Front. Cur. Trends. Engg. Tech. Vol. 1(1), *pp.* 28-36 (2016)
OPEN ACCESS ISSN: 2456-1185
Published by ACET. Available online: www.fctet.in

Detecting and preventing malicious nodes using cooperative bait detection scheme

M.Nandhini[1], J. Sathya[1], T.Sundaridevi[1], G. Sivaprakash[1], J. Jaya[1*] and P. Premalatha[1]

Abstract- Mobile Ad hoc networks (MANETs), is a primary requirement for the establishment of communication among nodes is that nodes should assist with each other. In the presence of malicious nodes, this requirement may lead to serious security problem; for instance, such nodes may disrupt the routing process. MANETs have been widely used for various applications such as military operation and emergency operation. The infrastructure-less nature and the dynamic topology features of MANET makes this network highly vulnerable of routing protocols and injecting harmful packets in the network. The challenge is how to prevent this security threats in MANETs. In this paper, based on DSR protocol, a detection scheme known as Cooperative Bait Detection Scheme (CBDS), which aims at detecting and preventing malicious nodes launching gray hole/black hole attacks in MANETs. In this scheme, it integrates the proactive and reactive defence architecture and randomly cooperates with the adjacent node as a bait destination end to bait malicious nodes to send a reply message (RREP) and strange nodes are detected using reverse tracing method thereby prevents and ensures security.

Index Terms -- Mobile Ad hoc Network (MANET), Cooperative Bait Detection Scheme (CBDS), Collaborative blackhole attacks, Dynamic Source Routing (DSR), Grayhole attacks, Route Request (RREQ), Route Reply (RREP), Ad hoc On Demand Vector routing(AODV), Malicious node.

1. INTRODUCTION

Mobile represents 'moving' and ad hoc represents 'temporary without any infrastructure'. Therefore, a mobile ad hoc network is made up of a group of mobile nodes, which cooperates to communicate with each other without any fixed central base station.

Received: 12 December 2015; Revised: 12 March 2016; Accepted: 28 March 2016; Published online: 06 April 2016

*Correspondence to: principal@acetcbe.edu.in

[1]Akshaya college of Engineering and Technology, Kinathukadavu, Coimbatore, Tamil Nadu, India

A mobile ad hoc network (MANET), sometimes called a mesh mobile network, is a network associated by wireless links. MANET is a kind of single path transmission type and is a set of mobile nodes communicate with each other by wireless network. Due to infrastructure-less nature of the network, steering management is done by the support of nodes, that is the nodes themselves maintains the functioning of the network. The topology vary speedy and unpredictable over time because of the mobility of the nodes. Besides, the security of MANET has many defects. These intimidations make the security of MANET lesser than a cable network and create many security issues.

Because the communication of MANET uses the open medium, attacker can easily listen in message that are transmitted. The design of previous routing protocol trusts entirely that all nodes would transmit route request or data packets correctly, dynamic topology, without any essential communications, and lack of certification authorities make MANET vulnerable to diverse types of attacks.

One of the common attacks is Black hole attack that is a malicious node can attract all packets by using fake RREP to falsely claiming a fresh and shortest route to the destination and then discard them without forwarding them to the destination. Black hole attack is a kind of Denial-of-Service attacks and derive Gray hole attack, a alternative of black hole selectively discards and forwards data packets when packets go through it. Cooperative black hole attacks denote numerous malicious nodes cooperate with each other and work just like a group. This kind of attack outcome in many detecting methods not succeeds and causes more vast hurt to all networks.

Ad hoc Networks are defined as the group of wireless networks that develop multi-hop radio relaying and are capable of in service without central coordinator which makes routing a demanding job. It is adaptive in temperament and is self organizing. A shaped network can be distorted and again

shaped on the section and this is concluded without the help of system administration. Each node may be proficient of acting as a router.

Since a destination node might be beyond range of a source node sending packets; a routing process is needed to find a path to forward the packets suitably among the source node and the destination node. Inside a cell, a receiver can reach all mobile nodes without routing by means of broadcast in common wireless networks.

1.1. Black Hole Attack

Black hole attack is known as Packet Drop Attack since it drops lots of packets. Black hole attack is an vigorous attack. Most common attack here is stop forwarding the data packets. If there is a malicious node, it keeps waiting for its neighbour node to initiate RREQ packet.

