Security Enhanced AOMDV Protocol to Prevent Black Hole Attack in MANET

K.Selvavinayaki #[1], Dr. E. Karthikeyan*[2]
[1]Asst Professor, Karpagam Institute of Technology , Coimbatore, India,
[1]uk.selvavinayaki@gmail.com
[2]Asst Professor,Department of Computer Science, Govt. Arts College, Udumalpet, India
[2]e_karthi@yahoo.com

Abstract-The dynamic nature of Manet will always degrade the reliability in data transmission between the nodes. The manet is not protected against the attacks due to lack of security. The most common attack experienced by the Manet is black hole attack. This paper address the security oriented solution to prevent the black hole attack using the digital certificates to authenticate the routes selected during the route discovery process. The digital certificate authentication avoids the black hole node during the Route discovery itself. This methodology is implemented on AOMDV protocol. The algorithm is simulated using NS2.

KeyWords : MANET, BlackHoleAttack, Digital Certificates, Hash function ,AOMDV

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is the collection of self organized mobile nodes where creating the infrastructure would be impossible or prohibitively expensive. Mobile nodes in the adhoc network do not communicate through the fixed structures. Each mobile node acts as a host when requesting information from the nodes or providing information to the nodes in the network. The mobile nodes are self organized which will act as the router when discovering and maintaining routes for other nodes in the network.

The mobile nodes are always dynamic in nature, which mean that they may leave or join the network at any time. The control towards the nodes becomes distributed .This features degrades the reliability in secured data transmission and makes the network to suffer from various routing attacks. [6]

A. Routing Attacks

General attacks are the threats against the Physical, MAC and network layer which are the most important layers that functions for the routing mechanisms of MANETs. Attacks in the network layer either not forward the packets or edit the messages by adding or changing the parameters in the routing messages. The fundamental attack that a malicious node can execute is to stop forwarding the data packets. When the route with malicious node is selected it denies the communication to take place. [15, 16]

B. Black Hole Attack

In this type of attack, the malicious node waits for the neighbours to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets through the malicious node. A malicious node does not allow forwarding any packet anywhere. The attack is called a black hole as it drops all the objects and the data packets.[7,15]

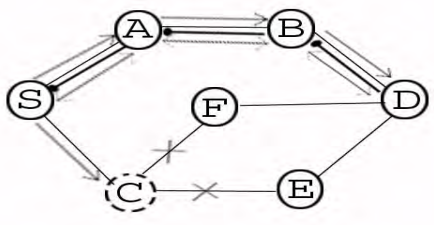

Figure 1: Black Hole Attack

For example in Figure1, Assume node C to be a malicious node. Using the AOMDV routing protocol, node C claims that it has the route to the destination node whenever it receives RREQ packets, and sends the response to source node at once. The destination node may also give a reply. If the reply from a normal destination node reaches the source node of RREQ first, everything works well; but the reply from node C could reach the source node first, if node C is nearer to the source node. Moreover, node C does not need to check its RT when sending a false message; its response is more likely to reach the source node firstly. This makes the source node to think that the routing discovery process is completed and queues all other reply messages in the routing table, and begin to send data packets. The forged route has been created. As a result, all the packets through node C are

simply consumed or lost. Node C could be said to form a black hole in the network, and we call it as the black hole attack.

C .Adhoc On Demand Multipath Distance Vector Routing Protocol.(AOMDV)

The objective behind the design of AOMDV is to provide efficient fault tolerance in the sense of faster and efficient recovery from route failures. The key feature of the proposed protocol is the on-demand computation of multiple loop free link-disjoint paths. AOMDV is the multipath routing protocol which combines the destination sequence number in DSDV with the route discovery technique in the DSR protocol. [17]

AOMDV computes the multiple loop free paths during the route discovery process. With the availability of the multiple paths, the protocol switches from one route to next possible best route when the previous route fails. The new route discovery process in initiated only when all the paths to a specific destination fails. The loop free link disjoint paths and multipath routing are very effective there by reduces routing overheads and supports better load balancing. A switch to the alternative routes will avoid the node congestion. The multipath routing avoids the routing overhead .AOMDV allows the multiple paths for the same destination sequence numbers. The multiple paths are formed via the neighbours through which the RREQ or RREP are received from that neighbour. The alternate route selection due to the route failure while completely eliminates the route discovery latency. [8]

The paper is organized as follows. The analysis of the related methodology is presented in the chapter 2.The Proposed solution is described in Chapter 3. The Chapter 3 describes the proposed solution in Three phases. The first phase explains the digital certification process and elaborates the route discovery process. The second phase explains the Authentication Phase. And the last phase describes the Black hole detection process.

