Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining

E. A .Mary Anita
Research Scholar
Anna University
Chennai

V. Vasudevan
Senior Professor and Head/IT
Kalasalingam University
Krishnan coil, Virudunagar

ABSTRACT
Security in wireless ad-hoc networks is a complex issue. The wireless and dynamic nature of ad-hoc networks makes them more vulnerable to security attacks when compared with fixed networks. The existing routing protocols are optimized to perform the routing process without considering the security problem.. Black hole attack is one of the routing attacks in which, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In this paper we propose a certificate based authentication mechanism to counter the effect of black hole attack. Nodes authenticate each other by issuing certificates to neighboring nodes and generating public key without the need of any online centralized authority. The proposed scheme is implemented in two phases: certification phase and authentication phase following the route establishment process of On Demand Multicast Routing Protocol (ODMRP). The effectiveness of our mechanism is illustrated by simulations conducted using network simulator ns-2.

Keywords
MANET; Black hole; ODMRP; Certificate Chain; BHS-ODMRP

1. INTRODUCTION

A mobile ad-hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links in which nodes cooperate by forwarding packets for each other thereby enabling communication beyond direct wireless transmission range. Security in wireless ad-hoc networks is a complex issue. This complexity is due to various factors like insecure wireless communication links, absence of a fixed infrastructure, node mobility, dynamic topology and resource constraints [1]. In mobile ad hoc networks, nodes also perform the role of routers that discover and maintain routes to other nodes in the network. The primary concern of routing protocols of MANET is to establish an efficient and optimal route between the communicating entities. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Nodes are more vulnerable to security attacks in mobile ad-hoc networks than in traditional networks with a fixed infrastructure. The security issues of MANETs are more challenging in a multicasting environment with multiple senders and receivers. Thus, security in network layer plays an important role in the security of the entire network. There are different kinds of attacks by malicious nodes that can harm a network and make it unreliable for communication. These attacks can be classified as active and passive attacks [2]. A passive attack is one in which the information is snooped by an intruder without disrupting the network activity. An active attack disrupts the normal operation of a network by modifying the packets in the network. Attacks can be further classified as internal and external attacks. External attacks are carried out by nodes that do not form part of the network. Internal attacks are from compromised nodes that were once legitimate part of the network.

A black hole attack is one in which a malicious node advertises itself as having the shortest path to a destination in a network. This can cause Denial of Service (DoS) by dropping the received packets.

Public Key Infrastructure (PKI) has been recognized as one of the most effective tools for providing security for dynamic networks. However, providing such an infrastructure in ad hoc wireless networks is a challenging task due to their infrastructure-less nature. The proposed scheme uses the route discovery scheme of ODMRP to issue certificates. Since there is no fixed infrastructure, nodes carry out all required tasks for security solutions including routing and authentication in a self organized way.

The rest of the paper is organized as follows. The next section discusses about black hole attack. Section III gives an overview of ODMRP and the security issues in it. Section IV reviews related work. Section V discusses the proposed method of certificate chaining. In section VI the results of simulation experiments illustrate the impact of localized certificate chains in providing authentication .We present a security enhancement to ODMRP focusing on the route discovery procedure and its resistance to black hole attack. Finally section VII summarizes the conclusion with directions of future work.

2. BLACK HOLE ATTACK

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack in which a malicious node makes use of

the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [3]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the route discovery process, the source node sends route discovery 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 route reply 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.

Malicious nodes take over all routes by attacking all route request messages. Therefore the quantity of routing information available to other nodes is reduced. The malicious nodes are called black hole nodes. The attack can be accomplished either selectively or in bulk. Selective dropping means dropping packets for a specified destination or a packet every‘t’ seconds or a packet every ‘n’ packets or a randomly selected portion of packets. Bulk attack results in dropping all packets. Both result in degradation in the performance of the network.

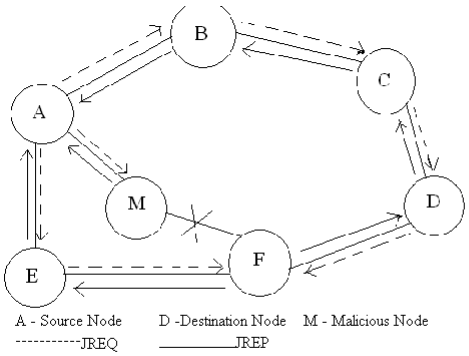

Figure 1 Black Hole Attack

For example, source A wants to send packets to destination D, in figure1, source A initiates the route discovery process. Let M be the malicious node which has no fresh route to destination D. M claims to have the route to destination and sends join reply JREP packet to S. The reply from the malicious node reaches the source node earlier than the reply from the legitimate node, as the malicious node does not have to check its routing table as the other legitimate nodes. The source chooses the path provided by the malicious node and the data packets are dropped. The malicious node forms a black hole in the network and this problem is called black hole problem.