As a node receives the RREQ packet, it will send a false RREP packet immediately with a adapted high sequence number. So that the source node will assume that there is a route is available towards the destination. The source node ignores the RREP packet from the other nodes including the precise nodes where it repeatedly denies the other nodes and it will start sending the packets on the way to the malicious nodes.

1.2 Gray Hole Attack

A variation of black hole attack is the gray hole attack, in which nodes can fall the packets selectively. Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is really an attacker and it will act as a usual node. So the attacker can't be easily identified since it behaves as a normal node.

The address of the adjacent node is used as the bait destination address, bait malicious nodes to send RREP reply messages and identify the malicious nodes by using the reverse tracing program.

2. RELATED WORK

In a MANET, each node not only works as a host but can also act as a router. While receiving packets, nodes also need to cooperate with themselves to forward packets, thereby forming a wireless local area network.

Indeed, the afore mentioned applications impose some severe constraints on the security of the network topology, routing and data traffic. For instance, the presence and collaboration of malicious nodes in the network may interrupt the routing process.

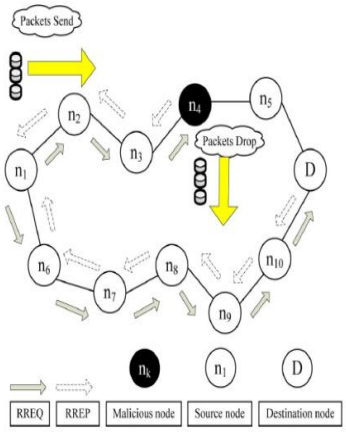

Figure 1. Black hole attack–node n4 drops all the data packets.

Many research works have determined on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual disobedient nodes. In this regard, the efficiency of these method becomes weak when multiple malicious nodes collide jointly to initiate a collaborative attack, which may result to more devastating damages to the network.

The require of any communications added with the active topology feature of MANETs make these networks highly defenceless to routing attacks such as black hole and gray hole. In black hole attacks (see Figure.1), a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the aim of intercepting communication.

In this case, a malicious node (so-called black hole node) can pull towards all packets by using counterfeit Route Reply (RREP) packet to falsely claim that "fake" shortest route to the destination and then discard these packets devoid of forwarding them to the destination. It then selectively discards/forwards the data packets when packets go through it.

This focuses on detecting gray hole/collaborative black hole attacks using a DSR based routing technique.

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

If an intermediate node has routing information to the destination in its route store, it will reply with a RREP to the source packet.

When the RREQ is forwarded to a node, the node add a address information to the route in the RREQ packet.

When destination receives the RREQ, it can know every mediator node's address between the route. The destination node rely on the collected routing in order to send reply RREP message to the source node along with the whole routing information of the recognized route.

3. PROPOSED SYSTEM

In this malicious node detection scheme, named as CBDS, which is able to detect and prevent malicious nodes produce black or gray hole attacks and cooperative attacks. Using the address of the adjacent node as the target bait address, it bait malicious nodes to send a RREP reply and detects the malicious nodes by the proposed reverse tracing program and subsequently prevents their attacks.

Accordingly, this application merges the advantage of proactive finding in the early stage and the authority of reactive response that reduce the waste of resource. Consequently, in this mechanism doesn't like the technique that just use automatic architecture would suffer black hole attack in initial stage.

The source node cannot recognize closely which in-between node has routing information to destination node and respond RREP and sends packets to the shortest path that the malicious node declare and the network go through black hole attack that produce packet loss. Conversely, the network that uses DSR can't know which malicious node cause the loss. This function assists in sending the bait address to attract the malicious nodes and use the reverse tracing technique of CBDS to sense the correct addresses of malicious nodes

3.1 System Architecture

To determine collaborative black-hole attacks problem by designing a AODV routing as DSR-based routing mechanism, which is called CBDS that integrates the reward of both proactive and reactive defence architectures. In this approach, the source node stochastically selects an nearby node with which to found cooperation, the address of this node is used as bait destination address to deceive malicious nodes to send a RREP reply message.

3.2 Network Design

In this design, we are mainly dealing with security side, to check the protocol strength, attacker and defender nodes is designed. The attacker node able to check the route request and can give the fake reply to the source and mugger can recognize the data packet and it will drop. Legitimated nodes can make the cooperation with neighbour and can make the communication, and forwards the data from one to other nodes, and can try to defend from attacker.

