ratio.

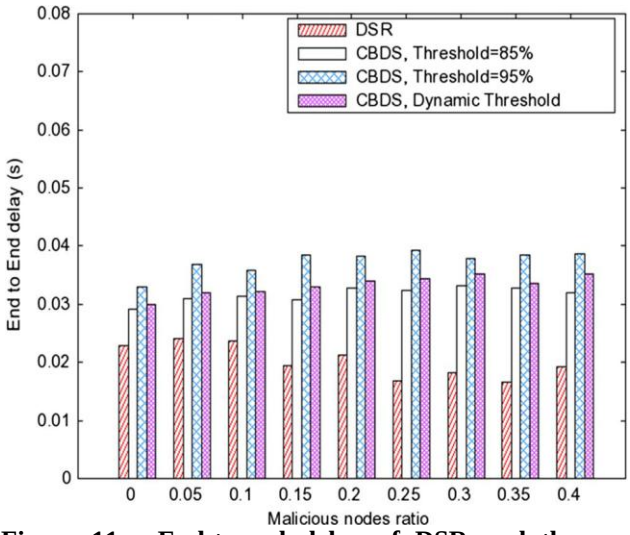


**Figure 11 : End-to-end delay of DSR and the CBDS for different thresholds.**

4) THROUGHPUT

This is defined as the total amount of data that the destination receives them from the source divided by the time it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second.

In Figure 12 it can be observed that DSR suffers the most from maliciousnode attacks compared with the CBDS. In addition, the CBDS with different thresholds results in higher throughput than DSR.

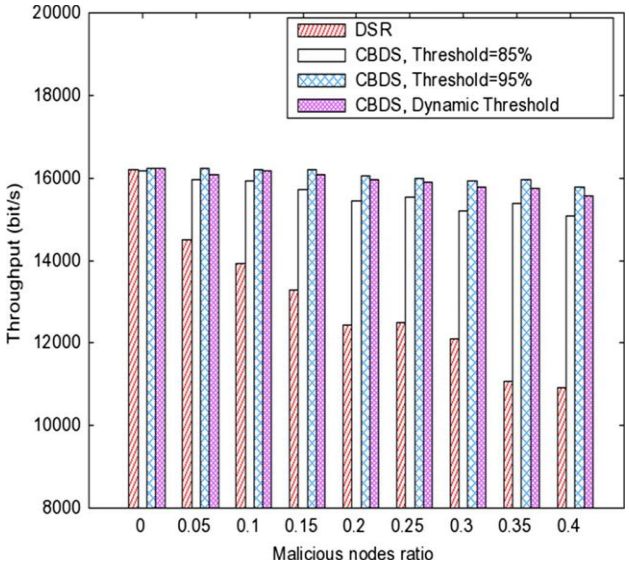


**Figure 12 : Throughput of DSR and the CBDS for different thresholds.**

## VI. CBDS WITH ORGINATING MESSAGE

Cooperative Bait Detection Scheme with Orginating Message is used to detect the hidden hacker node in the network.In this method Destination node check the data rate of the data packets delivered from source to destination.If the data packets are delayed or loss to reach to destination.The destination node trigger the reply to source there is hidden hacker is present in the network.Source node send the recommendation message to neighbor nodes for to identify the details of the hacker node in the route.Neighbor node collect the details of each node if there is any packet loss it collect the information and send the details to source node.Source node update the malicious node details in the route cache.Source node will select the good route to send the data to the destination node.

## VII. CONCLUSION

Cooperative Bait Detection Scheme With Orginating Message is used to reduce the packet loss and the delay and to increase the overall network throughput using the destination check route information.

## REFERENCES

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai,Defending Against Collaborative Attacks By Malicious Nodes In MANETs:A cooperative Bait Detection Approach,2014. page number:1-11.

[2] A.Baadache and A.Belmehdi,"Avoiding blackhole and cooperative blackhole attacks in wireless adhoc networks,"Intl.J.Comput.Sci. Inf.Security, vol. 7, 1, 2010.Page number : 35-43 .

[3] K.Vishnu and A.J Paul, "Detection and removal of cooperative black/gray hole attack in Mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, 2010.page number: 28–32.

[4] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen,"CBDS:A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl.Conf.WirelessCommun.,VITAE,Chenai, India,Feb.28–Mar.,03,2011,page number: 1–5.

[5] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,Jan. 1999. (Last retrieved March 18, 2013).page number:1-6.

[6] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc.WiSec, 2009,page number:103–110.