3. OVERVIEW OF ODMRP

ODMRP is a mesh based multicast routing protocol that uses the concept of forwarding group. Only a subset of nodes forwards the multicast packets on shortest paths between member pairs to build a forwarding mesh for each multicast group [4].

In ODMRP, group membership and multicast routes are established and updated by the source on demand. When a Multicast source has packets to send, it initiates a route discovery process as shown in figure 2. A JOIN REQUEST packet is periodically broadcast to the entire network. Any intermediate node that receives a non- duplicate JREQ packet stores the upstream node ID and rebroadcasts the packet. Finally when this packet reaches the destination, the receiver creates a JOIN REPLY and broadcasts it to its neighbors. Every node receiving the JREP checks to see if the next node id in JREP matches its own. If there is a match, it is a part of the forwarding group, sets its FG_FLAG and broadcasts its JREP built upon matched entries. This JREP is thus propagated by each forwarding group member until it reaches the source via a shortest path. Thus routes from sources to receivers build a mesh of nodes called forwarding group.

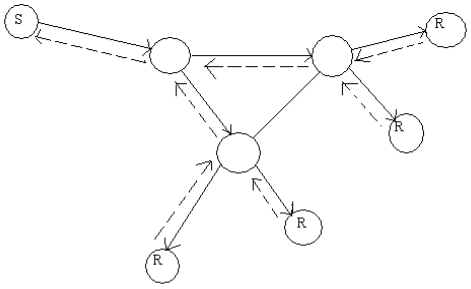

Figure 2 On demand route and mesh creation

The forwarding group is a set of nodes that forward the multicast packets. It supports shortest paths between any member pairs. All nodes inside the bubble (multicast members and forwarding group nodes) forward multicast data packets. A multicast receiver can also be a forwarding group node if it is on the path between a multicast source and another receiver. The mesh provides richer connectivity among multicast members compared to trees.

After the route establishment and route construction process, a multicast source can transmit packets to receivers via selected routes and forwarding groups. A data packet is forwarded by a node only if it is not a duplicate one and the setting of the FG_Flag for the multicast group has not expired. This procedure minimizes traffic overhead and prevents sending packets through stale routes.

In ODMRP, no explicit control packets need to be sent to join or leave the group. A multicast source can leave the group by just stop sending JREQ packets when it does not have any data to be sent to the group. If a receiver no longer wants to receive data from a particular group, it removes the corresponding entries from its member table and does not transmit the JOINTABLE for that group.

3.1 Security in ODMRP

ODMRP does not include any provisions for security. The existing routing protocols are optimized to spread updated routing information quickly when network topology changes without considering the security problem [5]. The messages in ODMRP are basically assumed to be trusted. They are neither encrypted nor authenticated. Hence ODMRP is susceptible to both internal

and external attacks. Attacks can be launched by outsiders who do not possess the credentials to join the network. Secondly, attackers can be compromised group members. The third category of attackers can be non-member nodes who may join the network but do not form part of the multicast group [6].

Black hole attack is an attack on the route discovery process. Black hole attacker first implements rushing attack and gains access to the routing mesh and then drop data packets to become a black hole node. Our focus in this paper is to secure ODMRP from black hole attack by authenticating the routing messages using localized certificate chains.

4. RELATED WORK

Several researchers have studied the vulnerabilities of ad hoc networks against black hole attacks.

Deng et al [7] propose a solution to black hole problem by using one more route to the intermediate node that replays RREQ messages to check whether the route from intermediate node to destination node exists or not. This method avoids the black hole problem and prevents the network from further malicious behavior but the routing overhead is greatly increased. Also, this solution cannot prevent cooperative black hole attacks on MANETs.