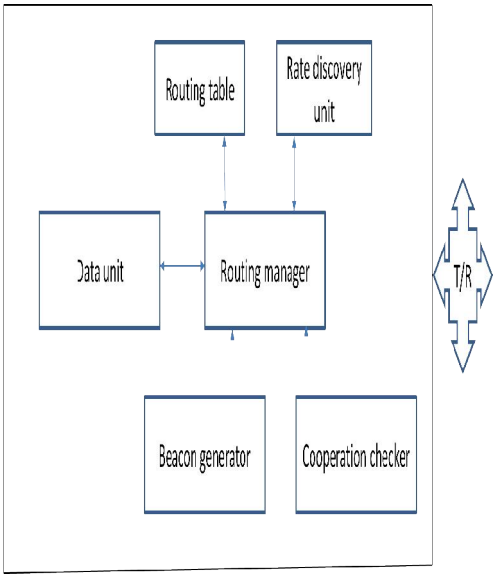

Figure 2.System architecture

Cooperation Checker

In this module, the timer is used to keep the time expire and intimates to generate the irregular packet. The beacon generator can produce the packet and that packet can be read by any neighbour node, the beacon life is only for one hop. The work of neighbour management unit is to store the neighbour information into table when it receives the beacon packet from the neighbour.

Route Discovery

Normally the source can find the route when the data is coming up in buffer with no route by using the route request and route reply. The source will generate fake request with destination address as cooperating neighbour.

Source already knows the information, for RREQ no reply. But in case if there is reply from any node, then that node will be identified as malicious by using the source routing mechanism.

Route Maintenance

In this element, if route is failed the intermediate node will share the error message. Based on the fault message the source node will find another route to destination. With secure route discovery model.

3.3 Secured Routing Protocol

In this, participate significant role in mobile ad hoc network. Secured routing protocol protected the attack such as caterpillar whole attack, black hole attack and previous interior and exterior attack. In alteration of on-demand routing protocol for anticipation of attack, various authors projected a scheme such as EAODV (Enhanced on demand distance vector routing protocol) and SBRP (secured backup routing protocol).

SBRP is very proficient protocol for secured communication in ad hoc network.

The process of Secured backup routing protocol produces in three phase.

(1) Secured route discovery crosswise the node
(2) Backup node setup
(3) Route maintenance diagonally the node.

The secured process consumes time for carrying out of process of SBRP protocol.

The process of SBRP protocol are not power efficient, but it is secured protocol adjacent to exterior and interior attack of ad hoc network.

The process of foundation of SBRP protocol separated into three groups for power saving mode such one is snooze mode, transit mode and energetic mode of exploit of node. The choice of suitable node in minimum period and other node in sleep mode the spending of power is decreases. Each node locally assigned priority value of node. P=Σ, + 1 is the power of certain node. The number of nodes in a group is known as establish group of node and denoted by GA. Having the alike group at the entire nodes ensures that identical regular threshold rate. The node neighbours a and b are uninformed that they are exacting by thresholds charge. Having practical a collision in its narrow time t, node w transmits at time t+GA,

Protocol Steps For Modified Control Message Protocol

- Initialized node state
  • Initial selection value is set 0
  • Calculate the power of energy of particular node for request as P=Σ , + 1 here the group of node is M-1 and node choice is 0 to M. If Power of node is minimum Pi then certain group of inauguration
  • Create group creation phase GAi[t]←0,t=0.....GA-1 ti←0 solo node in system

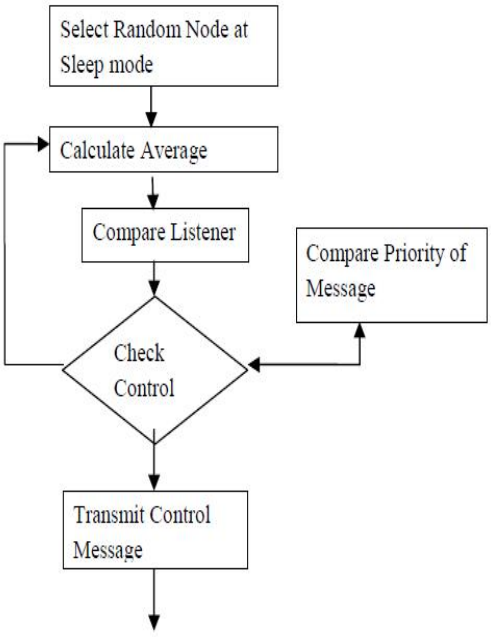

Figure 3. Protocol for efficient routing

• Now collection of only node in group node compute whole power of Transceiving power as = Σ (, + 1 +) for selection of active node for conniving a national threshold as Tval= −1
• If rate of Tval is less than certain node power rate then certain lower power node as master
• If node=0 then
• Select ←Random(0....gGA-1)
• Send direct message
• If not priority group then
• If send several group of precedence at transmitter then
• node←0
• else if node ++≥1/precedence node then
• node ←active mode