II.RELATED WORK.

There are many solutions given by the researchers to prevent the black hole attacks in manet. The solutions are proposed and implemented on the various protocols like DSR,AODV and AOMDV.[11,12,14,18].

Marti.S et al [5] has proposed a Watch Dog and Path Rater approach against black hole attack which is implemented on the top of Dynamic Source Routing Protocol.

E.A Mary Anita et al [2] proposed a solution implemented on the top of ODMRP protocol .The authors proposed a certificate based authentication mechanism to counter the effect of black hole attack.

Sanjay Ramasamy et al [3] proposed a method for identifying multiple black hole attack. They modified the AODV protocol by introducing data information table and cross check. Every entry of the table is maintained by table.

Latha Tamil Selvan et al [4] proposed a solution with the enhancement of AODV protocol which avoids multiple black holes in the group. The technique is to identify cooperative black hole nodes and to discover the safe route for transformation. The methodology uses fidelity table where every participating node is given a fidelity level that will provide reliability to that node. Any node having " 0" value is considered as malicious node and that node is eliminated.

Hesiri Weerasinghe [9] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution add some modifications to sanjay Ramasamy proposal to improve the accuracy in detecting the black hole attack.

K.Selvavinayaki et al[1]proposed a solution using digital certificates chains . The methodology is added on the top of the DSR protocol to prevent the black hole attack in Manet.

The proposed algorithm is the solution to prevent the black hole node and improve the packet delivery ratio. The solution is placed on the top of AOMDV protocol .This proposed solution proves to be efficient in improving the performance of the AOMDV protocol by increasing the packet delivery ratio and minimizing the route over head .

III. PROPOSED SOLUTION

A. Digital security certificates

The Digital certificate is the security certificate which is self organized PKI infrastructure and Public key is authenticated by the chain of nodes . Authentication is represented as a set of security certificates .Every node in the network can issue certificate to every other node within the radio communication range of each other. Every node in the network should be able to authenticate the other nodes in the network, by creating and issuing the certificates to the neighbours .The node also maintains the certificates received from the other neighbours. The certificates are issued based on security trust value. The nodes make a periodical request for the certificates from the neighbours. The certificates are validated for the public key. If it is found that there are two different nodes having the same Public key or two different key assigned for the same node then the corresponding node is assumed to be malicious node. The route including the malicious node is avoided and the best alternative route is selected.[18]

After the route discovery process the nodes enter into the Authentication phase. All the nodes in the route concerned tries to authenticate its neighbours. The nodes request the IP address of its neighbour and apply the hash function and generates the Public key.[19]

$$HMAC_{PK}(M) = H((K + SPAD) \| H((K + EPAD) \| M))$$

Where HMACpk(M) is the hash function of the Message M.Here the message is the IP address of the node.h is the hash function ,spad and epad is the padding sequence. h () is the underlying hash function. K is the secret key. HMAC provides the secured public key which cannot be attacked by the intruders. The public key forms the part of the digital certificate.

The digital certificate contains the following components.

[IP - ADDRESS, PK, TV, ET] KEY OF THE ISSUE NODE

Example: Certificate issued by source S to intermediate node I.

[DC(S- > I) = [IP, key I, TV, ET] key S.

PK is the public key of the receiver node. TV is the Trust Value of the node and ET stands for Expiration time of the certificate.

Before a Certificate is generated the issue node checks whether the TV value is feasible. If feasible, the public key is generated and certificate is issued to the receiving node and a copy of the same is stored in the routing table of the issuer .TV is calculated based on the time taken to process the RREQ packet and the location of the node. The Malicious node which receives the RREQ will immediately process the RREQ by sending the RREP immediately without verifying the Route table for the availability of the node. When the source node receives the RREP too earlier than the expected time, it suspects the RREP initiator as the malicious node. If the source node suspects a node to be malicious node it eliminates the node from that route and select the alternate route. The Certificates are exchanged periodically between the neighbouring nodes.[12]

DC(S → A) DC(S → B) DC (D → A) .