Al Shurman et al [8] have proposed two different solutions for black hole. The first solution suggests unicasting a ping packet from source to destination through multiple routes and then chooses a safe route based on the acknowledgement received. The second solution is based on keeping track of sequence numbers so that the black hole nodes which usually modify these sequence numbers can be detected. But these solutions have a longer delay and lower number of verified routes

Marti et al [9] have proposed a Watchdog and Pathrater approach against black hole attack which is implemented on top of Dynamic Source Routing protocol. The Watchdog module cannot detect misbehaving nodes in the presence of ambiguous collisions, receiver collisions, limited transmission power, directional antennas, false misbehavior and partial dropping. Since the system avoids the use of cryptographic methods for securing exchanged messages, it suffers from the possibility of blackmail attacks.

CONFIDANT (Cooperative of Nodes, Fairness In Dynamic Ad-hoc NeTworks) [10] proposed by Buchegger and Le Boudec is an extended version of Watchdog and Pathrater which uses a mechanism similar to Pretty Good Privacy for expressing various levels of trust, key validation and certification. CONFIDANT allows negative ratings from other nodes resulting in false accusation. Moreover CONFIDANT does not address partial packet dropping.

CORE (Collaborative Reputation)[11] is a reputation based system proposed by Michiardi et al similar to CONFIDANT. CORE consists of a set of reputation tables and a watchdog module. Each function that is monitored has a reputation table and a global RT combines the reputations calculated for different functions. The limitation with CORE is that the most reputed nodes may become congested as most of the routes are likely to pass through them. Also the limitations of the monitoring system in networks with limited transmission power and directional antennas have not been addressed in CORE.

Patcha et al [12] have proposed a collaborative architecture for black hole prevention as an extension to the watchdog method.

Bansal et al [13] have proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks), which is the enhanced version of DSR protocol. OCEAN uses a monitoring system and a reputation system to identify malicious nodes. But OCEAN fails to deal with misbehaving nodes properly.

These papers have addressed the black hole problem on unicast routing protocols such as AODV or DSR. Our proposed scheme Black Hole Secure-ODMRP (BHS-ODMRP) is implemented on top of the route discovery process of ODMRP where in the security service is distributed over multiple nodes and nodes authenticate each other in a self organized manner.

5. PROPOSED SCHEME

5.1 Certificate Chaining

Certificate chaining is a self organized PKI authentication by a chain of nodes without the use of a trusted third party. Here authentication is represented as a set of digital certificates that form a chain. Each node in the network has identical roles and responsibilities thereby achieving maximum level of node participation. Every node in the network can issue certificates to every other node within the radio communication range of each other. A certificate is a binding between a node, its public key and the security parameters [14]. Certificates are stored and distributed by nodes themselves. Every node participating in certificate chaining must be able to authenticate its neighbors, create and issue certificate for neighbors and maintain the set of certificates it has issued. The issue of certificates can be on the basis of security parameters of the node. Each node has a local repository consisting of certificates issued by the node to other nodes and certificates issued by others to the particular node. Therefore each certificate is stored twice, one by the issuer and the other for whom it is issued.

Periodically certificates from neighbors are requested and repository is updated by adding new certificates. If any of the certificates are conflicting, i.e., same public key to different nodes or same node having different public key, it is possible that a malicious node has issued a false certificate [15]. A node then labels such certificates as conflicting and tries to resolve the conflict. If certificates issued by any node are found to be wrong, then that node may be assumed to be malicious. If multiple certificate chains exist between a source and destination, the source selects a chain or a set of chains for authentication.

