International Journal of Current Engineering and Technology

ISSN 2277 – 4106
©2013 INPRESSCO. All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Secured routing protocol for avoiding BlackHole in MANETS

Neeta D Bangalur[a*] and Rajashree V Biradar[a]

[a]Ballari Institute of Technology& Management, Bellary

Abstract

An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. This lack of centralised infrastructure in ad hoc network makes it vulnerable to various attacks. The routing process is disrupted if malicious nodes start performing malicious activity instead of the intended function. One among several severe attacks is a BlackHole attack where a malicious node tries to capture the path towards itself by falsely claiming larger sequence number and smaller hop count to the destination and then absorb all data packet without forwarding them to destination node. In this paper, we propose a protocol for avoiding BlackHole attack without the special hardware constraints and dependency on physical medium of wireless network. BRRP modifies AOMDV & uses its link disjoint multi-path during path discovery to provide greater path selection in order to avoid multiple malicious nodes in the path using Reliability table maintained by each node in the network. Thus with the help of Reliability ratio stored in the Reliability table, Non-malicious nodes gradually avoid the BlackHole nodes while making path between source and destination. The proposed protocol will be implemented using NS-2 simulator.

Keywords: *BRRP, AOMDV, BlackHole, MANET, routing protocol, route_switch packet, Reliability points.*

1. Introduction

In situations where creating the infrastructure is impossible or prohibitively expensive is exactly where MANET comes into picture. MANET is a self-organised network system without any centralised infrastructure. Typically, the nodes act both as host as well as routers at the same time. Unlike a network with fixed infrastructure, mobile nodes in ad hoc networks do not communicate through the fixed structures.

Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network. They can form random topologies depending on their connectivity with each other in the network. These nodes have the ability to arrange themselves and because of their self-configuration ability, they can be deployed immediately without the need of any infrastructure.Many MANET routing protocols exploit multiple paths to route the packets (Z. Zaide et. Al, 2003) (Vaidya B et. Al,2007) (Ye Z. et. Al, 2003) (Charles E Perkins et al, 2002). These nodes have the ability to organize themselves and because of their self-configuration ability, they can be deployed urgently without the need of any infrastructure. Many MANET routing protocols exploit multiple paths to route packets. The probability of successful packet transmission on a path is dependent on the reliability of the wireless channel on each hop of routing. It is this demeanour that has made MANET the most vulnerable network to security threats.

Security Issues in Mobile Ad Hoc Network is the most important concern for the basic functionality. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met by implementing certain measures. MANETs are often suffering from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, supportive algorithms and no clear security mechanism. These factors have changed the battle field situation for the MANET against the security intimidation. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer (B.Awerbuch et al, 2004) (F.Akyildiz et al, 2002) (x. Lin et al, 2002). MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, vigorously changing topological arrangements and limited resources.

A particular severe attack among several routing attacks is called *BlackHole attack* (Y.C Hu et al, 2004), (L.Tamilselven et al, 2008). In this attack, a malicious node tries to capture the path toward itself by falsely claiming larger sequence number and smaller hop count to the destination and then absorb all data packet without

*Corresponding author: **Neeta D Bangalur** forwarding them to destination node. In Fig. 1 (a) we illustrate the progress of a BlackHole attack, wherein the source node A is intended to establish a route to destination node I, by broadcasting route request (RREQ) packet. However, when BlackHole node BH receives an RREQ, it immediately sends an RREP which is having larger sequence number and smaller hop count. On Receipt of an RREP from BH, the source starts transmitting the data packets, which BH simply drops instead of forwarding to the destination.

A BlackHole can be formed either by a single node or by several nodes in collusion (L.Tamilselven et al,2008)as shown in Fig. 1 (b). In case of a single node attack, the node drops all the packets instead of forwarding to destination whereas in case of multi-node collusion attack, BH1 forwards all the data to BH2 and BH2 drops them instead of forwarding to the destination. BlackHole attacks have serious impact on routing algorithms which uses sequence numbers to determine fresh messages and select the shortest route based on the hop count such as Dynamic Source Routing (DSR) or Adhoc On-Demand Multipath Distance Vector Routing (AOMDV).