Initially the TV value is set to the threshold value. If the security of the node is found to be compromising the TV values keeps reducing and once if it reach zero then node is marked as the malicious node. Threshold value is the time dependent trust value. Initially node s have the trust value on intermediate node B is at time T1.[20] If the security of the node is found to be compromising the TV values keeps reducing and once if it reach zero then node is marked as the malicious node. Let A^TB (t1) be the trust value of node A to node B at time t1 and A^TB (t2) be the decayed value of the same at time t2. Then trust value can be defined as follows,

$$_ATv_B(t_2) = {}_AT_B(t_1) * e^{-({}_AT_B(n)\Delta t)^{2k}}$$

The algorithm can be divided into three phase.

1).Route Discovery Process

2).Authentication Process

3).Black Hole Detection Process.

The proposed solution enters into the route discovery process and the selected route will be authenticated by the issuing the digital security certificate to all the nodes in the route after the node being authenticated by the neighbouring nodes.

1).Route Discovery Process: When a source node S wants to find a route to a destination node D, it checks in the Routing table whether the route to the Destination is already available. If there is no previous route to the destination then the Source broadcasts a RREQ packet to the neigh boring nodes. when a RREQ packet arrives at an intermediate node, RREQ is scanned; if the destination address of the RREQ is same as address of intermediate node then the intermediate node acts as destination node to send route reply else it rebroadcast the RREQ The destination node or any other node that has a valid route to the destination now replies to the RREQ. The RREP packets in Security enhanced AOMDV are similar to the DSR. Any malicious node may reply to the request from the source by claiming to have the shortest path to the destination. All the Disjoint routes are stored in the Routing table. The K-level shortest path algorithm is used to discover the entire shortest path among the disjoint links. The stored routes in the routing table are sorted based on the shortest communication cost.

2). Authentication Process: To prevent the black hole nodes from being dropping the packets, the selected route is not used for the data transmission immediately. All the nodes in the route enter into the authenticated phase for being authenticated by the neighbouring nodes in the path. The source waits for the authenticated reply from the destination node. The destination node sends the authenticated messages appended with the digital security certificate that is issued by the neighbouring node in the network.

The authenticated RREP packet from the destination would be in the given form.

[Source ID, next hop ID, final dest node, DSC]

The RREP packet from D would be [D, A,DSC(A->D)].When this packet reaches the node A,it checks its routing cache to verify whether DSC(A->D) is available. It checks whether D is the black hole node by verifying the certificate issue list by A. If D is the promiscuous node then it forwards the RREP packet to S by appending the Certificate of A.

The forwarded RREP will be in the form as follows.

[[D, A, S, DSC(D → A), DSC(A → S)]

The process is continued by all the intermediate nodes in the route until the RREP reaches the SourceNode. When the RREP reaches the S, S node checks the whole certificate group. If there is no issues in the certificate, Node S trust that the route is secured one and start sending the packets through the route.

3) Black Hole Detection Process: If any of the Digital Security Certificates is found to be mismatching, which means same certificate from different nodes or certificate having the same key or same node having different certificates then the corresponding node is marked as the malicious node . The alternate route is selected from the routing table. The source ignores all the alternate paths [10], if it includes the malicious node which is been traced in the previous route. The following procedure elaborates route discovery process and the alternate path selection process for the secured data transmission approach in Manet.

```
1.  BEGIN
2.  Initialize Source, Destination. Nexthop, SV
3.  Assign  SN – Source , IN- Intermediate node, DN-Destination ,NHN-NextHop Node
4.  Assign  Sv = 1;
5.  Calculate the Delay Time for all the node in the Network
6.  DT = (α · Old_DT) + ((1 − α) · New_DT)
7.  Route Discover(data packet)
8.  BEGIN
        If (SN)  THEN Lookup Route Table (Dest_id)
        {If (Route_not_found) then addRouteEntry(Destination_id)
                Dest_seq_no= undefined;
                seq _ no=  seq _no +2;
                Endif
                }ELSE     Bcast_id = Bcast_id +1;
9.  Broadcast_RREQ(sourc0e_id:seq_no:0,00.Destination_id:Dest_id,Dest_seq_no:
    Dest_seq_no,advertisedHopCount:0)
10. END
11. IF (IN is NOT DN) THEN
12. {Rebroadcast RREQ}
13. ELSE
14. {DN return RREP
15. DN unicasts RREP}
16. All INs forward the RREP
17. If (RREP reaches SN)  THEN
18. {
19. If RREP Time <  the Delay time   THEN
20. Set SDC =0; \\ Do not Issue Security Certificate.
21. Check the route cache for alternate route.
22. }
23. ELSE
24. {
25. Route is established between SN and DN}
26. STORE the Alternate Routes
27. Nodes forming the route certify each other:
28. {
```

```
29. Request id and security parameters of NHN
30. Generate public key of NHN based on ID
31. Issue Certificates encrypted with public key
32. Store certificates in route cache
33. Exchange Certificates with neighbor nodes
34. }
35. DN sends certified RREP appended with  Digital Security certificate from NHN
36. For I = N to  1
37. {
38. IF isAvaialbe( SDC (D) )  in IN  THEN
39. {
40. If(IN SDC(D)) =  SDC(D)  THEN
41. INs append their certificates and forward the certified RREP}
42. ELSE
43. Revoke the SDC form the Node.
44. }
45. RREP reaches SN
46. SN verifies certificate chain of the Route unicasted by DN.
47. isVALID(CertificateChain) THEN
48. send the DataPackets through the Route.
49. Else
50. Broadcast the route as Malicious route to all the other nodes in the network.
51. Stop forwarding data packets.
52. Select the alternative route. From Route Cache.
53. END;
```

