Prevention of Co-operative Black Hole Attack in MANET

Latha Tamilselvan
BSA Crescent Engineering College,
Vandalur, Chennai, Tamilnadu, India,
Ph.: 91 44 2275 1375, Fax: 91 44 4211 4282,
Email: latatamil@hotmail.com

Dr. V Sankaranarayanan
BSA Crescent Engineering College,
Vandalur, Chennai, Tamilnadu, India,
Ph.: 91 44 2275 1375,
Email: sankarammu@yahoo.com

***Abstract* – A mobile ad hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc On demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack [1]. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. Our approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated. Computer simulation using GLOMOSIM shows that our protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.**

***Index Terms* - Ad hoc Networks, Routing Protocols, AODV, Black Hole Attack, fidelity level.**

I. INTRODUCTION

Wireless networks can be basically either infrastructure based networks or infrastructure less networks. The infrastructure based networks uses fixed base stations, which are responsible for coordinating communication between the mobile hosts (nodes). The ad hoc networks falls under the class of infrastructure less networks, where the mobile nodes communicate with each other without any fixed infrastructure between them.

An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes [1][17].

Most important networking operations include routing and network management [2]. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type include Destination Sequence Distance Vector (DSDV). Reactive or source-initiated on-demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP). Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature of dependence on other nodes for transmission. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. [1][4][16].

A. AODV Routing Protocols

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions [3][6][7]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A

RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. This is illustrated in figure 1.

Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node *M* can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of 'Black Hole' attacks.

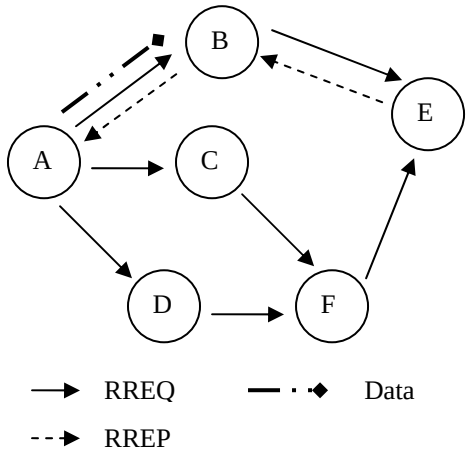


Figure 1. Propagation of RREQ & RREP from A to E

II. BLACK HOLE ATTACK

A Black Hole attack [1][5][20] is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. Co operative Black hole means the malicious nodes act in a group [18][19]. As an example, consider the following scenario in figure 2. Here node S is the source node and D is the destination node. Nodes 1 to 5 act as the intermediate nodes. Nodes 4 (B1) and 5 (B2) act as the cooperative Black holes. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole B1 reaches the source node, well ahead of the other RREPs, as it can be seen from the figure 2. Now on receiving the RREP from B1, the source starts transmitting the data packets. On the receipt of data packets, B1 simply drops them, instead of forwarding to the destination or B1 forwards all the data to B2. B2 simply drops it instead of forwarding to the destination. Thus the data packets get lost and hence never reach the intended destination.

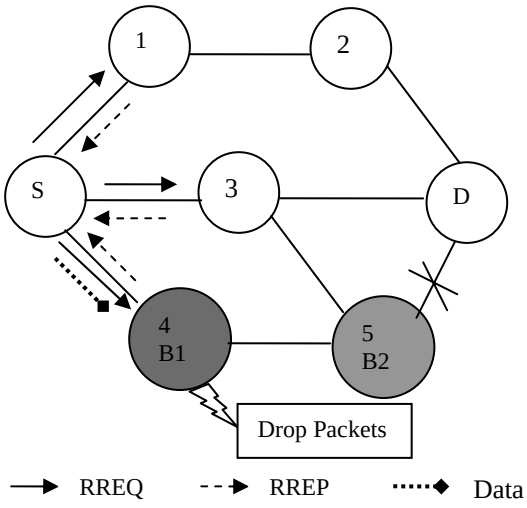


Figure 2. Black Hole Attack

III. RELATED WORK

Recently, a lot of research has focused on the cooperation issue in MANET. Several related issues are briefly presented here.