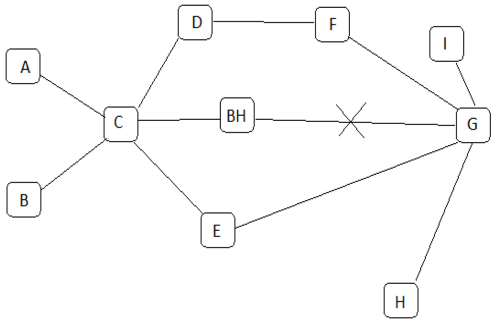

Fig 1 (a): single BlackHole node

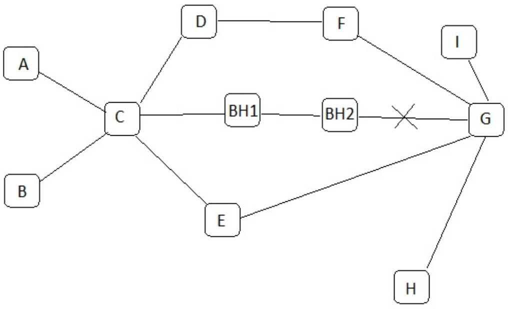

Fig1 (b): multiple BlackHole nodes

The routing protocols for adhoc networks are Proactive routing protocol and Reactive routing protocol. The proactive routing protocols are Table driven. A routing table is maintained by each node in the network. The table contains the routing entries for all the possible nodes in the MANET. The reactive routing protocols are on demand routing protocols. The routes are propagated only on demand. The most commonly used reacting routing protocol for ad hoc networks are DSR, AODV & in some special cases as considered in this paper AOMDV. In this paper we are using AOMDV with some important modifications to counter the BlackHole attack.

2. Related work

Most of the previous research has focused on problems of routing for communication assuming a trusted environment. However, many applications run in untrusted environments and require secure routing for communication such as military or police networks, emergency rescue operations etc.

The methods proposed earlier fall broadly into two categories. The first category is of those which modify specific well known routing protocols such as AODV, DSR and OLSR to avoid/detect BlackHole attack during route reply (Shurman et al, 2004), (S.Lee et al, 2002). The second category is of those which adopt an extra monitoring system such as a watchdog, confidant protocol or intrusion detection system (S.marti et al, 2000), (S.Buchegger, et al, 2003), (M-Y . Su et al, 2010).

Saurabh Gupta et.al, 2011 proposed a BRRP routing protocol in which they have used a modified version of AODV protocol to avoid the BlackHole attack. However, this approach worked well in case of single BlackHole node. But in case of multiple BlackHoles, since AODV was used it imposed much overhead & incurred much time in calculating path to the destination.

Tamilselvan et. Al, 2008 introduced fidelity table as an enhancement to the existing AODV protocol. The fidelity level of each arriving RREP is checked and the one with the highest level is selected and processed. These RREPs are stored in the response table for further use. After acknowledgement is received, the fidelity level of the node is updated proving it safe and reliable. However, updating the fidelity table of each node by broadcasting it to other nodes results in congestion and also the selection of wrong RREP from the response table cause another route request flooding.

Burchegger et al introduced the confidant protocol in which each node monitored its next hop's behavior and this information is used to make decisions based on ratings about providing or accepting route from it. However, the use of this system makes this confidant protocol impractical to include in the network.

Marti et.al used additional tools such as watchdog & pathrater to identify the BlackHole nodes. The watchdog identifies BH nodes by promiscuously to the next node's transmission & the pathrater uses the information obtained by the watchdog to choose the right path. However, this procedure is inaccurate due to partial dropping, collision & transmission power.

3. Overview of AOMDV protocol

The main feature of AOMDV is that it provides multiple paths to destination. The paths are loop free and mutually disjoint. AOMDV uses the value of advertised hop-count to maintain multiple paths to destination with the same destination sequence number. The RREQ message initiates a routing table entry. The AOMDV protocol has the following additional fields along with the usual default fields that we have in the AODV in the routing table of a node:

Table I: routing table entries of a node using AOMDV protocol.

……
-destination IP addr,
-sequence number,
-advertised hop count,
-routes:{(next hopIP1, HC 1),…},
……

Thus, route discovery in AOMDV results in selection of multiple loop-free, link-disjoint paths between source and destination.