3.4 Ad Hoc On Demand Distance Vector Routing Protocol (Aodv)

If the stage of an imperative task in video-conferencing, reserve education, supportive work, and video on demand, imitation database updating and querying, etc. Numerous multicast routing protocols have been planned for ad hoc networks, that are classify as whichever mesh based or tree based.

In a tree based multicast protocol, there is only a lone path among a couple of source and recipient, thus primary to higher multicast competence.

The creation of a multicast tree can be completed whichever from the source (source-initiated) or from a recipient (receiver-initiated).

The ad hoc background affects from regular trail breaks due to mobility of nodes; hence proficient multicast group protection is essential.

A few examples of tree based multicast protocols are ad hoc Multicast Routing (AMRoute) ad hoc Multicast Routing protocol utilizing Increasing id-numbers (AMRIS) , Bandwidth Efficient Multicast Protocol, Multicast operation of the Ad hoc On demand Distance Vector (MAODV) routing protocol , and Multicast Core- Extraction Distributed Ad hoc Routing (MCEDAR) protocol.

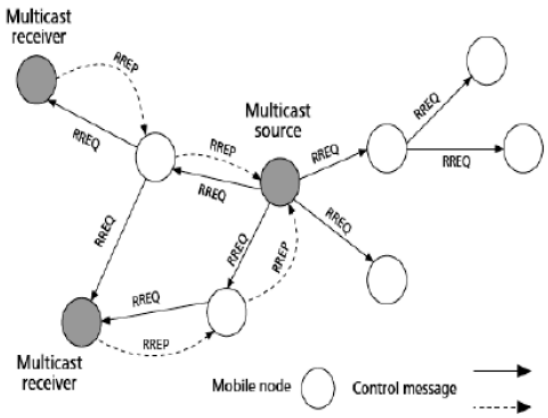

Figure 4 Path Discovery in the AODV Protocol.

In difference to the tree based model, mesh based multicast protocols may have several paths linking any source and receiver pairs, thus on condition that more affluent connectivity amid the multicast members. The ODMRP protocol is a mesh based protocol that uses a transmitting group conception for multicast packet deliverance. Only the participants of forwarding group presumptuous data packets.

For maintaining the multicast mesh it uses soft state method. But the main divergence between them is that the previous one is a source-initiated multicast protocol, while the last one is receiver-initiated multicast protocol. Both FGMP and ODMRP protocols apply control packets flooding to form the multicast mesh, thus ensuing in sizeable control slide.

AODV based on collective trees on-demand to bond multicast set of members. AODV has ability of unicast, broadcast, and multicast.

AODV protocol can be course information gained while probing for multicast. When a node desires to fix a multicast group or it has information to send to the group but does not has a route to that group, actually it is a route request (RREQ) message.

Simply the members of the multicast group reply to the bond RREQ. If an in-between node receives a stick together RREQ for a multicast group of that it is not a member or it gets a route RREQ and it does not have a route to that group, it rebroadcast the RREQ to its near by nodes. But if the RREQ is not a bond request whichever node of the multicast group may replied.