Table1: Route Discovery and Alternate Path Selection Algorithm

The following algorithm explains the alternate path selection approach , in the Black Hole Detection and Removal process .The source node implements this algorithm to select the alternate route when the route selected for the transmission from the source to destination is attacked by the malicious nodes.

```
1.  BEGIN
2.  Let S is a set of S-1 Alternate  paths
3.  // Let p1,p2,p3,……p s-1 be the s-1 Alternate  paths that are stored at two dimensional array S.
4.  //INTIALIZE N;
5.  Let N=set of paths that are node- disjoint and free from malicious links.
6.  Initialize N= 0.
7.  // N is computed as follows
8.  Let Pm be the path with malicious node.
9.  For k=1 to S-1 do
10. {
11. //Select Pk from S and Check whether it includes the malicious link. //
12. If ( Pk ∩ Pm =0 )
13. then add Pk to N;
14. }
15. If N=0 then
16. Goto  Route Discover(data _packet)";
17. Else
18. Route selected = Pk   // Pk is  the shortest path with no  malicious link.
19. END
```

Table2: Alternate Path selection Algorithm

IV. PERFORMANCE EVALUATION

A. Simulation setup.

The algorithm is simulated using NS2 simulator. In our simulation, 200 mobile nodes move in a 1600 meter x 1600 meter square region for 60 seconds simulation time. [13]All nodes have the same transmission range of 250 meters. Our simulation settings and parameters are summarized in table 3.

No. of Nodes	200
Area Size	1600 X 1600
Mac	802.11
Radio Range	250m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Transmitter Amplifier	150 pJ/bit/m2
Package rate	5 pkt/s
Protocol	AOMDV

Table 3: Simulation Parameters

The methodology is implemented on AOMDV protocol. The performance results are compared with the other algorithms like DSR, AOMDV and previously implemented SEDSR protocols. SAOMDV is the protocol where the proposed algorithm is implemented. This protocol is based on AOMDV. SDSR is the modified DSR protocol with black hole node prevention mechanism.

B. Performance metrics:

The performance of the algorithm is mainly evaluated based on the following performance metrics.

1. Average End-to-End Delay
2. Packet Delivery Ratio.
3. Through Put.
4. Routing Over Head.

1) Average End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

2) Packet Delivery Ratio: It is the ratio of packet received to packet sent successfully. This metric indicates both the loss ratio of the routing protocol and the effort required to receive data. In the ideal scenario the ratio should be equal to 1. If the ratio falls significantly below the ideal ratio, then it could be an indication of some faults in the protocol design. However, if the ratio is higher than the ideal ratio, then it is an indication that the node receives a data packet more than once. It is not desirable because reception of duplicate packets consumes the network's valuable resources. The relative number of duplicates received by the node is also important because based on that number ,the node can possibly take an appropriate action to reduce the redundancy.

3) Throughput: It is defined as the number of packets received successfully.

4) Routing overhead: The ratio of routing packets to delivered data packets.

C. Results and Discussion

The Simulation has been carried out in two aspects. In the first aspect , the algorithm is simulated by modifying the number of nodes. In the Second aspect the simulation is carried out by modifying the speed of the nodes.