Researchers have proposed solutions to identify and eliminate a single black hole node [1]. However, the case of multiple black hole nodes acting in coordination has not been addressed. For example, when multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its teammates B2 as the next hop, as depicted in Fig 2. According to [1], the source node S sends a "Further Request (FRq)" to B2 through a different route (S-3-B2) other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D.

Because B2 is cooperating with B1, its "Further Reply (FRp)" will be "yes" to both the questions. Now, as per the solution proposed in [1], node S starts passing the data packets assuming that the route S-B1-B2 is secure. However, in reality, the packets are consumed by node B1 and the security of the network is compromised.

Misbehavior detection and reaction are described in [8], by Marti, Giuli, Lai and Baker. The paper presents two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission. This technique is imperfect due to collisions, limited transmit power and partial dropping. However, according to simulations [9], it is highly effective in source routing protocols, such as DSR. The path rater uses the knowledge from the watchdog to choose a path that is most likely to deliver packets. The path rating is calculated by averaging the rating of the nodes in the path, where each node maintains a rating for all the nodes it knows in the network. Watchdog is used intensively in many solutions for the cooperation problem. The main drawback of this idea is that it enables selfishness and misbehaving nodes to transmit packets without punishing them, and thus encourages misbehavior.

Buchegger and Le Boudec [10] present the CONFIDANT protocol .Each node Monitor the behavior of its next hop neighbors in a similar manner to watchdog. The information is given to the reputation system that updates the rate of the nodes. Based on the rating, the trust manager makes decisions about providing or accepting route information, accepting a node as part of a route and so on. When a neighbor is suspicious in misbehaving, a node informs its friends by sending them an ALARM message. If a node's rating turns out to be intolerable, the information is relayed to the path manager, which proceeds to delete all routes containing the intolerable node from the path cache. This does not address partial packet dropping.

Michiardi and Molva propose the CORE scheme and various related issues in [11][12] . In this scheme, every node computes a reputation value for every neighbor, based on observations that are collected in the same way as watchdog. The reputation mechanism differs between subjective reputation, indirect reputation, and functional reputation. Subjective reputation is calculated directly from neighbors past and present observations, giving more relevance to past observations in order to minimize false detection influence. Indirect reputation is the information collected through interaction and information exchange with other nodes using positive values only. Functional reputation is the global reputation value associated with every node. By avoiding the spread of negative rating, the mechanism resists attacks, such as denial of service. When a neighbor reputation falls below a predefined value, the service provided to the misbehaving node is suspended. The working of the model and its performance were not reported**.**

Banal and Baker propose OCEAN [13], a scheme for robust packet-forwarding. OCEAN, similarly to previous schemes, is based on nodes' observations. In contrast to previous mechanisms, no rating is exchanged and every node relies on its own information, so the trust management is avoided. The rating is based on a counter that counts the positive and the negative steps a node performs and based on a faulty threshold, the node is added to a faulty list. In the method for route selection, a DSR node appends an avoid list to every generated RREQ and a RREP based on this list. A second-chance mechanism is provided to give nodes that were previously considered misbehaving another opportunity to operate. OCEAN simulations concludes that a scheme which relays only on first-hand observation performs almost as well and sometimes even better than a scheme that also relies on second-hand information. OCEAN also fails to deal with the misbehaving nodes properly.

Bracha Hod,in his thesis[19] highlights various aspects of cooperation enforcement and reliability, when AODV is the underlying protocol. Furthermore, it presents a scalable protocol that combines a reputation system with AODV that addresses reputation fading, second-chance, robustness against liars and load balancing. .

The proposed solution constructs different reputation properties and misbehaving reaction better suiting to AODV. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack [1]. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. The proposed approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated. Computer simulation using GLOMOSIM shows that our protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

IV. PREVENTION OF CO-OPERATIVE BLACK HOLE ATTACK-PCBHA

We propose a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid multiple black holes acting in the group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. Our solution assumes that nodes are already authenticated and hence participate in communication. Assuming this condition, the black hole attack is discussed Our approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and it is eliminated.

The source node transmits the RREQ to all its neighbors. Then the source waits for 'TIMER' seconds to collect the replies, RREP. A reply is chosen based on the following criteria,

In each of the received RREP, the fidelity level of the responding node, and each of its next hop's level are

checked. If two or more routes seem to have the same fidelity level, then select the one with the least hop count; else, select the one with the highest level.