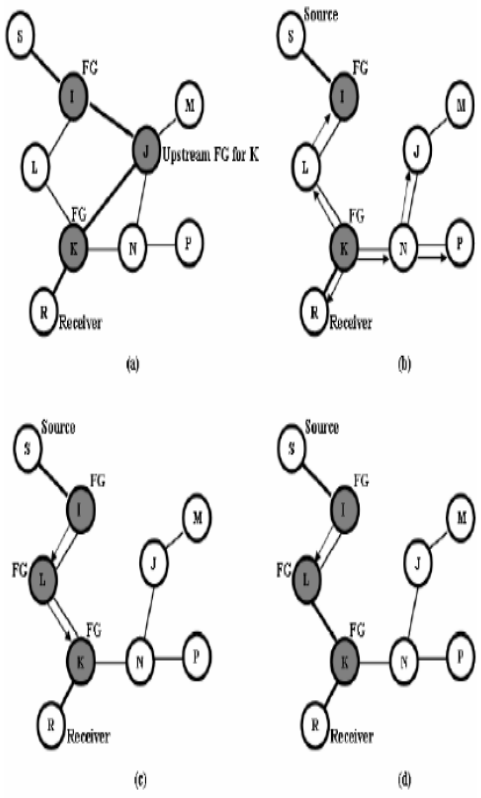

Figure 5 Patch AODV Process

3.5. Algorithm For Detecting Gray/Black Hole

Action by Source Node S

Step 1: Seperates the data packets to be sent in **k** same parts.
DATA [1,….,K]; Initialize **i = 1;**
Step 2: Transmit **prelude(S,D,ni)** message to the destination node **D.** Where **ni** is the no of data packets to be sent in recent block.
Step 3: Broadcast **monitor (S, D, NNR)** message to all its near by nodes. Instructing neighbours to supervise next node in the route (**NNR**).
Step 4: Begins transmitting data packets from the obstruct **Data[i]** to **D.**
Step 5: Assigns timeout **TS** for the acceptance of the **postlude (D, S, d_count)** message having **d_count**, no of data packets received by D.
Step 6: If **TS** not expired and **postlude** message received,
if (ni (1−μ)≤ d _ count)
Augmentation **i** by **1** and move to **Step 8**.
else Begin Gray/Black hole elimination process.
Step 7: If **TS** expired and **postlude** message not received after that begin Gray/Black hole eliminate process.
Step 8: Continues from **Step 2** while **i** less than alike to **k.**
Step 9: Terminates **S**'s stroke. Stroke by Destination Node D

Step 1 On receiving **prelude(S,D,ni)** message from **S** extracts **ni** Initialize **d_count = 0.**
Step 2: Assigns timeout **TD** for the acceptance of the recent data model and waits for the data packets.
Step 3: While **TD** not expired and a data packet received renew **d_count += 1**
Step 4: while **TD** expired transmit **postlude(D, S, d_count)** message to **S.**

Step 1 On receiving **monitor (S, D, NNR)** message nodes expands the id of the next node in the route **NNR**, source node id **S** and destination node id **D**.
Step 2: If the getting node is neighbour of **NNR** then,
Step 2.1: Turn on Promiscus mode**.**
Step 2.2: Initialize **dataCountNNR = 0**.
Step 2.3: Determine next node id **Nnext** to which **NNR** is transmitting the data packets.
Step 2.4: start including data packets by increasing **dataCountNNR += 1.**
Step 2.5.: If **Nnext** is not destination node **D** after that
Step 2.5.1: Broadcast **monitor (S, D, NNR)** message to each and every one of its nearest swapping **NNR** by **Nnext**.
Step 3: Else Rebroadcast **monitor (S, D, NNR)** message to each of its neighbours.
Step 4: Terminates its stroke.

3.6 Gray/Black Hole Removal Process

Accomplishment by Source Node S

Step 1: Broadcast **query(S, D, NRREP, ni)** message to each of its nearest. Where **NRREP** is the id of the node transmitting route reply message to **S**.
Step 2: Assigns timeout **TRES** for the confession of the **result (MN, S, NRREP)** message from the monitoring node **MN.**
Step 3: While **TRES** not expired and **result** message received or **"NRREP Malicious"** received after that extracts **NRREP**.
Step 3.1 If **NRREP** previously produces in **FindMalicious** chart
Step 3.1.1: Then addition of **voteCount** for **NRREP** by 1.
Step 3.1.2: If **votecount >= thresholdCount**
Step 3.1.2.1: Eliminate **NRREP** from **FindMalicious** chart and affix **NRREP** in **Gray/BlackHole** chart.
Step 3.1.2.2: Broadcast **"NRREP Malicious"** to the system.
Step 3.2: Else
Step3.2.1: Affix **NRREP** in **FindMalicious.**
Step 3.2.2: Initialize **voteCount** = 1.
Step 4: Initialize **j = 1**.
Step 5: While **j <=** length of **FindMalicious** chart
Step 5.1: Broadcast **VREQ(S, Nj)** to the system requesting erstwhile nodes in the system to vote for **Nj** if it is malicious.
Step 5.2: Assigns timeout **TVREP** for reply from the system **VREP(RN, S, Nj)** where **RN** is id of whichever ordinary node in the system.
Step 5.3: While **TVREP** not expired and **VREP** message received after that.
Step 5.3.1: Augmentation **voteCount** for **Nj** by **1.**
Step 5.4: If **voteCount >= thresholdCount.**
Step 5.4.1: Eliminate **NRREP** from **Find Malicious** chart and affix **NRREP** in **Gray/BlackHole** chart.
Step 5.4.2: Broadcast **"*NRREP Malicious*"** to the system.
Step 5.4.3: Assign **findHoleStatus = true** in the routing chart of S for the route to **D.**
Step 5.5: Augment of **j** by **1.**
Step 6: If **findHoleStatus** is **True**
Step 6.1: Terminate sending data. Determine new route to **D**.
Step 7: Restart its normal stroke. Action by Neighbours on receiving on receiving *query(S, D, NRREP, ni)*message