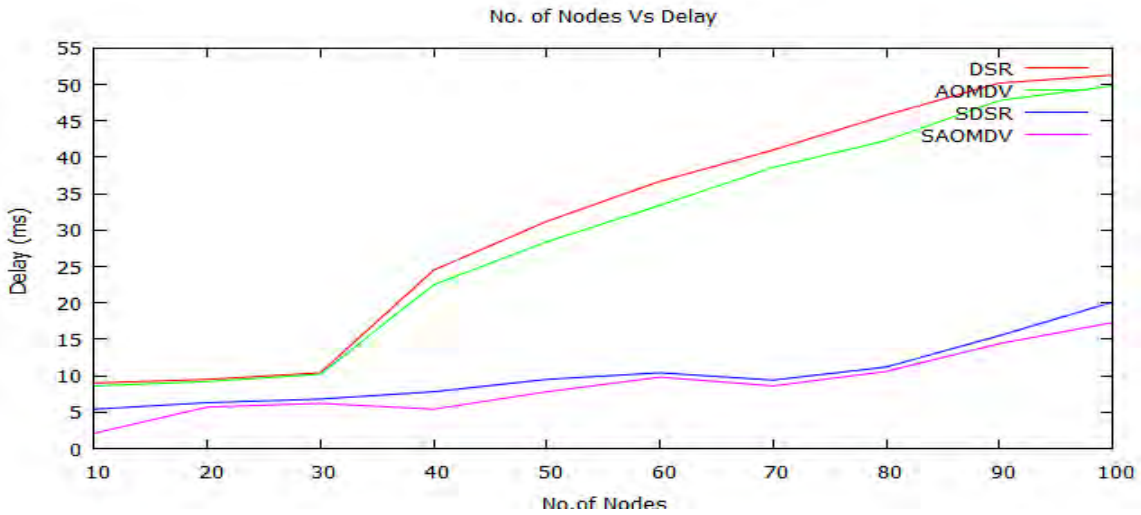

Figure2: Average End to End Delay

Figure 2 shows the comparison of the Average End to End Delay of the Various protocols like SAOMDV,AOMDV,DSR and SDSR. The average End to End Delay varies with reference to the no of nodes. Obviously The SAOMDV protocol ,which is our proposed protocol has less end to end delay when compared with the other protocols because of more authentication process.

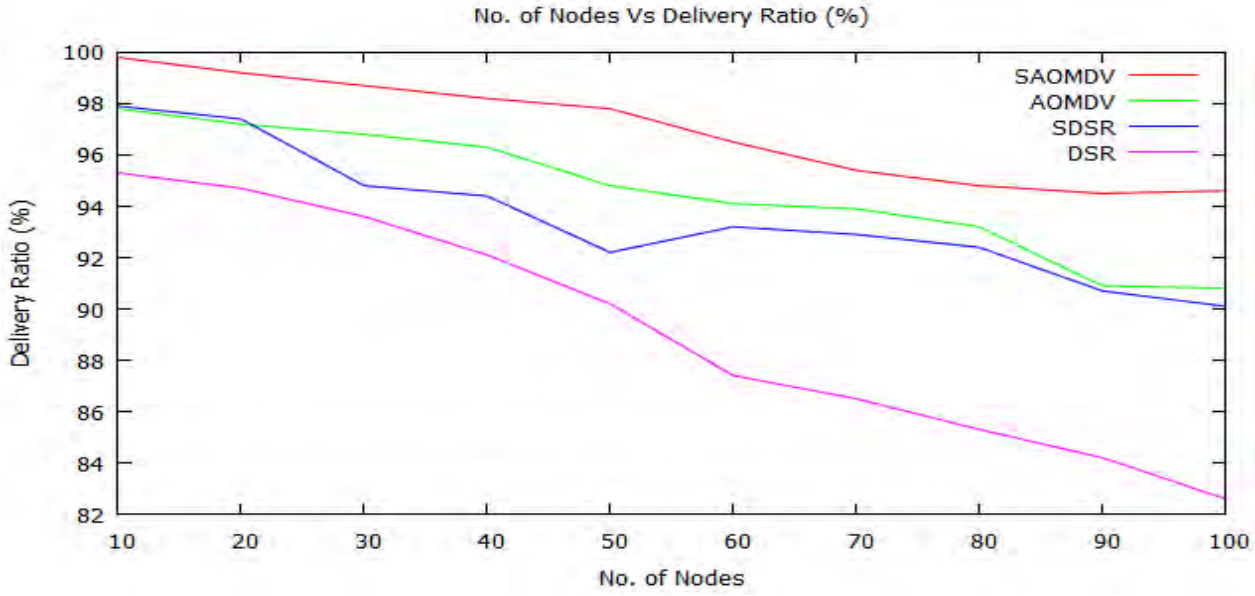

Figure 3: Packet Delivery Ratio

Figure 3 shows the comparison analysis of the packet delivery ratio . SAOMDV protocol provides very high packet delivery ratio due to the fact that the protocol is highly authenticated and data packets are transmitted only through the secured and reliable route. .

