ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 5, MAY 2015, PP 337-341

Prevention of Black Hole Attack in MANET

[1]C.Mohammed Gulzar, Associate Professor, Dept. of CSE, Dr.KVSRIT, Kurnool

[2]Dr.Ragini Kashyap, Faculty, Dept. of Computer Science, MJPRU, Bareily, Uttar Pradesh, India

,

Abstract-The reliability in the transmission of data among the nodes will always degrade with the dynamic nature of Manet. Due to lack of security the manet is not protected against the attacks. Black Hole attack is the most common attack experienced by the Manet. To prevent the black hole attack, this paper addresses the security oriented solution to authenticate the routes selected during the route discovery process using the digital certificates. During the route discovery itself the digital certificate authentication avoids the black hole node. This methodology is implemented on AOMDV protocol.

Index Terms— MANET, BlackHoleAttack, Digital Certificates, Hash function, AOMDV.

1 INTRODUCTION

Mobile Ad Hoc Networks are autonomous and decentralized wireless system. MANETs consist of nodes that are free moving in and out in the network. Through the fixed structures mobile nodes in the adhoc network do not communicate. When providing information to the nodes or when requesting information from the nodes in the network, each mobile node acts as a host. When detecting and maintaining routes for other nodes in the network the mobile nodes are self organized which will perform as the router. 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 dispersed .This features degrades the reliability in secured data transmission and makes the network to endure from various routing attacks. [5]

The attacks can be classified into active attack and passive attack. It can be further classified into internal attack & external attack. An active attack disrupts the regular operation of the network by modifying the packets in the network. Passive attack is one where the information alone is snooped by the intruder without distressing the network. The Internal attacks are from compromised nodes that were the part of the network. External attacks are from the nodes which are not the part of the network.

A. 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]

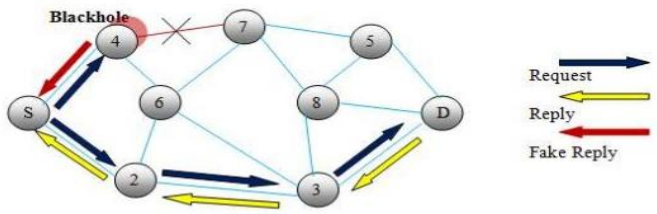

Figure 1: Black Hole Attack

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 reply to source node at once. The destination node may also give a reply. If the reply from a usual destination node arrives at 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 closer to the source node. Moreover, node C does not have to to check its RT when sending a fake message; its response is more probable to reach the source node initially. This makes the source node to consider that the routing discovery process is completed and queues all other reply messages in the routing table, and start to send data packets. The phony route has been created. As a result, all the packets through node C are simply consumed or vanished. Node C could be said to form a black hole in the network, and that has been named with black hole attack.

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

The objective behind the design of AOMDV is to provide efficient fault tolerance in the sagacity of faster and efficient recovery from route failures. The important 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 finding technique in the DSR protocol. [17]

During the route discovery process, AOMDV computes the multiple loop free paths. With the ease of use of the multiple paths, when the preceding route fails, the protocol switches from one route to next likely finest route. The new route discovery process is initiated only when all the paths to a precise destination fails.

The loop free link disjoint paths and multipath routing are very effective there by reduces routing overheads and supports enhanced load balancing. A change to the alternate routes will evade the node blocking. The multipath routing prevents the routing overhead. AOMDV allows the multiple paths for the similar destination sequence numbers. The multiple paths are formed via the neighbours during which the RREQ or RREP are recognized from that neighbour. The alternate route selection due to the route failure while completely eliminates the route detection latency. [8]

The paper is organized as follows. The Proposed solution is described in Chapter 2. The Chapter 2 describes the proposed solution in three phases. The first phase explains the digital certification process and elaborates the route discovery process. The second phase describes the Authentication Phase. And the last phase explains the Black hole detection process.

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

2. PROPOSED SOLUTION

A. Digital security certificates

The Digital certificate is the security certificate which is self organized PKI infrastructure and Public key is validated by the chain of nodes. Authentication is specified 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. By creating and issuing the certificates to the neighbours, every node in the network should be able to verify the other nodes in the network. The node also maintains the received certificates from the other neighbours. Based on security conviction value the certificates are issued. For the certificates from the neighbours the nodes make a periodical request. The certificates are validated for the public key. The corresponding node is assumed to be malicious node if it is found that there are two different nodes having the same Public key or two different key assigned for the same 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 tries to validate its neighbours. The nodes request the IP address of its neighbour and pertain the hash function and generates the Public key.[19]

$$HMAC\ {}_{P}K(M) = H((K + SPAD)||\ H\ ((K + EPAD)||\ M))$$

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. Intruders cannot attack the secured public key provided by HMAC. 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. The issue node checks whether the TV value is viable before a Certificate is generated. If viable, 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 instantly process the RREQ by sending the RREP directly without verifying the Route table for the accessibility of the node. When the source node receives the RREP prior to the expected time, it suspects the RREP originator as the malicious node. If the source node suspects a node to be malicious node it eliminates the node from that route and opt for another route.