The fidelity levels of the participating nodes are updated based on their faithful participation in the network. On receiving the data packets, the destination node will send an acknowledgement to the source, whereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented.

A. Working principle of PCBHA

A.1. Collecting response

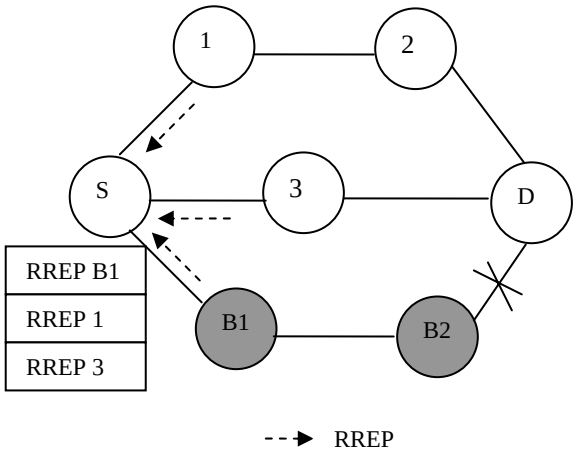


Figure 3. Collecting responses

The incoming responses are collected in a table, namely, the Response table. The entries will have fields like, source address, destination address, hop count, next hop, lifetime, destination sequence number, source and destination's header address. The responses will be collected till a timer expiry event. This is illustrated in figure 3.

A.2. Choosing a response

A valid route is selected from among the received responses based on the following methodology. A fidelity table' is maintained that will hold the fidelity levels of the participating nodes. The basic idea is to select the node with a high fidelity level. Initially the fidelity levels of the responded node and its next hop are looked for.

If the average of their levels is found to be above the specified threshold, then the node is considered to be reliable. On the receipt of multiple responses, the one with the highest fidelity level is chosen. In case, two or more nodes seemed to have the same fidelity levels, then the one with the minimum hop count is chosen.

As shown in Figure 4, the source S chooses the response RREP-3, as highlighted, after checking the fidelity levels. It then transmits the data packets.

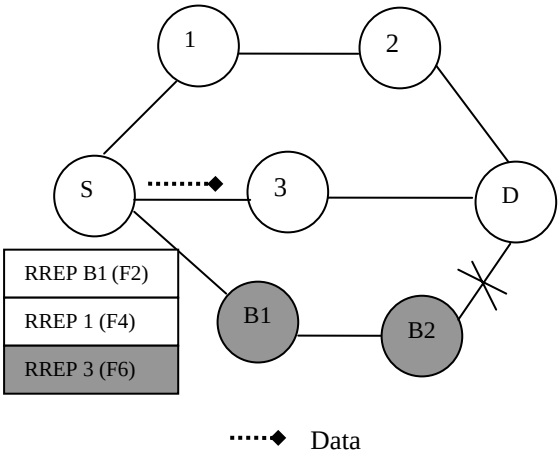


Figure 4. Choosing a response to forward data

A.3. Updating the fidelity level

Every destination node sends back an acknowledgement to the source node, upon the reception of the data packets. The receipt of the acknowledgement enables the source node to increment the fidelity level of the intermediate node, for it has proved reliable and safe. In case, the source node doesn't receive the acknowledgement within a timer event, the source node will decrement the fidelity level of the intermediate node which replied and also the level of the node which was given as the next hop of the intermediate node to identify the co-operative attack. This eliminates possible positive next hop information by a cooperative black hole. Periodically the fidelity tables are exchanged among the participating nodes.

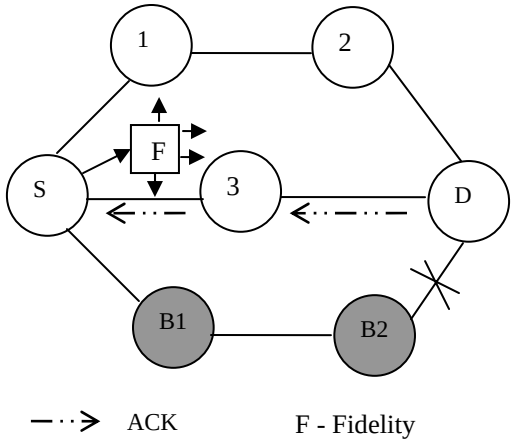
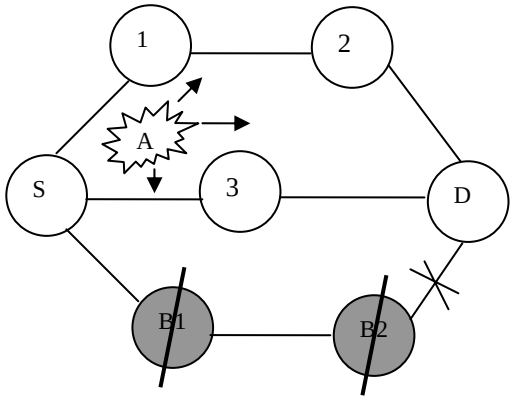