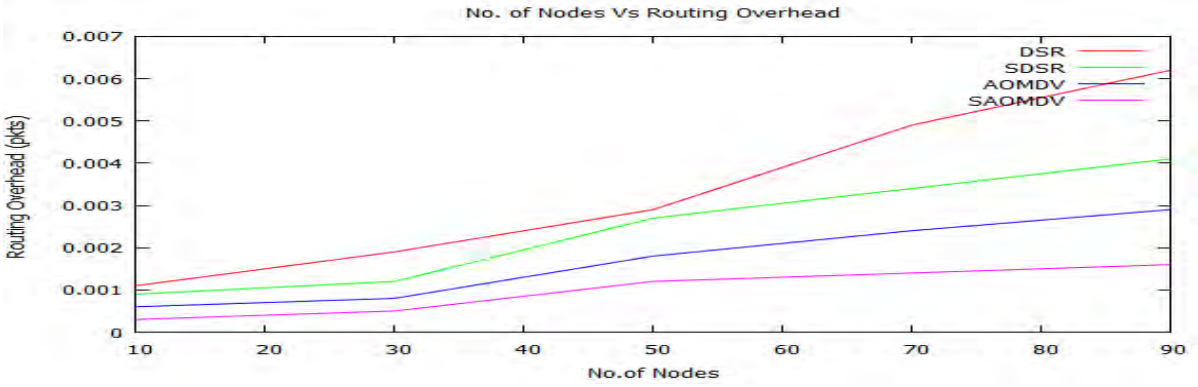

Figure4: Routing Overhead

Figure 4 illustrates the comparison of the Routing Overhead with reference to the number of nodes. SAOMDV has minimum overhead when comparing with other routing protocols. SAOMDV uses the alternath path which is already stored in the routing table. It does not move to the Route Discovery process ,when the currently used route is affected by the Black Hole node. Where else the DSR based protocols initialize the Route Discovery process each time to find the new route when the currently used route is affected by the Black hole node.

Figure5 shows the comparison analysis of the protocols for Packet delivery ratio with reference to the variation in the speed of the data transmission. SAOMDV has provided the high packet delivery ratio because the data packets are transferred through the secured route.

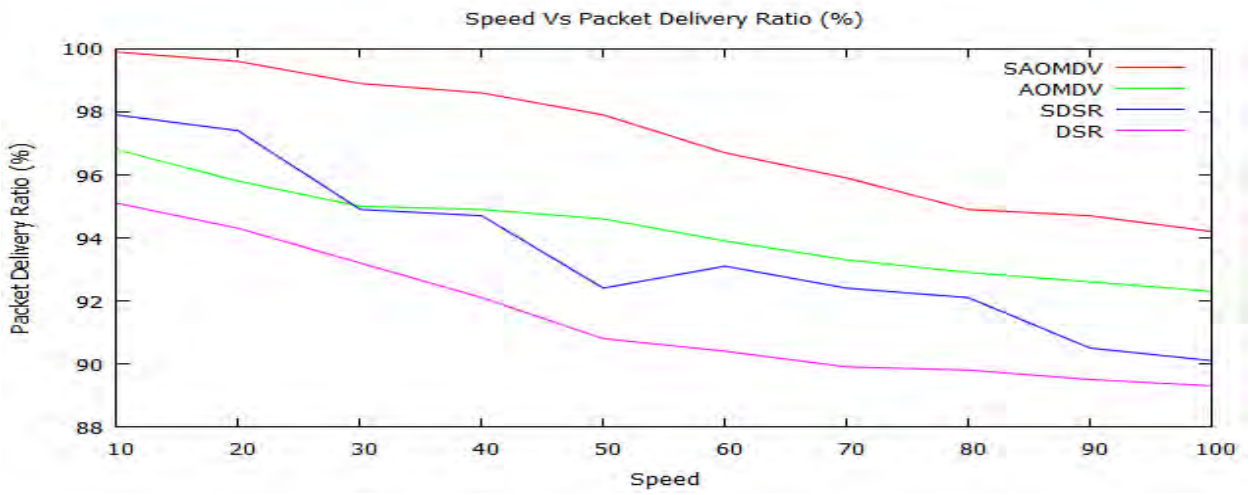

Figure 5: Packet Delivery Ratio Vs Speed.