Between the neighbouring nodes, the Certificates are exchanged periodically.[13]

$$DC(S \rightarrow A)\ DC(S \rightarrow B)\ DC\ (D \rightarrow A)\ .$$

Initially the TV value is set to the threshold value. If the security of the node is found to be undermine the TV values keeps reducing and once if it arrives at zero then node is marked as the malicious node. Threshold value is the time reliant trust value. Initially node s have the trust value on intermediate node B is at time T1.[19]

If the security of the node is found to be imperil, the TV values keeps falling and once if it reach zero then node is marked as the malicious node. Let ${}_{A}{}^{T}B$ (t1) be the trust value of node A to node B at time t1 and ${}_{A}{}^{T}B$ (t2) be the decayed value of the same at time t2. Then trust value can be defined as follows,

$${}_{A}TV_{B}(t_2) = {}_{A}T_{B}(t_1) * e^{-({}_{A}{}^{T}{}_{B}{}^{(n)}\Delta t)2k}$$

The algorithm can be classified into three phase.

1) Route Discovery Process
2) Authentication Process
3) Black Hole Detection Process.

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

1).Route Discovery Process: When a source node S needs to locate 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 earlier 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 target node or any other node that has a suitable 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 respond 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 depending on the shortest communication cost.

2). Authentication Process: The selected route is not used instantly for the data transmission to avoid the black hole nodes from packets being dropped. 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 valid reply from the destination node. The destination node sends the valid messages appended with the digital security certificate that is issued by the neighbouring node in the network. The validated 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 arrives at 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 authenticated 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 transitional nodes in the route until the RREP arrives at the SourceNode. When the RREP arrives at the S, S node checks the whole certificate group. If there is no issues in the certificate, Node S hope 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 similar node having distinct certificates then the corresponding node is marked as the nasty 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 earlier route. The succeeding procedure elaborates route discovery process and the alternate path selection process for the tenable 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(source_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; \\ Not to give Security Certificate.
21. Verify the route cache for different route.
22. }
23. ELSE
24. {
25. Route is established between SN and DN}
26. STORE the Alternate Routes
27. Nodes that come across the route certify each other:
28. {
29. Request id and security parameters of NHN
30. Produce public key of NHN based on ID
31. Issue Certificates encrypted with public key
32. Save certificates in route cache
33. Exchange Certificates with neighbor nodes
34. }
35. DN forwards certified RREP affixed 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 affix 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 elimination process. The source node implements this algorithm to select the alternate route when the route elected 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

3. PERFORMANCE EVALUATION

The methodology is implemented on AOMDV protocol. The performance outcome is compared with the other algorithms like DSR, AOMDV and formerly 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.

A. Performance metrics:

The performance of the algorithm is mainly computed 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 existing 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 needed to receive data. In the ideal scenario the ratio should be equal to 1. If the ratio falls drastically below the ideal ratio, then it could be a sign of some faults in the protocol design. However, if the ratio is higher than the ideal ratio, then it is an sign that the node receives a data packet more than once. It is not desirable because reception of duplicate packets consumes the network's precious resources. The virtual number of duplicates received by the node is also important because based on that number the node can perhaps take a suitable action to decrease the redundancy.

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

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

4. CONCLUSION

The methodology described in the Paper is the modification applied to the initial work - Security enhanced Dynamic Source Routing Protocol. The proposed protocol can rectify some of the drawbacks in the formerly designed protocol. The earlier protocol suffered from the higher delay time and higher routing overhead. The proposed protocol can rectify the shortcoming by using the AOMDV protocol. Here we have used the Digital security certificates for validating the nodes in the selected route. Neighboring nodes scrutinize the data transmission process. When the nodes fail in authentication, Certificate is revoked. In case if any of the black hole node is detected, alternate route is selected. The proposed work 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 preferred protocols.

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] 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.

[3] 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.

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

[5] 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.

[6] 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.

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

[13] 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
[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] W. Liu and Y. Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," Proc.IEEE INFOCOM 2004.
[20] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems," Proc. CRYPTO '89, pp. 307-315,Aug. 1989.