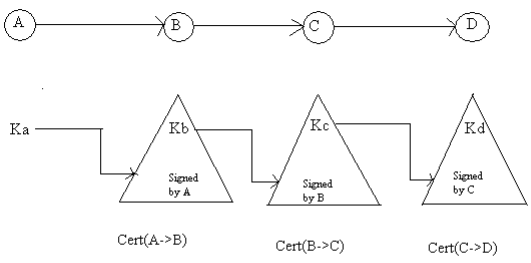

Figure 3 Certificate Chain model

Consider nodes A, B and C in a network as shown in figure 4. Node A issues certificate to node B if it is convinced about the security level of node B. The security parameters to counter the effect of black hole attack may be node id, location of the node and the delay in processing the RREQ packet. The delay for malicious nodes is zero as these nodes do not refer the routing table and respond immediately with a RREP message. The legitimate nodes would have a certain delay time in referring the routing table. The certificate contains the security parameters and the public key of B signed by A. Every other node in the network can verify the signature using A's public key. Certificate issued from node A to node B is represented as cert (A→B). Here A is the issuer and B is the subject of the certificate. Every node forming the route has to prove its identity and obtain a certificate from its neighboring node. Each certificate is issued with a limited validity period and contains the time of issue and expiration time [16]. Before a certificate expires, the issuer issues an updated version of the same certificate with an extended time of expiry if the issuer node is still convinced of the security level of the subject node. This updated version of certificate is called certificate update. When node A wants to communicate with node D, it finds a chain of valid public key certificates leading to D. The chain is such that the first hop uses an edge from A i.e., a certificate issued by node A and the last hop leads to D i.e., certificate issued to D. All intermediate nodes are trusted through the previous certificates in the path. The last certificate contains the public key of the destination.

5.2 Authentication using Certificate Chaining

BHS-ODMRP is a security extension of ODMRP where the route discovery phase is extended and messages are signed to guarantee their authentication. The extended route discovery process of BHS-ODMRP consists of the original route discovery process followed by a certification phase and an authentication phase.

5.2.1 Certification phase

The certification phase is implemented in three parts: key generation and certificate issuing part, certificate update part and the certificate revocation part.

5.2.1.1Key generation and Certificate issuing

Once the route is established between the source and the destination, the nodes forming the route enter into a certification phase. The source node requests the identity of the next hop node and generates a public key based on its identity. The security parameters of the next hop node are then requested and public key certificates are issued if the issuer is convinced about the security parameters. The time taken to process the JREQ packet and the location of the node are ideal parameters to determine the security level of the node with respect to black hole attack. For different attacks, different security parameters may be chosen. All certificates issued are stored in the repositories of the issuer and the certificate subject. Exchange of certificates between neighboring nodes takes place periodically. By this certificate exchange mechanism, nodes accumulate certificates in their repositories at a low communication cost because the exchanges are performed locally in one hop. For example if node B is within the radio range of node A, node A issues a certificate to B.

$$\text{Cert}\ (A \rightarrow B) = [ID_B, K_B, t, e, S]\ K_A \qquad (1)$$

The certificate contains the identity of node B, the public key of B, the time of issue of the certificate, the time of its expiry and the security level of the node, signed by the public key of A.

Initially the security level is set to 1 if an issuer node is convinced of the security parameters of the subject node. If security is found to be compromised, the security level parameter S is reduced to zero. A node bearing a certificate with S=0 is set aside as malicious node.

The public key is calculated by applying a one way hash function H, to the identity of the node. The identity may be either IP address or MAC address.

$$K_B = H\ (ID_B) \qquad (2)$$

Since the same hash function is used by all nodes, the public key generated by different neighboring nodes for a particular node would be the same.

5.2.1.2 Certificate Update

Each certificate has an expiry time after which it becomes invalid. If the certificate is still required to be used, the issuer has to update the certificate if it is still convinced about the security level of the subject node. On the other hand, if the issuing node feels that the subject node is compromised, it will not provide the certificate update.

5.2.1.3 Certificate Revocation

When the binding between a node and its key is found to be invalid, the issuing node can revoke the certificate. The revoked certificate is not usable.

5.2.2 Authentication phase

The authentication phase follows the certification phase. When a source node A wants to find a route to a destination node D, it broadcasts a JREQ packet. The destination node or any other node that has a valid route to the destination now replies to the JREQ. The JREQ and JREP packets in BHS-ODMRP are similar to that of ODMRP. Any malicious node may reply to the request from the source by claiming to have the shortest path to the destination. To overcome this black hole attack, source node does not initiate the data transfer process immediately after the routes are established. Instead it waits for the authenticated reply from the destination. After the certification process, the destination node sends authenticated messages appended with certificates taken from the corresponding node's repository. The certified JREP ($JREP_{cert}$) packet from the destination would be of the form:

[source id, next hop id, final destination id, certificate chain] (3)

Consider the following network shown in figure 4

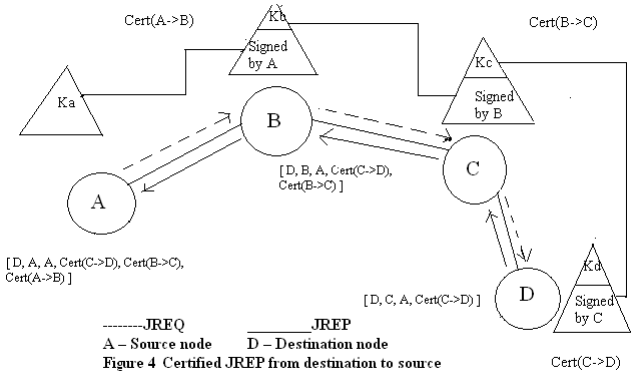

Figure 4 Certified JREP from destination to source

The $JREP_{cert}$ packet from D would be

[D, C, A, cert (C→ D)] (4)