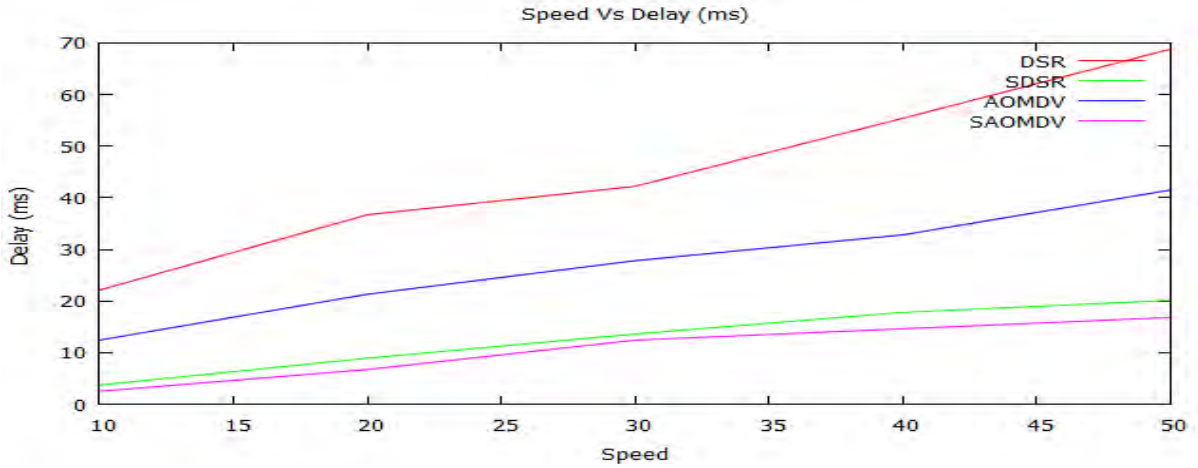

Figure 6: Average End to End Delay.

Figure 6 shows the comparison of the Average End to End Delay of the Various protocols like SAOMDV,AOMDV,DSR and SDSR. The average End to End Delay varies with reference to the variation in the speed of data transmission. Obviously the SAOMDV protocol, which is our proposed protocol, has less end to end delay when compared with the other protocols because of more authentication

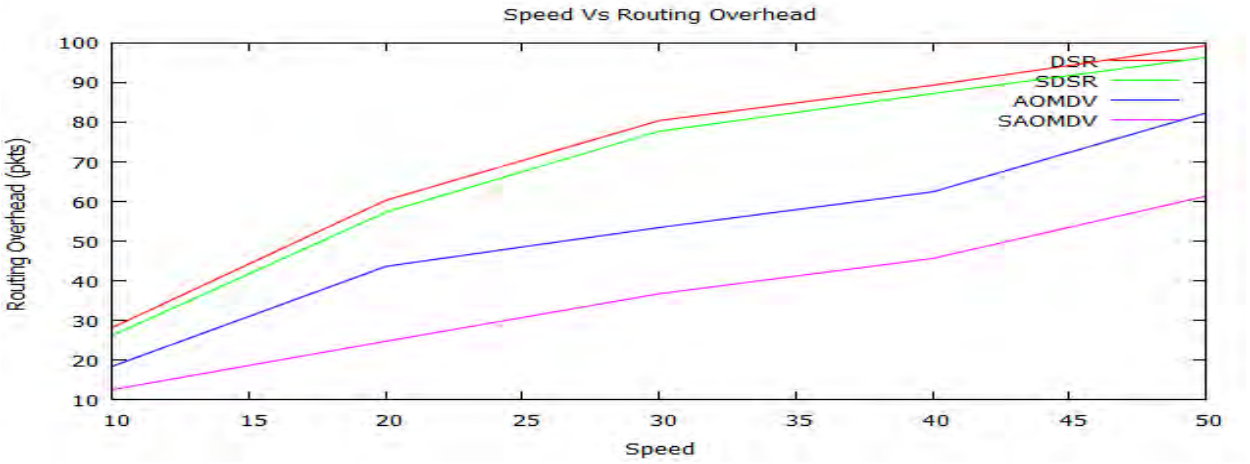

Figure 7: Routing Overhead Vs speed

Figure7 shows the comparison of the Routing Overhead with reference to the speed of nodes. SAOMDV has achieved the better performance with minimum overhead when comparing with other routing protocols.

