ISSN 2047-3338

A Reliable Data Transmission Approach to Prevent Black Hole Attack in MANET

K. Selvavinayaki[1] and Dr. E. Karthikeyan[2]
[1]Bharathiar University, Coimbatore, India
[2]Department of Computer Science, Govt. Arts College, Udumalpet, India

***Abstract*– The dynamic nature of infrastructure in MANET makes security as a critical issue. The security of the network can be improved by preventing the black hole attack in MANET by enhancing the data confidentiality and reliability. One of the way to achieve this is to protect the messages from being compromised when they are delivered over the insecure network. This paper focuses on protecting the data from compromised nodes by dividing the data in to multiple shares. Each message is encoded by a public key and then transferred over multiple paths. Destination receiving the multiple shares will integrate into original message. The optimal option of multiple path routing protocol is MAOMDV where the secret sharing schemes and message shares can be optimally allocated on each path to provide maximum security. The Algorithm is implemented on NS-2 simulator. The results show that algorithm implemented on MAOMDV is more secure and provide high degree of reliability.**

***Index Terms*– Black Hole Attack, MAOMDV, Secret Sharing and Scheme & Reliability**

I. INTRODUCTION

A mobile Ad-Hoc network is a self configurable, self organizing and infrastructure less multihop mobile wireless network. Security in MANET is a complex issue. This is because of insecure wireless communication link, absence of fixed infrastructure, node mobility, dynamic topology and bandwidth limitation. The main role of routing protocol is to establish an efficient, optimal and secure route between the nodes. Any kind of attack in MANET will disturb the entire communication and the total network can be collapsed. The security issues in MANET become tedious with multiple numbers of nodes. Any node can be a sender or a receiver. There are many attacks by the compromised nodes that collapse the network and make it unreliable for communication.

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 normal 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 disturbing 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

Black Hole attack is a passive attack where the malicious node advertises itself as having the shortest path to the destination in the network and then absorbs all the data without forwarding to the destination. A black hole can be formed either by a single node or by several nodes in collusion. In case of a single node attack, the node drops the entire packet instead of forwarding to destination whereas in case of multi-node collusion attack, black hole node will forward the packet to another black hole node.

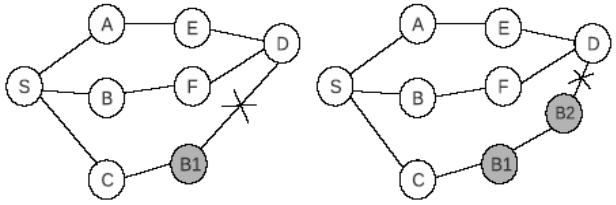

Fig. 1: Black Hole Attack

In Fig. 1 we illustrate the progress of a blackhole attack, wherein the source node S is intend to establish a route to destination node D, by broadcasting route request (RREQ) packet. However, when blackhole node B1 receives a RREQ, it immediately sends a RREP which is having larger sequence number and smaller hop count. On receipt of a RREP from B1, the source starts transmitting the data packets, which B1 simply drops instead of forwarding to the destination. B1 forwards all the data to B2 and B2 drops them instead of forwarding to the destination.

B. MAOMDV Protocol

The Routing protocol can be classified into proactive & reactive protocols. Hybrid protocols are the combination of proactive and reactive protocol. Proactive protocols are table driven .DSDV is this type of protocol. Reactive protocols are on demand routing protocols. DSR, AODV, AOMDV, MAOMDV are of this kind.

Multipath routing is called traffic dispersion. The idea is to spread the traffic from the source in space rather than in time for load balancing and fault handling. Modified Ad-hoc On-demand Multipath Distance Vector Routing (MAOMDV) protocol is an extension to the AOMDV protocol for computing multiple loop-free and link disjoint paths. The routing entries for each destination contain a list of the next-hops along with the corresponding hop counts. All the next hops have the same sequence number. This helps in keeping track of a route. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all the paths, which is used for sending route advertisements of the destination. Each duplicate route advertisement received by a node defines an alternate path to the destination. Loop freedom is assured for a node by accepting alternate paths to destination if it has a less hop count than the advertised hop count for that destination. Because the maximum hop count is used, the advertised hop count therefore does not change for the same sequence number. When a route advertisement is received for a destination with a greater sequence number, the next-hop list and the advertised hop count are reinitialized.

MAOMDV can be used to find node-disjoint or link-disjoint routes. To find node-disjoint routes, each node does not immediately reject duplicate RREQs. Each RREQs arriving via a different neighbor of the source defines a node-disjoint path. This is because nodes cannot broadcast duplicate RREQs, so any two RREQs arriving at an intermediate node via a different neighbor of the source could not have traversed the same node. In an attempt to get multiple link-disjoint routes, the destination replies to duplicate RREQs, the destination only replies to RREQs arriving via unique neighbors. After the first hop, the RREPs follow the reverse paths, which are node disjoint and thus link-disjoint. The trajectories of each RREP may intersect at an intermediate node, but each takes a different reverse path to the source to ensure link disjointness. The advantage of using MAOMDV is that it allows intermediate nodes to reply to RREQs, while still selecting disjoint paths. But, MAOMDV has more message overheads during route discovery due to increased flooding and since it is a multipath routing protocol, the destination replies to the multiple RREQs those results are in longer overhead.