4. BlackHole attack in manets

Routing protocols in MANETs are exposed to a wide range of attacks including SinkHole, WormHole, Sybil attack or even the most dreaded BlackHole attack. BlackHole attack is an attack which might either provide a room for an intruder (man-in-middle) or play the denial-of-service(DOS) in which the misbehaving node makes use of the loopholes of the route discovery packets of the protocol to advertise itself as having the best path to the node whose packets it want to intercept. In this attack the malicious node convinces the source node claiming it has the best possible route to the destination so that the source starts sending the traffic through the specific node in control of the attacker.

During the *Route Discovery process*, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires.

A BlackHole can be formed by either by a single node or by several nodes in collaboration. In case of a single node attack, the node drops the entire traffic that it is receiving instead of forwarding to the destination. In case of multiple BlackHole nodes, BlackHole node will forward the packet to another BlackHole node.

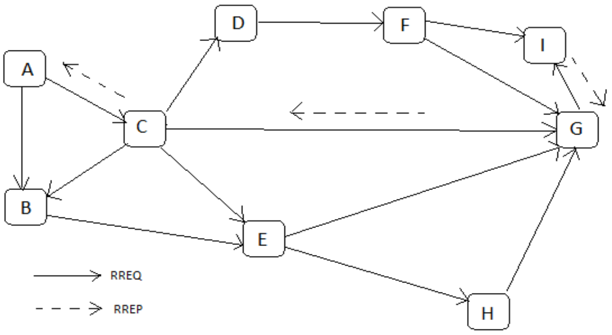

Fig 2 (a): BlackHole attack with a single BH node.

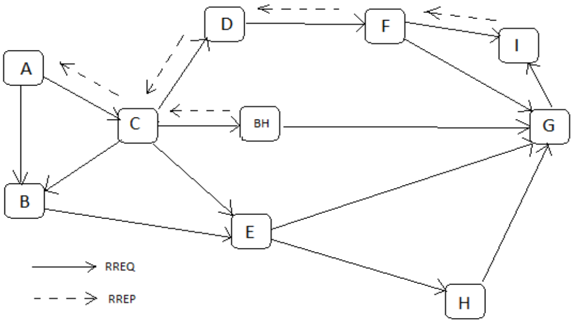

Fig 3: BlackHole attack with multiple BH nodes.

In the above figure 2, imagine a malicious node ‘BH’. When node ‘A’ broadcasts a RREQ packet, nodes ‘B’ & ‘C’ &receive it. From node ‘C’ it is received by ‘BH’ and ‘BH’ being a malicious node, does not check up with its routing table for the requested route to node ‘I’. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node ‘C’ receives the RREP from ‘BH’ ahead of the RREP from other connected nodes and relays the same to node ‘A’. Node ‘A’ assumes that the route through ‘BH’ is the shortest route and sends any packet to the destination through it. When the node ‘A’ sends data to ‘BH’, it absorbs all the data and thus behaves like a ‘Black hole’.

In AOMDV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP message, a destination node compares its current sequence number, and the sequence number in the RREQ packet plus one, and then selects the larger one as RREPs sequence number. Upon receiving a number of RREP, the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from the other nodes. The source then starts to send out its packets to the black hole trusting that these packets will reach the destination. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination.

5. Proposed solution

The routing protocol we propose here BRRP (BlackHole’s Reliability Ratio Protocol) is based on the existing AOMDV protocol with some necessary modifications to the actual protocol so that it can be efficiently used to avoid multiple BH attacks during path setup between source and destination. BRRP (BlackHole’s Reliability Ratio Protocol) is designed by drawing the basics of AOMDV protocol so that it can efficiently avoid the presence of multiple BlackHole nodes during the path setup process.

When a source node wishes to establish a path to the destination a few of the intermediate nodes may have multiple paths to the destination. So, the source now needs to select only one path to the destination. With the help of AOMDV's link disjoint multi-path during the route discovery process.

In BRRP, every node maintains reliability points of their one-hop neighbors to form the correct path to the destination. Thus, in the route discovery process of BRRP, an intermediate node will choose a route that excludes the nodes whose reliability points are below the lower threshold. Continuing this way, gradually the malicious nodes will be avoided by the non-malicious nodes.