Step 1: On receiving ***query(S, D, NRREP, ni)*** message nodes extracts **NRREP** (id of the node transmitting route reply message to **D**), **S**, **D** and **ni**(no of data packets sent to D).
Step 2: If the receiving node is neighbour of **NRREP** then,
Step 2.1: If *ni* (1−μ) ≤ *dataCount*
Step 2.1.1: while **Nnext** is not **D**
Step 2.2: Else
Step 2.2.1: If **Nnext** common to **NULL** then **Nnext** itself falling each and every packects
Step 2.2.1.1: Reply **"*NRREP Malicious*"** to S.
Step 2.2.2: Else

Step 2.2.2.1: Reply ***result (MN, S, NRREP)*** to **S,** that defines **NRREP** may be malicious.
Step 2.2.2.2: Broadcast ***query(S, D, NRREP, ni)*** message to each of its neighbours swapping **NRREP** by **Nnext** and **ni** by **dataCount** for **NRREP.**
Step 3: If the getting node is not the nearest of **NRREP** after that broadcast ***query(S, D, NRREP, ni)*** message to each its neighbours.
Step 4: Terminates its stroke. Stroke by whichever normal nodes (RN) on getting on receiving *VREQ(S, Nj)*message.

Step 1 On getting ***VREQ(S, Nj)*** message nodes extracts **Nj**
Step 2: If **Nj** produces in **Gray/BlackHole** chart.
Step2.1: Reply ***VREP(RN, S, Nj)*** to **S**.
Step 3: Terminates its process. Process by whichever ordinary nodes (RN) on getting on receiving "NRREP Malicious"

Step 1 On receiving **"NRREP Malicious"** each ordinary nodes in the system verify **Gray/BlackHole** chart**.**
Step 2: If **NRREP** not produces in **Gray/BlackHole** chart, after that.
Step 2.1: If **NRREP** not produces in **FindMalicious** chart.
Step 2.1.1: Affix **NRREP** in **FindMalicious** chart.
Step 2.2.2: Initialize **voteCount = 1**.
Step 3: Terminates its stroke.

3.7 Numerical Results

Take a arbitrary scheme with one source Po, one destination Pd, NP = 8 prime nodes, an alike transmitting power for major and minor users, i.e. EP = ES, which yields _P = _S = _, anywhere set _ = −5 dB. instruct nodes are equally located at casual in a four-sided figure area with normalized side equivalent to single, where source Po and destination Pd are sited in the central of two differing parts. Best possible policies are gained setting = 0.99, that is sufficient for stationary networks.

The division of power owed to major transmissions is calculated by getting the largest which convince Pout,SS(dS) = _S for _S = 0.1 and a distance dS = 0.1. plot the presentation of well thought-out routing schemes in terms of major lengthwise throughput (4) *vs* crucial energy expenditure (articulated in dB, i.e., 10 log10 E(k,RP,Q).

4. PERFORMANCE EVALUATION

Scurry the draft by typing at the incurable as Ns filename.tcl.

On conclusion of the scurry, copy production of the file "filename-out.tr" and name production file "filename-out.nam" are produced by the casual development technique.