Figure 5. Receiving acknowledgement and broadcasting fidelity packets

On receiving the acknowledgement, as seen in Figure 5, the fidelity levels of the respective nodes are incremented, and the fidelity packets are exchanged.

A.4. Eliminating the Black holes

When the fidelity level of a node drops to 0, it implies it has not forwarded the data packets faithfully and hence a Black hole. The detection of a Black hole has to be intimated to the other participating nodes in the network. This is accomplished by sending alarm packets.



A – Alarm Packet

Figure 6. Black hole nodes elimination

When a node receives an alarm packet, it will identify the Black hole and so can eliminate the use of that node from then on. The final scenario where the Black holes have been detected and hence eliminated is shown in Figure 6. The algorithm for the proposed solution is as follows:

Notations:

RREQ : Route Request
RREP_COLLECT_TIME: Time for which responses(route replies) are collected
RSPT : Response Collection Table
IN : Intermediate Node
ACK_TIMEOUT: Time for which a node waits for ACK

```
source broadcasts RREQ
while(simclock=current_time+RREP_COLLECT_TIME)
{
        store in RSPT
}
if(size of RSPT = 0)
{
        retransmit RREQ
}
else
{
find AVG_FIDELITY_LEVEL =FIDELITY_IN + FIDELITY_next hop
        select route with highest AVG_FIDELITY_LEVEL
if FIDELITY_IN > THRESHOLD and FIDELITY_next hop > THRESHOLD
        {
                send data
        }
        else
        {
                repeat until a maximum TTL value.
        if not {
                declare no valid route is found
              }
        }
}
while (simclock = current_time + ACK_TIMEOUT)
{
        if RACK is received
        {
                increment the fidelity level of the IN
                broadcast the fidelity packets
        }
}
if (no RACK is received)
{
decrement the fidelity level of the IN and next hop
        broadcast the fidelity packets
}
if (FIDELITY of a node = 0)

{
remove the node from neighbour table and fidelity table
broadcast alarm packets
}
```

Figure 7. PCBHA Algorithm

Minimum threshold value used for the simulation is taken as 2 units as a test case. To find a valid route the proposed solution tries up to a maximum of RREQ_RETRIES TIMES at the maximum TTL value. Otherwise declare no valid route is found.

V. SIMULATION RESULTS

A. Metrics

The simulation is done using GloMoSim (Global Mobile Simulator) [14] [15], to analyze the performance of the network by varying the nodes mobility. The metrics used to evaluate the performance are given below.

Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

Average End-to-End Delay: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc.

Routing Overhead: This is the ratio of number of control packet generated to the data packets transmitted.

B. Simulation profile

The simulation profile is illustrated in the Table 1.

TABLE 1
SIMULATION PROFILE

Property	Value
Nodes	25
Simulation Time	300 S
Mobility	Random way point model (a node randomly selects the destination and moves in the direction of destination) – pause time 30 m/s – Node mobility varied between 10 S to 90 S
Load	100 items, Data pay loads 512 Bytes. Interdeparture time of 1S.
Coverage Area	800 m by 800 m
Number of Transactions	5 – 8

B.1. Packet Delivery Ratio

To evaluate the packet delivery ratio, simulation is done with 25 nodes with the source node transmitting 100 packets to the destination node. Each packet is of 512 bytes and is transmitted with an interval of 1 second. As it can be seen from the figure 8, with PCBHA the packet delivery ratio is more compared to AODV. The number of transaction indicates number of flows initiated during a particular duration of time from same or different sources to same or different destinations.