A. RREQ and RREP packets

The original RREQ and RREP packet formats are taken from the AOMDV protocol with slight modifications. Additional fields are incorporated to realise the concept of reliability points. BRRP adds an additional *hop1* field to the RREQ packet as shown in the fig 3(a) below. This field stores the IP address of the first hop after it left the originating node. Intermediate nodes would not process the RREQs that have the same *hop1* field value. Using the *hop1* field, the BRRP forms link disjoint multiple paths in the path discovery phase but during the path setup process, it chooses only single link with the highest reliability points among the available ones as discussed above.

hop1	hop count	G	U
Originator IP addr			
Originator seq numb			
Destination IP addr			
Destination seq numb			

Fig 3(a): RREQ packet of BRRP

In the RREP packet, BRRP adds an additional field called initiator as shown in the fig 3(b) below. This field stores the identity of the node who claims a path to the destination. This node can either be an intermediate node or the destination. This fields value is stored in the *hop1* field of the routing table when a node receives RREP.

types	size	hop count	*initiator*
Source IP addr			
Destination IP addr			
Destination seq numb			

Fig 3(b): RREP packet of BRRP

B. Reliability table

Every node in BRRP maintains a reliability table shown in the table II below.

Table II: Reliability table

Node ID	A	B
-	-	-
C	1	2
D	2	3
E	4	5
-	-	-

This table is used to choose the most reliable node (among the multiple backward disjoint link to source node and next hop to destination) while sending RREP back to the source node

Reliability table contains the following fields:

- *Node ID*: stores the IP address of the node whose reliability is being studied.
- *α count*: specifies the number of times the node has been chosen in the route formation.
- *β count*: gives the number of times connection to the destination has been successful through the *node ID*.

The above two count fields are used to obtain the reliability ratio of a *Node ID* being studied by using the following formula:

Reliability ratio: $\beta/(\alpha+1)$

A higher ratio of a node means the higher possibility of the node being non-malicious.

C. *Route_switch* packet

An additional packet is being used by the BRRP as shown in the fig below

switch bit
Source addr
Destination addr

Fig 4: Route_switch packet of BRRP

These fields are used by the nodes to

a. To inform the first node in the backward path (having multiple entries for destination) to change the route to another path which has next highest reliability ratio

b. To flush the counter of the counter of all nodes in the backward path. Switch bit in the packet has special purpose which has multiple entries to the destination node, so that other nodes in the backward path would not switch the route to another path.

D. Routing table

Routing table in BRRP has the following additional fields:

- hop1: used to store the value of hop1 field of RREQ. However, a node receives an RREP. This field is used to store the value of the initiator field of RREP.
- value bit{0,1,-1}: a 0 in this field indicates a path to the destination through the next hop may not be correct. A

1 specifies path is free from malicious node and a -1 indicates entry has not been chosen for data transfer.

- Count: denotes the number of RREPs received with the same sequence.

Table III: Routing Table

hop1
Validbit
Count
Hop count
Next hop
Destination seq number
Destination IP address

After the entries are stored in the routing table, HELLO packets are used to broadcast the *Node ID* whose reliability ratio crosses the lower threshold level among its one-hop neighbour nodes.

6. Receiving RREQ in BRRP.

The three fields namely source IP, sequence number & the *hop1* participate in determining whether an RREP is duplicate or not. For an intermediate node, if the hop count in the RREQ is larger than the hop count of the entry in the routing table which has the same sequence number and source IP, then RREQ is directly dropped. A node would create multiple entries (multiple link disjoint path) when the sequence number is same; hop count is smaller and the *hop1* field value is different from the existing reverse entries. However, the destination node replies to each RREQ in spite of the values in hop count and *hop1* field of RREQ when the sequence number is equal or larger than the existing entry (M-Y su et al,2010).

Fig 5 below illustrates a situation, in which A and I represent the source and destination respectively. The arrow represents the RREQ broadcasting traces; the top section represents the *hop1* of the RREQ; first box in the bottom section represents the hop count and the second box in the bottom section represents the sequence of the RREQ arrivals at the node.

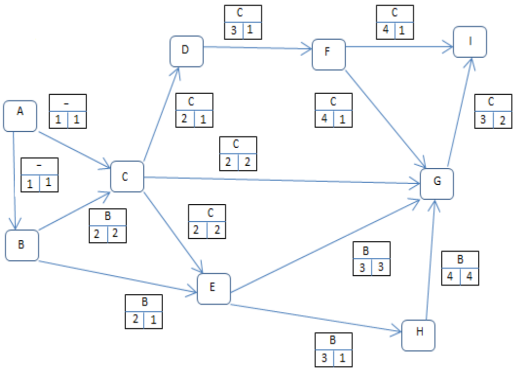

Fig 5: RREQ processing in BRRP

As the nodes B, C received the RREQs they find the hop count is 1. They now place their own IP address into the *hop1* field and add a 1 to the count field and broadcast the packet.