The terminate process is specified as

```
proc finish{}
 {
$ns flush-trace
close $r
close $nf
exec nam –r filename. nam &
exit 0
}
```

4.1 Simulation And Results

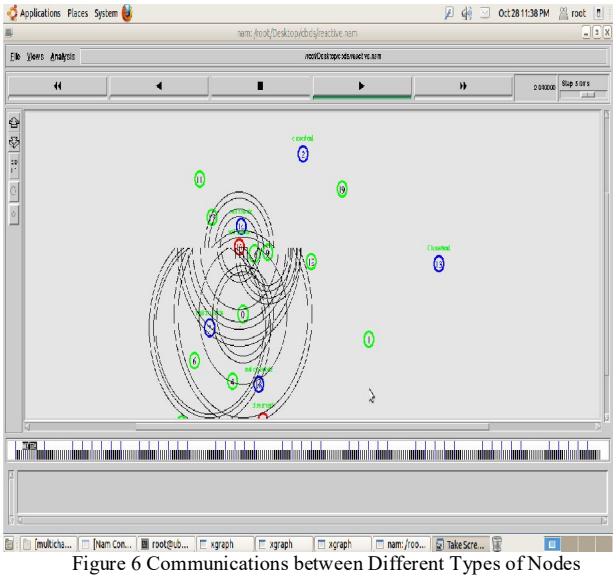

Figure 6 Communications between Different Types of Nodes

Figure 6 gives it can be pragmatic that while the count of malicious nodes increases, DSR creates the lowest routing overhead compared with the CBDS.

4.2. Virtual Multicast Tree Formed By AODV route

In Figure 7 gives core gets a JOIN_REQ packet from other core in the equal multicast group.

It replies with a JOIN_ACK. A fresh bidirectional subway is created stuck between the two cores, and one of them is certain as a core behind the mesh combination. While the mesh has been taking place, the core begins the tree construction process.

4.3 Effect Of Malicious Node On PDR

In Figure 8 it preserve also be experiential so as to DSR heavily affects from increasing black hole attacks since it does

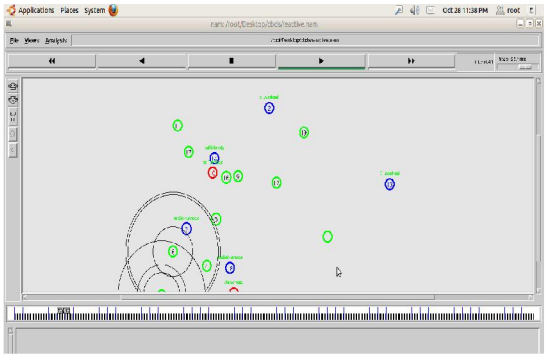

Figure 7 Virtual multicast tree formed by AODV Route

not have any exposure and defence method to check blackhole attacks. While the percentage of malicious nodes vary in the system from 0% to 40%, BFTR does not sense malicious nodes openly.

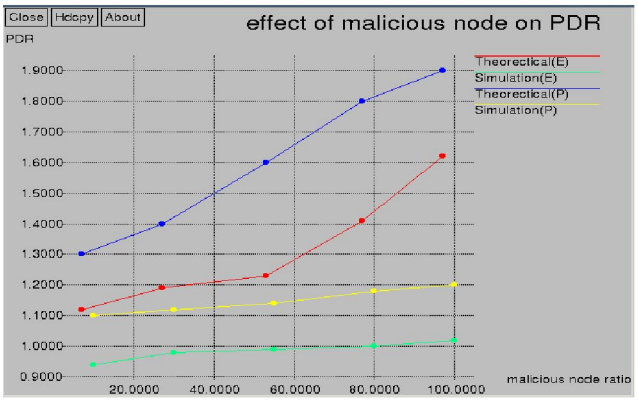

Figure 8 Effect of malicious node on PDR

It chooses a fresh route that may still contain malicious cause of malicious nodes on the packet delivery ratio. Nodes when the lengthwise presentation of a route varies from the predefined activities of first-class route.

$$\boldsymbol{PDR} = \frac{1}{n}\sum_{i=1}^{n}\frac{\boldsymbol{pktd_i}}{\boldsymbol{pkts_i}}$$

Where ,

$pktd_i$ is the count of packets received by the destination.

$pkts_i$ is the count of packets sent by the source.

4.4. Effect Of Malicious Node In Routing Over Head

Figure 9 it represents that while the percentage of malicious nodes increases, DSR causes the lowest routing overhead compared with each schemes together with the CBDS.