When this packet reaches node C

a) Node C checks its repository to see if cert (C→ D) is there.
b) Then it checks the certificate revocation list to find if node D is malicious or not.
c) If these two verifications lead to a positive result, node C forwards the $JREP_{cert}$ to the next hop node B. While doing so it appends cert (B→ C).

The $JREP_{cert}$ packet from C would be

[D, B, A, cert (C→ D), cert (B→ C)] (5)

All intermediate nodes perform the same procedure until the final destination A is reached. The $JREP_{cert}$ packet from B would be

[D, A, A, cert (C→D), cert (B→C), cert (A→B)] (6)

When node A receives the packet, it checks the whole certificate chain. If there is no problem with the certificate chain, node A trusts the route and starts sending data packets through this route.

In case of a legitimate node turning malicious over a period of time, the node's behavior would be recorded and the certificate would not be renewed after its expiry time, thus isolating the node from further participation in the network activities.

Since the security levels of participating nodes are updated based on their faithful participation in the network, any malicious nodes between the source and destination can be very well isolated from the network as these nodes would not be able to produce the certificates to be appended with the $JREP_{cert}$ message.

5.3 Algorithm for BHS-ODMRP

Notations:
SN : Source Node
IN : Intermediate Node
DN : Destination Node
NHN: Next Hop Node

a) At source node

SN broadcasts JREQ
IF (IN is NOT DN) THEN
Rebroadcast JREQ
ELSE return JREP

b) At destination node

DN unicasts JREP

All INs forward the JREP

JREP reaches SN

Route is established between SN and DN

c) Certification Phase

Nodes forming the route certify each other:
Request id and security parameters of NHN
Generate public key of NHN based on id
Issue Certificates encrypted with public key

Store certificates in repository

Exchange Certificates with neighbor nodes

d) Authentication Phase

DN unicasts certified JREP appended with certificate from next hop node.

All INs append their certificates and forward the certified JREP

$JREP_{cert}$ reaches SN

SN verifies certificate chain

Routes data packets through the secure path

6. PERFORMANCE EVALUATION

The goal of this section is to compare the performance of our proposed protocol BHS-ODMRP with that of the original ODMRP under different scenarios. The metrics used for evaluation are:

Packet Delivery Ratio: The ratio of the number of data packets delivered to the destinations to the number of data packets generated by the sources.

Average End-to-End Delay: This is the average delay between the sending of packets by the source and its receipt by the receiver. This includes all possible delays caused during data acquisition, route discovery, queuing, processing at intermediate nodes, retransmission delays, propagation time, etc. [17]. It is measured in milliseconds.

6.1 Simulation Profile

The simulation settings are as follows. The network consists of 50 nodes placed randomly within an area of 500m x 500 m. Each node moves randomly and has a transmission range of 250m. The random way point model is used as the mobility model. In this model, a node selects a random destination and moves towards that destination at a speed between the pre-defined maximum and minimum speed. The minimum speed for the simulations is 0 m/s

while the maximum speed is 50 m/s. The channel capacity is set to 2Mbps and the packet size is 512 bytes. The CBR traffic is generated with a rate of 4 packets per second. The simulation time is 900secs. The simulations were carried out with different number of attackers. The malicious nodes were selected randomly.

6.2 Discussion of results

Figure 6 shows the variation of packet delivery ratio (PDR) with mobility for a multicast group consisting of 1 sender and 20 receivers with 3 black hole nodes. To simulate such a scenario we set the delay of all legitimate nodes to 30ms and that of the attackers to 0ms.

It is observed that the PDR of ODMRP varies from 98% to 96% for a variation of node mobility from 10 m/s to 50 m/s and most packets get to the destination in the absence of attackers.

When there are 3 black hole nodes in the group, the PDR reduces by around 9%. By securing the route using BHS-ODMRP the PDR improves by around 5%. This is due to the fact that the malicious nodes are identified during the certification phase and blacklisted in the repository of each node in the network. Therefore, even if a malicious node tries to send a false RREP to the source node claiming to have the shortest path to the destination, it will not be able to succeed as it would lack the authenticated certificate. Thus the impact of black hole nodes on the performance of the network is countered.