Further, D and E receive the RREQ from C and B respectively. E receives the RREQ from both C and B. It saves the one which has arrived earlier and the second copy of RREQ also has the same hop count but from a different originator hence, it creates one more entry from C and discards the RREQ.

Later, the node G receives RREQ form various nodes (F,D,C,E,H). It chooses the one with the smaller hop count and discards the remaining. Now the node I receives the RREQ from F as well as G. the RREQ from F is dropped since it has a higher hop count and the reverse entries are created at each nodes as and when the RREQs are received.

7. Receiving RREP in BRRP.

Regardless of the number of RREQs received, the destination node will reply to each RREQ unless the sequence number of RREQ is not smaller than the existing sequence number in the routing entry. Intermediate nodes will reply to RREQ only when they have an entry to the destination node with $validBit$=1 in the routing table. Node receiving an RREP from any of its neighbor will first check the Reliability ratio of the neighbor. If the Reliability ratio crosses the lower threshold level than the node will drop the RREP, otherwise will forward it to the neighbor which has the highest Reliability ratio among multiple backward entries and delete the other backward entries. Whenever a node creates an entry in the routing table after receiving RREP, it sets the $validBit$ as 0 and $count$ field as 1. A node who is generating RREP must store its identity into the *initiator* field of the RREP packet. The intermediate node will create single forward entry in the routing table regardless of the RREPs received (having same sequence number) with next hop set to the neighbor which has the least hop count to the destination and set the $count$ field of the entry to the number of RREP received. Malicious node may send the RREP with its own identity or with the identity of the destination node (spoofing) in the *initiator* field of the RREP. Malicious node replies with higher sequence number because they do not know the exact sequence number of the destination node. Intermediate nodes forward only the first RREP arrival and drop the others. Intermediate node store the identity of the replying node in the *hop1* field of the routing entry.

Fig. 7 illustrate another example, in which S and D represents the source and the destination respectively. The arrow represents the neighbour chosen among multiple backward entries because of its high Reliability ratio; the first box represents the *initiator* of the RREP; second box represents the hop count and the third box represents the sequence of the RREP arrivals at the node. B1 and B2 are two blackhole nodes where B1 replies with its own identity and B2 with the destination node identity (spoofing). We have assumed that the node K knows a path to the destination node via node M.

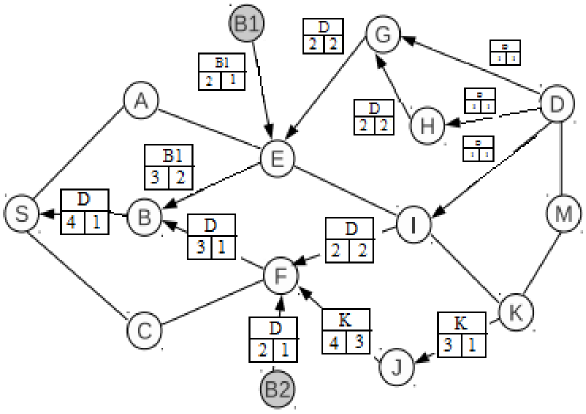

Fig 6:RREP processing in BRRP

Node G receives two RREP from the destination and H respectively. On receipt of first RREP, G will create forward entry towards destination and forwards the packet to the only backward entry node E. After second RREP arrival, node G finds an entry to the destination having same sequence number. Therefore, it retains a single entry towards destination which has least hop count i.e first entry and sets the $count$ field in the routing entry to 2. When node I receives the reply, it would check its reliability table to find which backward entries (E or F) has higher reliability ratio and eventually chooses node F. In sequence, node F receive three replies, i.e from B2, I and J. Node B2 replies with higher sequence number and spoofs the destination node identity in the *initiator* field, whereas, node K replies with its own identity. Next hop would have been chosen on the following criteria:

- If reply from I and J are having same sequence number, then node F would create two forward entries; first towards either I or J based on their Reliability ratio if they have same hop count to destination, otherwise to the node which has lower hop count to destination with $count$ field set to 2; and the second entry towards B2. Node F will choose first entry for forwarding data packets by setting its $validBit$=0 and others $validBit$=-1 because first entry $count$ field is higher than second entry which means the higher possibility of correct path through first entry.
- If reply of node K has an older sequence number of node D, then each reply has different sequence number. Node F would create three entries for each reply comes from B2, I and J respectively. The RREPs having destination address in the *initiator* field had a higher probability of correct path to destination than other RREPs because RREP originated by other nodes (than destination node) may claim an older path to destination. Since two replies had different sequence number with the *initiator* field containing destination address (it means any of them comes from malicious node), node F would choose forward entry whose next hop has higher Reliability ratio in spite of their hop count by setting its $validBit$=0 and others with -1. If both entries have similar Reliability ratio then node F randomly choose any of them.

Accordingly, node E receives the first reply from B1 and it copies the reply content into the routing entry and forward the reply to the backward entry having higher Reliability ratio i.e B. When node E received another reply from node G which had *initiator* field filled with the destination address and different sequence number with an existing entry, then node E sets the second entry for data transfer regardless of the Reliability ratio of next hop by setting its $validBit$=0 and others $validBit$=-1. But, it will not delete previous entry because the second RREP could have been generated by malicious node by spoofing destination address (not in this case). Node B will perform in a similar way to node E.

After the source node receives the reply, it starts sending data packet to the destination node. While forwarding data packet, each node in the path will set the counter to an interval so that it would get data packet reply or *route_switch* packet within the interval time. Otherwise, as the node counter interval period expires, it would increment the α field of the next hop in the Reliability table and send the *route_switch* packet to the backward entry node. Counter interval is t = (15− $HopC$)(2{d/v}+δ) where v is the velocity of the light, d is the maximum transmission range, δ is the processing time of the node, $HopC$ is the hopcount between the source node and the intermediate node which set the counter and 15 is assumed as maximum hop count in the ad hoc network. We have assumed that S, B, F and B2 is the path formed for the RREQ sent by the source node. Nodes in the path i.e S, B and F will set the counter as they forward the data packet. Since B2 is the BlackHole node, it will drop the packet. When the counter interval of node F expires, it would increment the $Pathcount$ field of node B2 in its Reliability table and delete the corresponding entry in the routing table and send the *route_switch* packet to node B with switchBit set to 1 (because node F has change the path to node I). Node B flushes the counter and does not make a decision to switch to next path because the node ahead in the route already had changed the path by setting *switchBit*=1, then each node send the *route_switch* packet along reverse route unless source node reached. Assume remaining entries in the routing table of node F towards destination node results in to dropping, then Node F on last entry would send *route_switch* packet to node B with switchBit=0. After the complete data has been transferred, destination node will send final data acknowledgement (REP_ACK) packet back to source node. Each node in the path will change the sequence number of the forwarding entry as listed in the REP_ACK packet and set the $validBit$=1 in the routing entry; delete other entries in the table towards destination; and increment the α and β field of the previous hop and next hop of REP_ACK in the Reliability table.

8. Simulation results

NS 2.34 is used for the simulation of BRRP protocol. The parameters chosen are as follows:

- number of nodes :45

- Mobility area used:2000*2000m^2
- Radio range:300m

Source, destination & BlackHole nodes are chosen randomly in the network area. Source sends around 10kb data which is UDP CBR/sec with a packet size of 512 bytes. Fig 7 shows comparison between the actual AOMDV and the edited AOMDV(BRRP) to check the time required to establish the route to the destination.

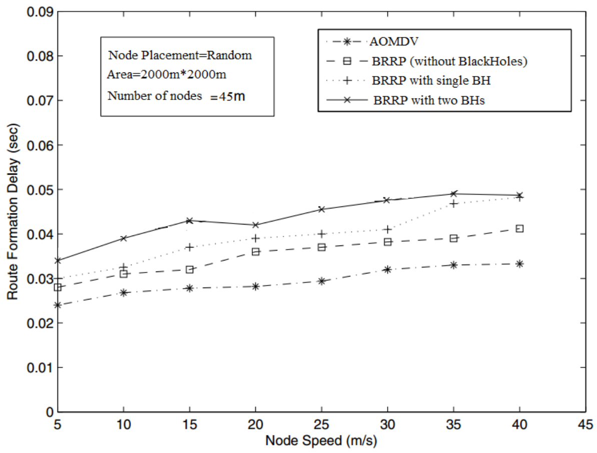

Fig 7:Route formation delay vs Node speed in BRRP

Fig 8 shows the effect of node speed on packet loss. As the nodes starts moving with high speed, the BlackHoles as well as the other nodes tend to move from neighborhood of the nodes very randomly which affects the data collected in the reliability table. Thus, packet loss increases significantly.