Furthermore, the CBDS is able to attain proactive detection in the preliminary stage and then modify into reactive response in the afterwards stage. Routing overhead shows the ratio of the amount of routing linked control packet transmissions to the amount of data transmissions.During this aspect, the benefit of proactive detection and the authority of reactive response can be combined to decrease the desecrate of resource.

$$\boldsymbol{RO} = \frac{1}{n}\sum_{i=1}^{n}\frac{\boldsymbol{cpk_i}}{\boldsymbol{pkt_i}}$$

Where,

cpk_i is the count of control packet transmitted.

pkt_i is the count of data packet transmitted.

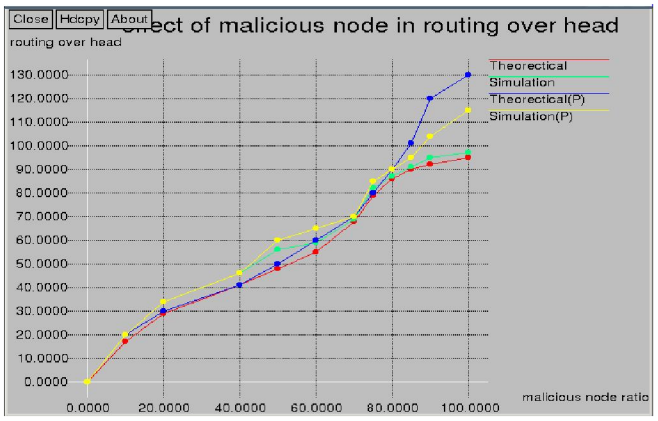

Figure 9 Effect of malicious node in routing over head

4.5 Routing Over Head DSR & CBDS

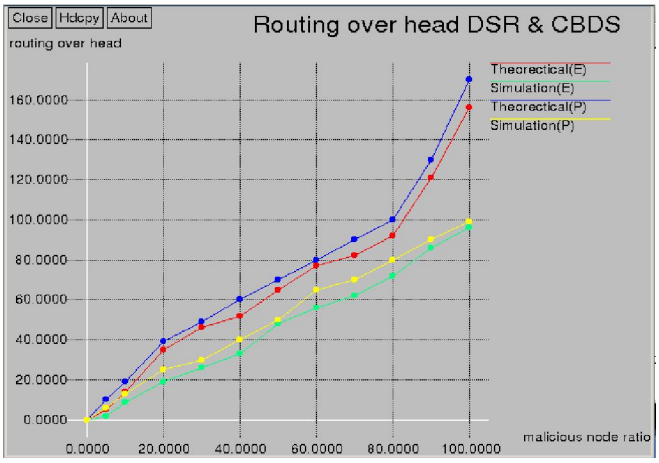

Figure 10 Routing over head DSR & CBDS

Figure 10 gives that when the count of malicious nodes increases, DSR causes the lowest routing transparency compared with the CBDS. In fact, the routing transparency produced by the CBDS for altered thresholds is a little bit privileged than that caused by DSR.

5. CONCLUSION AND FUTURE WORK

Each and every protocols have their own merits and demerits. One constructs multicast trees to decrease lengthwise latency. Multicast tree-based routing protocols are proficient and convince scalability matter, they have numerous disadvantages in ad hoc wireless networks due to mobile personality of nodes that contribute during multicast assembly.

In this paper, the energy utilization is little bit elevated. As a future work, this can be minimised by dropping the amount of nodes traversal from the source to destination.

This assures good quality of links and reduces the chance of link failures and the overhead required to built the ways. In the mesh-based protocols gives more robustness in opposition to mobility and keep the large size of control transparency used in tree continuance. It is actually tricky to invent a multicast routing protocol allowing for all the above mentioned causes. At rest it is an open difficulty for researchers to enlarge a lone protocol that can convince as many ambition is to be possible in the future.

REFERENCES

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

[2] 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)*

[3] C. Chang, Y.Wang, and H. Chao, "An efficientMesh-based core multicast routing protocol onMANETs," *J. Internet Technol., vol. 8, no. 2, pp. 229–239, Apr. 2007.*

[4] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput., pp. 153–181, 1996.*

[5] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," *in Proc. IEEE Aerosp. Conf., 2002, vol. 6, pp. 2727–2740.*

[6] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.*

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," *in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.*

[8] 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, pp. 28–32, 2010.*

[9] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.*

[10] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," *IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.*

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," *in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.*

[12] H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," *in Proc. IEEE ICC, 2007, pp. 362–367.*

[13] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Pers.Commun., vol. 29, pp. 367– 388, 2004.*