The packet delivery ratio increases by using PCBHA compared to AODV till four transactions when the number of transaction is increased above four the packet delivery ratio is slightly decreased. This is due to the congestion of networks.

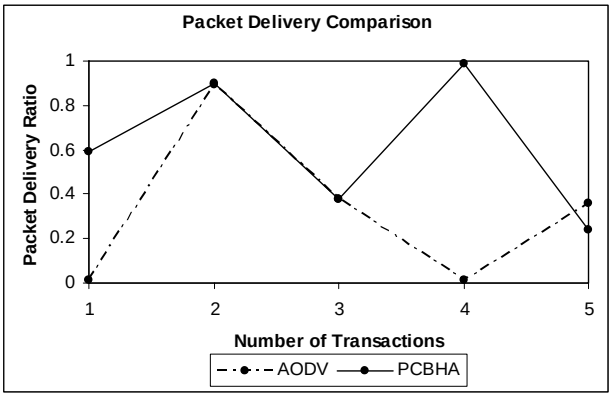


Figure 8. Packet Delivery Ratio

Figure-8 shows the packet delivery ratio in the presence of malicious node. In a 25 node topology, consider Source 5 sends packet to Destination 10. Here assume 4 and 6 are the malicious nodes. In AODV the packet delivery ratio is reduced to 1%. But in PCBHA the packet delivery ratio is around 60 %. From this figure 8 it is clear that the packet delivery ratio is increased around 90% in PCBHA. But in AODV it is around 30% only, when we used different source-destinations pair like 1-5, 3-7, 14-17, and 8-10.

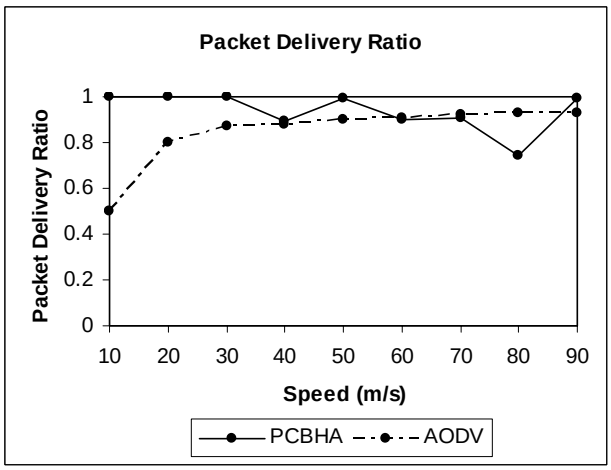


Figure 9. Packet Delivery Ratio

From the figures 8 & 9 it is clear that even when there is a Co-operation between the malicious nodes PCBHA gives a good result compared to AODV, in terms of packet delivery.

B.2. Average End-to-End Delay

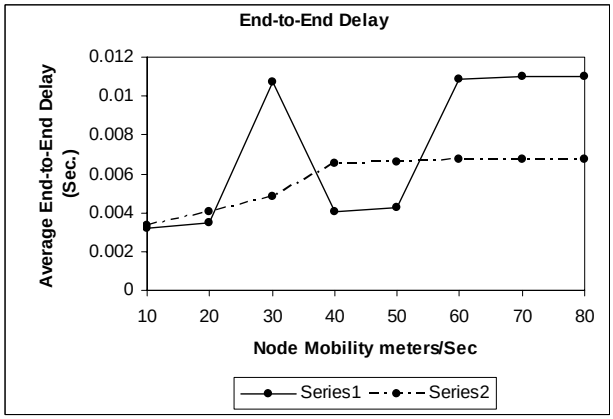


Figure 10. End to End delay

From the figure-10 it can be observed that, when PCBHA protocol is used, there is an increase in the average end-to-end delay, compared to AODV. This is due to the additional waiting time in each node before sending the reply. Again this is due to the immediate reply from the malicious node. i.e. the nature of malicious node here is it won't check its routing table for the route availability.

B.3. Routing Overhead

Figure-11 shows the routing overhead. To evaluate the routing overhead, simulation is done with 25 nodes and 5 CBR applications.