V. CONCLUSION

The methodology described in the Paper is the modification applied to the initial work- Security enhanced Dynamic Source Routing Protocol. The proposed protocol overcomes some of the demerits in the previously designed protocol. The previous protocol suffered from the higher delay time and Higher routing overhead. The proposed protocol overcomes the drawback by using the AOMDV protocol. Here we have used the Digital security certificates for authenticating the nodes in the Selected Route. Data Transmission process is monitored by the neighboring nodes. Certificate is revoked when the nodes fail in authentication. Alternate route is selected, in case if any of the black hole node is detected. The proposed work is simulated and the simulation results shows that the proposed algorithm performs good with the better packet delivery ratio, less routing overhead and less end to end delay time, when comparing with the other protocols preferred for comparison.

REFERENCES

[1] K.Selvavinayaki, K.K.Shyam Shankar And Dr.E.Karthikeyan, "Security Enhanced Dsr Protocol To Prevent Black Hole Attacks In Manets", International Journal Of Computer Applications Vol 7– No.11, October 2010, Pp.15-19.

[2] E. A. Mary Anita and V. Vasudevan, Black Hole attack Prevention in multicast routing Protocols For MANETs Using Certificate Chaining, IJCA, Vol.1, No.12, pp. 22–29, 2010.

[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, JohnDixon, and Kendall Nygard, "Prevention of Cooperative BlackHole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN"03), Las Vegas,Nevada, USA.

[4] Tamilselvan, L. Sankaranarayanan, V. "Prevention of Black hole Attack in MANET", Journal of Networks, Vol.3, No.5, May 2008.

[5] Marti, S., Giuli, T. J., Lai, K., & Baker, M.(2000),Mitigating routing misbehavior in mobile ad-hoc networks, Proceedings of the6th International Conference on Mobile Computing and Networking (MobiCom), , pp. 255-265.

[6] D. Djenouri, L. Khelladi and N. Badache, A Survey of SecurityIssues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys & Tutorials, Vol. 7, No. 4, 2005.

[7] 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.

[8] Mahesh K. Marina Samir R. Das , On-demand Multipath Distance Vector Routingin Ad Hoc Networks- WIRELESS COMMUNICATIONS AND MOBILE COMPUTING Wirel. Commun. Mob. Comput. 2006; 6:969–988Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.432.

[9] Hesiri Weerasinghe and Huirong Fu, Member of IEEE, Preventing Cooperative Black Hole Attacks in Mobile Adhoc Networks: Simulation Implemention and Evaluation,IJSEA,Vol2,No.3,July 2008.

[10] Yu, K.M, Yu, C.W, Yan, S.F. 2009. An Ad Hoc Routing Protocol with Multiple Backup Routes. In Proc. Springer Science+Business Media LLC. 1 November 2009

[11] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L(2011) Developing a BDSR Scheme to Avoid BlackHole Attack Based on Proactive and Reactive Architecture in MANETs.

[12] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys", IEEE transactions on dependable and secure computing, vol. 3, no. 4,october-december 2006

[13] NS2 tutorial, www.isi.edu/nsnam/ns/tutorial.

[14] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M.Belding-Royer, "Authenticated Routing for Ad-Hoc networks", IEEE Journal on selected areas in communications, Vol.23, No. 3, March 2005.

[15] Yih-Chun HU, Adrian Perrig, "A survey of secure wireless ad hoc routing" In IEEE Security & Privacy,2004.

[16] Nikola Milanovic, Miroslaw Malek, Anthony Davidson, Veljko Milutinovic, "Routing and Security in Mobile Ad-hoc network", IEEE Computer Society,Feb. 2004.

[17] Loay Abusalah, Ashfaq Khokhar, Mohsen Guizani, "A survey of secure Mobile Ad hoc routing Protocol"IEEE Communication Survey & Tutorials, Vol 10,No.4, 2008.

[18] Eduardo da silva, Aldri l. dos Santos, and Luiz Carlos p. albini, "ID-Based Key Management in Mobile Adhoc Networks: Techniques and Application", IEEE wireless communication, pp 46-52, October 2008.

[19] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems," Proc. CRYPTO '89, pp. 307-315,Aug. 1989.

[20] W. Liu and Y. Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," Proc.IEEE INFOCOM 2004.