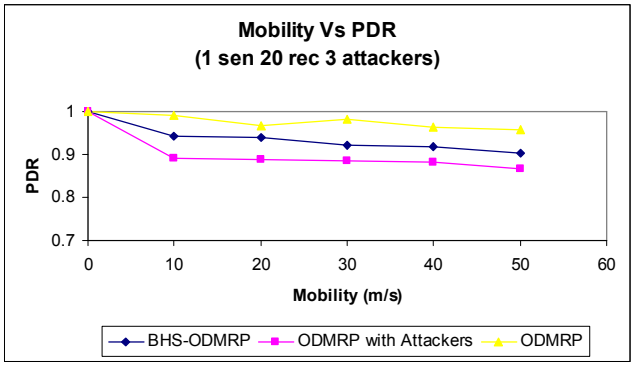

Figure 6 PDR for 1 sender 20 receivers with 3 attackers

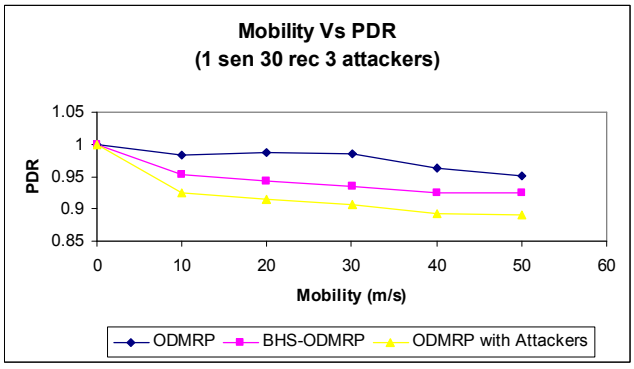

Figure 7 PDR for 1 sender 30 receivers with 3 attackers

Figure 7 depicts the effect of black hole attack on the same group but with an increased number of 30 receivers. It is seen that the reduction in PDR is comparatively lesser than that in the group with 20 receivers. Our proposed protocol improves this situation by around 3%. An increased number of receivers make the routing mesh denser thereby increasing the PDR. Therefore even if a packet is dropped on a path, a duplicate copy is delivered to receivers through other redundant paths in the mesh.

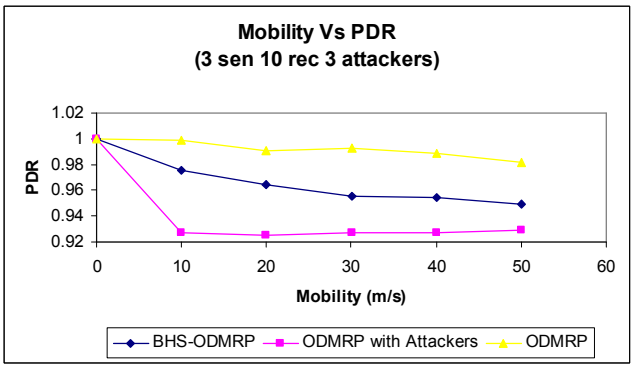

Figure 8 PDR for 3 senders 10 receivers with 3 attackers

Figure 8 shows a scenario with the number of senders increased to 3 with the same number of attackers. Our proposed protocol BHS-ODMRP improves the PDR by around 5%. Moreover it is seen that a multicast group with more number of senders is able to withstand the attack to a reasonable extent when compared to a smaller group which is easily susceptible to attacks. This effect is due to the presence of more alternative routing paths in the mesh.

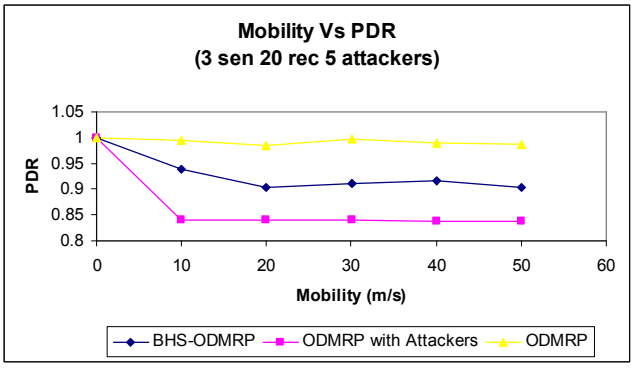

Figure 9 PDR for 3 senders 20 receivers with 5 attackers

When the number of attackers is increased to 5, the network is unable to bear the attack and there is a large reduction in the packet delivery ratio due to loss of packets in the black hole nodes. The reduction of PDR ranges from 13% to 15% when compared to the normal ODMRP without attackers as shown in figure 9 and figure 10.