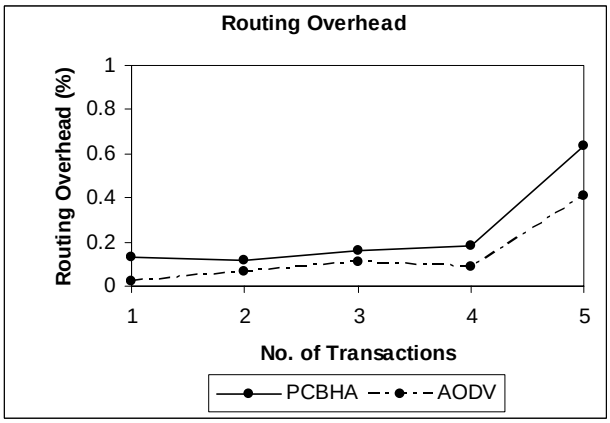


Figure 11. Routing overhead

As it can be seen from the figure11, with PCBHA the routing overhead is slightly more compared to AODV. This is due to the additional process involved to avoid the selection of malicious node.

Figure 12 shows the control overhead vs. speed. To evaluate the control overhead consider the source 2 transmits 100 data packets to Destination 10. For PCBHA the number of control packets generated is slightly more compared to AODV.This is due to the exchange of fidelity packet in PCBHA to achieve security.

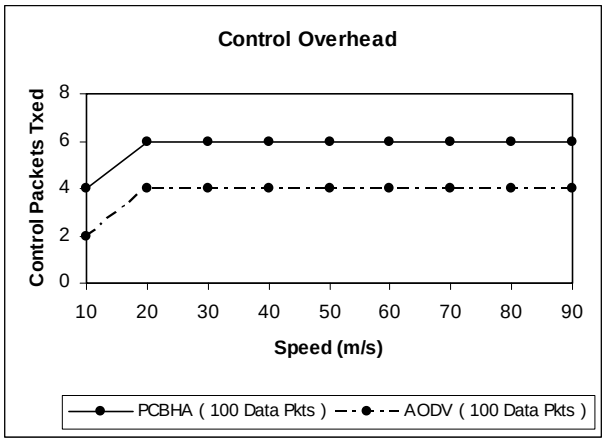


Figure 12. Control Overhead

Figure 13 shows the Route request transmitted vs. speed. As it can be observed that the number of route request transmitted is less in PCBHA compared to AODV.

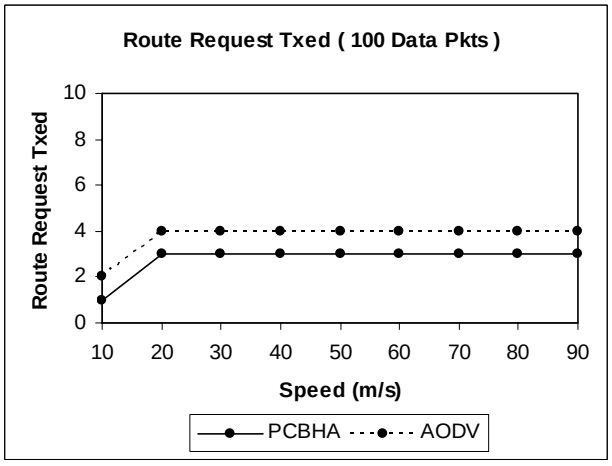


Figure 13. Number of Route Request Transmitted

Figure 14 shows the Link Breakage vs. Speed. It can be observed from the figure that the number of Link Breakage is less in PCBHA compared to AODV

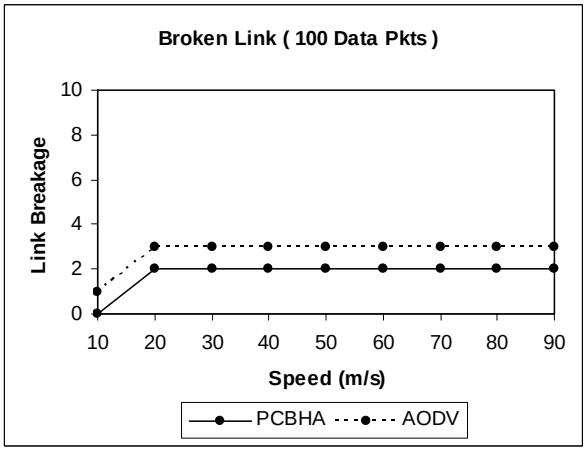


Figure 14. Number of Broken Links

From the above graphs we observed that the proposed method provides a better packet delivery ratio as the nodes are in motion. Also, the link breakages with speed increases is also less in the proposed procedure even with large number of packets delivered.