C. Secret Sharing Scheme

A secret sharing scheme consists of two algorithms. The dealer generates and distributes shares among the participants. The combiner collects the shares from the participants and recomputes the secret if the number of correct shares is less than T. Secret sharing scheme is used in secret key management. Assume we have a system secret K and we divide it into N pieces $s_1,s_2,\ldots s_n$ called shares. Each of N participants of the system, $,_{P1,P2,\ldots,Pn}$ hold one share of the secret respectively. Any less than T participants cannot learn anything about the system secret, while with an effective algorithm ,any T out of N participant can reconstruct the system secret K. This is called a (T,N) threshold secret sharing scheme. Shamir's secret sharing scheme is algebraic and is based on polynomial interpolation.

Assume K is the secret to be shared among N particiapants $P_1,P_2\ldots,P_n$. The dealer obtains the i^{th} participant P_i's share S_i by evaluating a polynomial of degree (T-1):

$$f(x) = (K + a_i x + \cdots\cdots + a_{T-1}x^{T-1}) mod\ P$$

$$At\ x = i_{[j=1,2,\ldots N]} Pi \rightarrow s_i = f(i) \qquad (1)$$

$a_1,a_2\ldots a_n$ are randomly chosen coefficients, p is randomly chosen prime number which is greater than any of the coefficients and must be available to both dealers and combiners. At the combiner with the knowledge of minimum number of T shares $f(i_1),f(i_2)\ldots F(i_r)$, the original polynomial f(x) can be recovered by Lagrange interpolation.

$$f(x) = \sum_{j=1}^{T} Si_j - li_j(x) mod\ p$$

$$where\ li_j(x) = \prod_{k=1,k=j}^{T} \frac{x - ik}{ij - i_k} \qquad (2)$$

It is computationally easy using Lagrange interpolation to determine the polynomial and to recover the secret.

II. RELATED WORK

Many researchers have addressed the black hole attack problem in MANET. All the solutions proposed and implemented were based on AODV and DSDV protocol.

Marti, S., Giuli, T. J., Lai,K., & Baker, M. [4] have proposed a Watchdog and Path rater approach against black hole attack which is implemented on top of source routing protocol such as DSR (Dynamic Source Routing).

CONFIDANT (Cooperative of Nodes, Fairness In DynamicAd-hoc Networks) is an extended version of Watchdog andPath rater which uses a mechanism similar to Pretty Good Privacy for expressing various levels of trust, keyValidation and certification. It is also implemented on unicast routing protocol such as DSR.

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. Nodes authenticate each other by issuing certificates to neighboring nodes and generating public key without the need of any online centralized authority.

Sanjay Ramaswamy et al. [6] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets.

LathaTamilselvan et al. [8] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is given to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the

solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0" value is considered as malicious node and is eliminated.

Hesiri Weerasinghe [3] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by S. Ramaswamy to improve the accuracy.

WENJING LOU [10] presented a solution for reliable data delivery using shamirs secret sharing scheme to protect data against Dos in wired networks.

III. THE PROPOSED SOLUTION

The fundamental idea is to enhance the security by distributing the secret in the network. When a source node wants to send a message to a destination then depending on the required message security level and the availability of the multiple paths the source determines a threshold secret sharing scheme to divide the message into multiple blocks and route them to the destination through the selected multiple paths . The destination upon receiving the certain number of correct shares recovers the original secure message.

System process is divided into four:

1. Secret Share Generation
2. Black hole node detection, prevention & removal
3. Share Allocation
4. Routing the message on optimal multiple path

A. Secret Share Generation

When a source node sends data to a destination node, the dealer process is implemented at source node and combiner process is implemented at destination.

In this system we are using shamir's secret sharing scheme to save the network bandwidth. This scheme is improved by assigning secrets to all coefficients $a_0(k),a_1,a_2\ldots\ldots a_{T-1}$. If the message is large it can be divided into blocks .All the message pieces are scrambled. Select the prime number based on limited size and the secret sharing is applied on every message blocks on block by block basis. This is similar to any block cipher used to encrypt a large message. A group of T blocks which corresponds to T secrets $a_0,a_1,a_2\ldots\ldots a_{T-1}$ are sent to the T inputs of the dealer process at one time. The output of the dealer process is a group of N blocks where i^{th} output corresponds to the value of f(i). Each block forms a single IP packet .Indentifying indices are added to the packets to get identified at the receiver end. A buffer at the destination node will store the received packets. Re-sequencing of the packets is done. For each group of received blocks the combiner reconstructs the original block by Lagrange interpolation. The reconstruction always requires that the combiner should have at least T different shares. It fails if the number of shares is less than T. The reconstructed block will be concatenated and passed to next layer.