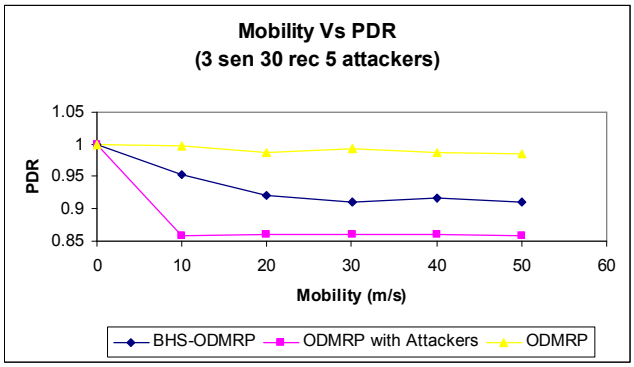

Figure 10 PDR for 3 senders 30 receivers with 5 attackers

Our proposed protocol improves this situation by increasing the PDR by around 10%. This implies that BHS-ODMRP resists black hole attack by identifying attackers and isolating them from the network.

Figure 11 shows the variation of PDR when the number of attackers in the network is varied from 0 to 5 in a group of 3 senders and 20 receivers. As the number of attackers increases from 0 to 5, the PDR of ODMRP reduces from 99% to 84%. BHS-ODMRP improves this situation by increasing the PDR to 97%, which amounts to about 13% increase in performance.

Figure 12 shows the variation in end-to-end delay of the network for a multicast group consisting of 3 senders and 20 receivers in the presence of 5 attackers. There seems to be a 10% increase in the delay in the presence of attackers. This is because of the fact that non shortest paths containing black hole nodes are selected for routing the packets.

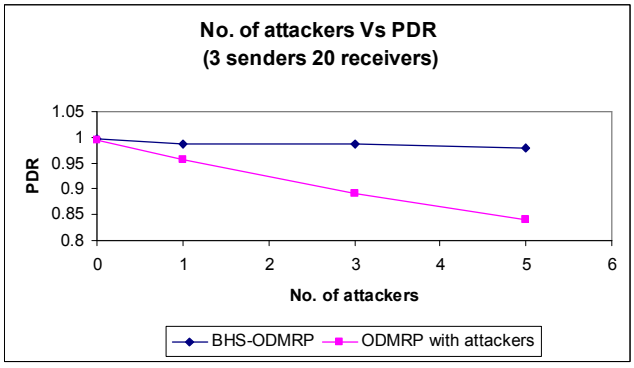

Figure 11 Variation of PDR with attackers

Our proposed protocol further increases the delay by a margin of only 5%. This may be attributed to the time taken to verify the repository and append the certificates to the $RREP_{cert}$ packet. The end –to-end delay also includes the delay in route discovery process.

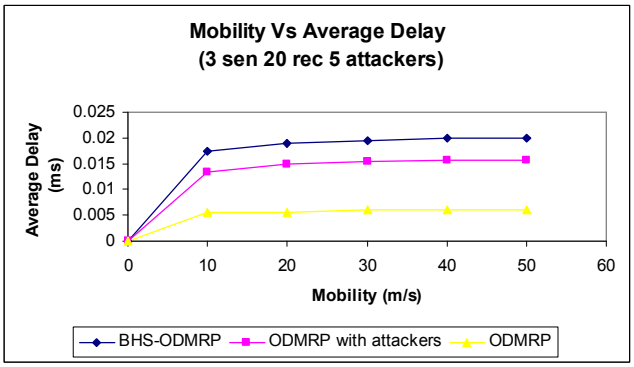

Figure 12 Delay for 3 senders 20 receivers with 5 attackers

Figure 13 depicts the variation in end-to-end delay of the network when the number of attackers is varied from 0 to 5 in a group consisting of 3 senders and 20 receivers. We see that BHS-ODMRP results in an increased delay of 8 to 9%. Given the improvement in network security and the impact of the attack on the performance of the protocol the increase in delay can be accepted as a reasonable value.