VI. CONCLUSION AND FUTURE WORK

In this paper the routing security issues of MANETs, are discussed. One type of attack, the black hole, which can easily be deployed against the MANET is described and a feasible solution for it by making use of 'fidelity tables' and assigning fidelity levels to the participating nodes. The percentage of packets received through our system is better than that in AODV in presence of co-operative black hole attack. The solution is simulated using the Global Mobile Simulator and is found to achieve the required security with minimal delay & overhead. Future works may be concentrated on ways to reduce the delay in the network.

REFERENCES

[1] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine,Vol.40, no.10, October 2002.

[2] V. Karpijoki, "Security in Ad Hoc Networks", Seminar on Net Work Security, HUT TML 2000.

[3] C.E. Perkins, S.R. Das, and E. Royer, "Ad-Hoc on Demand Distance Vector (AODV)", March 2000, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-05.txt

[4] Lidong zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue on network security, Vol.13, no.6, November/December 1999.

[5] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 1540-7993/04/$20.00 © 2004 IEEE, May/June 2004.

[6] Yih-Chun, Adrian Perrig, David B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks", sparrow.ece.cmu.edu/~adrian/projects/secure-routing/ariadne.pdf, 2002.

[7] Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R. Das, , Mobile Ad Hoc Networking Working Group, Internet Draft, February 2003.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker Mitigating routing misbehavior in mobile ad hoc networks. In mobile Computing and Networking (MOBICOM), pages 255–265, 2000. Available on: citeseer.ist.psu.edu/marti00mitigating.html.

[9] 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.

[10] S. Buchegger and J. Y. Le Boudec. A robust reputation system for mobile adhoc networks. Technical Report IC/2003/50, EPFL-DI-ICA, July 2003.

[11] P. Michiardi and R. Molva. Preventing denial of service and selfishness in adhoc networks. In Working Session on Security in Ad Hoc Networks, Lausanne, Switzerland, June 2002.

[12] 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.

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

[14] Jorge Nuevo, "A Comprehensible GloMoSim Tutorial" INRS - Universite du Quebec. www.sm.luth.se/csee/courses /smd/161_wireless/glomoman.pdf, March 4, 2004.

[15] Tony Larsson, Nicklas Hedman, "Routing Protocols in Wireless Ad-hoc Networks- A Simulation Study", Masters thesis in computer science and engineering, Lulia University of Technology, Stockholm, 1998.

[16] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei ,"A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", WIRELESS/MOBILE NETWORK SECURITY, 2006 Springer.

[17] C.Siva Ram Murthy and B.S.Manoj," Ad hoc Wireless Networks–Architectures and Protocols", Pearson Education, 2007.

[18] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", www.cs.ndsu.nodak.edu/~nygard/research /BlackHoleMANET.pdf 2003 .

[19] Bracha Hod, "Cooperative and Reliable Packet-Forwarding On Top of AODV", www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf, 2005 .

[20] Chen Hongsong, Ji Zhenzhou and Hu Mingzeng, "A Novel Security Agent Scheme for Aodv Routing Protocol Based on Thread State Transition". Asian Journal of Information Technology, 5 (1) : 54-60, 2006.

Latha Tamilselvan was born in India. She received her B.E. in Electronics & Communication Engineering from Bharathidasan University in 1990, M.E. in Communication Systems from Regional Engineering College, Bharathidasan University, Trichy in 1995. She is doing Ph.D in Computer Science & Engineering in Anna University, Chennai.

She has a teaching experience of 12 years. She is currently working as an Assistant Professor in Information Technology Department at B.S.A.Crescent Engineering College, Chennai, India.

V. Sankaranarayanan was born in India in 1942. He received his B.E. in Electical Engineering from Annamalai University in 1966, M.Sc. (Engg) in High Voltage from college of Engineering, Guindy, Chennai and Ph.D. in computer applications from IIT (Madras) in 1979.

He worked as professor in Anna University for about 3 decades. He was then deputed as Director Tamil Vitual University, from 2004 - 2006 Chennai. He is currently Director at B.S.A.Crescent Engineering College, Chennai, India.