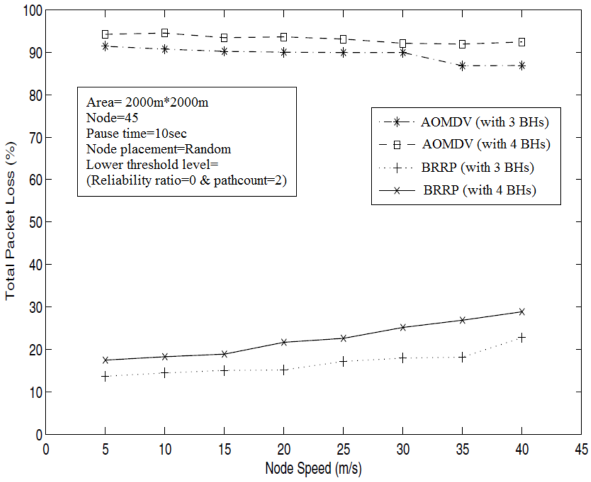

Fig 8: Node speed varied to check packet loss

Conclusion

The new protocol proposed in this paper (BRRP) is designed to detect the presence of multiple BlackHole nodes in the route formation process itself which is achieved only by making slight modifications in the working of the actual AOMDV protocol. The protocol is not bound by any hardware as well as software constraints. However, to achieve this it only requires an additional route_switch packet as well as a reliability table.

Simulation results depict only 5% to 10% loss of packet in the presence of 3 to 4 BH nodes as compared to 97% packet loss encountered by the actual AOMDV protocol.

References

Z. Zaidi and B. Mark (Mar 2003), A Mobility Tracking Model for Wireless Ad Hoc Networks, Proc. Wireless Comm. and Networking Conf.(WCNC), pp. 1790-1795,

Vaidya B, Pyun Y. J., Park J A., and Han S.J. (2007), Secure multipath routing scheme for mobile ad hoc network. In Proceedings of IEEE International Symposium on Dependable, *Autonomic and Secure Computing*, pages 163–171.

Ye Z., Krishnamurthy V., and Tripathi S.K. (Mar 2003), A framework for reliable routing in mobile ad hoc networks. *In Proceedings of the IEEE INFOCOM Conference*, volume 1, pages 270–280.

Charles E. Perkins, and Elizabeth M. Royer (2002), Ad-hoc On-Demand Distance Vector (AODV) routing, Internet Draft.

B. Awerbuch, D. Holer, and H. Rubens (Mar 2004), High Throughput Route Selection in Multi-Rate Ad Hoc Wireless Networks, Proc. Conf. Wireless On-Demand Network Systems (WONS), pp. 251-269.

F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci (Aug 2002), A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114.

X. Lin, Y.K. Kwok, and V.K.N. Lau (July 2002), RICA: A Receiver-Initiated Approach for Channel-Adaptive On-demand Routing in Ad Hoc Mobile Computing Networks, Proc. Int’l Conf. *Distributed Computing Systems* (ICDCS), pp. 84-91,

Y.C Hu, and A. Perrig,A survey of secure wireless adhoc routing, *IEEE Security and Privacy*, 2004, pp. 211-226.

L. Tamilselvan, and V. Sankaranarayanan (2008), Prevention of cooperative black hole attack in manet, Journal of Networks, Vol. 3 (5)pp.13-20

M.A. Shurman, S.M. Yoo, and S. Park (2004), Black hole attack in mobile adhoc networks, 42nd ACM Southeast Regional Conf., pp. 11-14.

S. Lee, B.Han, and M. Shin (2002), Robust routing in wireless adhoc networks, Intl. Conf. on Parallel Processing, 2002, pp. 73- 78

Saurab. Gupta, S. Kar, and S. Dharmaraja (2011), WHOP: Wormhole Attack Detection Protocol using Hound Packet, 7th *IEEE Intl. Conf. on Innovation in IT* (Innovation’11), pp. 226-231