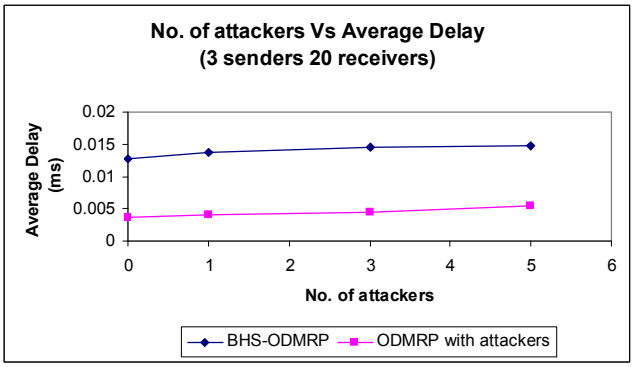

Figure 13 Variation of delay with attackers

From the analysis of the graphs, we conclude that our proposed protocol conforms to the standards of original ODMRP protocol while improving the security of the network.

7. CONCLUSION

Security is one of the major issues in MANETs. In this paper we have proposed a solution for black hole attack by authenticating nodes using localised certificate chains. Our simulations show that BHS-ODMRP is as effective as ODMRP in discovering and maintaining routes in addition to providing the required security. The proposed protocol reduces the packet loss due to black holes to about 20% which is about 15% higher compared to ODMRP protocol. Security is implemented on top of the route discovery process of ODMRP. There are no modifications made to the JREQ and JREP messages. Certified JREP messages are appended with the certificates to allow authorized nodes to participate in the routing process. This authentication mechanism eliminates the need for a centralized trusted authority which is not practical in MANETs due to their self organizing nature. Also, the proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate

publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbors.. After a period of time each node has a directory of certificates and hence the overhead incurred in this process is reasonable with a good network performance in terms of security. We believe that this is an acceptable performance, given that the attack prevented has a much larger impact on the performance of the protocol. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.

REFERENCES

1. D. Djenouri, L. Khelladi and N. Badache, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys & Tutorials, Vol. 7, No. 4, 4th Quarter 2005.
2. L. Zhou and Z. J. Haas, Securing Ad Hoc Networks, IEEE Network Magazine, Vol. 13, No. 6, Nov./Dec. 1999, pp. 24–30.
3. E. A. Mary Anita and V. Vasudevan, Black Hole attack on multicast routing protocols, JCIT, Vol.4, No.2, pp. 64–68, 2009.
4. A. Vasiliou and A. A. Economides, Evaluation of Multicasting Algorithms in Manets, PWASET, vol. 5, April 2005, pp. 94-97.
5. S.Lee, M.Gerla and C.Chain, "On Demand Multicast Routing protocol-(ODMRP)," Proc. of the IEEE Wireless Communication and Networking Conference (WCNC), September 1999.
6. E. A. Mary Anita and V. Vasudevan, Performance Evaluation of mesh based multicast reactive routing protocol under black hole attack, IJCSIS, Vol.3, No.1, 2009.
7. H. Deng, W. Li, and Dharma P. Agrawal, Routing Security in Ad Hoc Networks, IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, October 2002, pp. 70-75.
8. Al-Shurman, M. Yoo, S. Park, Black hole attack in Mobile Ad Hoc Networks, ACM Southeast Regional Conference, 2004, pp. 96-97.
9. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000), Mitigating routing misbehavior in mobile ad-hoc networks, Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom), ISBN 1-58113-197-6, pp. 255-265.
10. 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.
11. 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.
12. A. Patcha and A. Mishra, Collaborative security architecture for black hole attack prevention in mobile ad hoc networks, Radio and Wireless Conference, 2003. RAWCON '03, Proceedings, pp. 75-78, 10-13 Aug. 2003.
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. C. Srdjan, B. Levente, and H. Jean-Pierre, Self- Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, vol. 2, pp. 52-64, 2003.
15. C. Siva Ram Murthy and B. S. Manoj, Ad hoc Wireless Networks- Architectures and Protocols, Pearson Education, 2007
16. Ruidong Li, Jie Li, Hisao Kameda and Peng Liu, Localized Public Key Management for mobile ad hoc networks, IEEE Communications Society, 2004, 1284-1289
17. Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004), Security in mobile ad hoc networks: Challenges and solutions, IEEE Wireless Communications, 11(1), 38-47.