B. Black Hole Node Detection, Prevention & Removal

As in Fig 1, assume the node B1 as the black hole node. Even when B1 compromises a share, it has to compromise at least T shares, with less than T shares, B1 cannot know about the message. The Secret share generation scheme is designed in such a way that if some of the shares are compromised, the remaining shares can be modified in a way that the compromised shares cannot be used. Black hole nodes can be prevented by embedding black hole node detection and identification mechanism.

At the source, Choose the one –way hash function and prime number q such that h() <q.

Compute,

$$T = \sum_{i=1}^{N} h(si)p^{2(i-1)} + \sum_{i=1}^{N-1} cp^{2i-1} \quad (3)$$

Where c is a constant; Publish T&P.

At the destination, On receiving all the shares S_1, S_2, Sn, compute

$$T^* = \sum_{i=1}^{N} h(s_i^*)p^{2(i-1)}$$

For each s, check

$$\left\lfloor \frac{T - T^*}{p^{2(i-1)}} \right\rfloor (mod\ p) == 0 \quad (4)$$

If it is zero, then the Si* is valid share .otherwise it is a fake share. This method detects and identifies the black hole node. This can be inferred that one or more black hole nodes along the path can be identified.

Once if the black hole node is identified, then the MAOMDV protocol at the network layer will back tracks all the blocks on the path send to that node and select the next optimal path to reach the destination.

C. Share Allocation

Here we choose share allocation scheme with redundancy to achieve both data confidentiality and reliability. All the shares are transferred onto multiple paths, long paths are preferred. Reliability is achieved by sending more information than the minimum requirement, so that the original message can be reconstructed even in case of certain data loss. With the threshold secret sharing scheme, when T<N, redundancy is introduced. When we combine the redundancy with multipath routing the system becomes more error tolerant. The system will be error tolerant even if the black node compromises certain packets, it will not affect the share reconstruction. To achieve the maximum security the total number of shares allocated to any m-1 or less paths is always less than T.

D. Multi path Routing

At the network layer MAOMDV protocol will allocate the N message shares in one group onto different paths to the destination according to the share allocation scheme. To maximize the security path assignment is scrambled. MAOMDV protocol is capable of maintaining multiple paths from source to destination. Here we need independent and disjoint paths. The protocol will broadcast the RREQ message throughout the network and then gathers the RREP messages from the destination. Path selection is not made directly. It is based on the hop count. Source nodes store all the route information in the route cache, to prevent the route discovery process for already available route. Here all the routes at the source are decomposed into single routes. This helps to form an optimal route set. When a black hole node is detected, MAOMDV protocol will perform alternate path routing. The alternate path is selected form the optimal route set.

The Following algorithm explains the entire process:

Step1: Divide the original message in to multiple blocks.

Step 2: For each block assign the secret to all the shares to encrypt the message block. Add Indices to all the blocks.

Step3: Allocate the N message shares in one group onto different paths to the destination according to the share allocation scheme.

Step 4: If a black hole node is identified, stop sending the blocks on the specified route. Back track the data and select alternate path to the destination.

Step 5: At the destination, Re-sequencing of the packets are done. For each group of received blocks the combiner reconstructs the original block by Lagrange interpolation. The reconstructed block will be concatenated and passed to next layer.

IV. PERFORMANCE ANALYSIS & EVALUATION

Here we have used NS2 simulator. The Source and Destination node can be selected randomly. The simulation parameters chosen for the experiment are only for illustration purpose. The Behavior of the nodes has been changed in to black hole node and they are deployed according to the mobility model. Basic configuration of the simulation environment is as follows:

Table 1: Simulation Environment

Area	1000x1000m.sq
No of Nodes	50 nodes
Traffic Source	CBR
Packet Size	1460B
Sending Rate	1 Mbps
Mobility Model	Random Way Point
Simulation Time	21ms

A. Performance Evaluation

The Performance is evaluated based on the following metrics.

1. Packet Delivery Ratio.
2. Packet Loss Ratio.
3. Average Throughput.
4. Average Hop Count.
5. Average End-to End Delay.
6. Normalized Routing Overhead.

Fig. 2 Illustrates the Packet Delivery Ratio of the data transmission with 43 nodes. The PDR varies from 97% to 99.7% for the variation of node mobility. Most of the packets are delivered even in the presence of Black hole node.

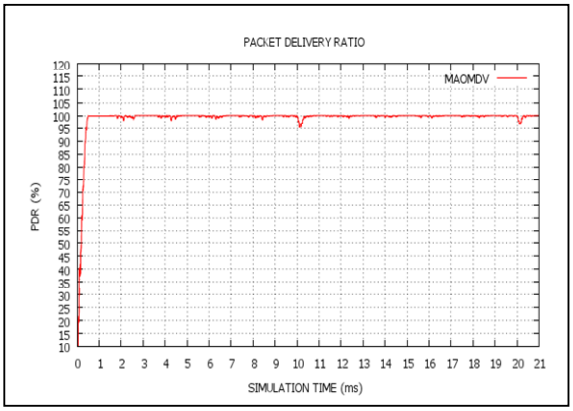

Fig. 2: Packet Delivery Ratio

Fig. 3 shows the Average Hop count level. The Hop count value varies from 0 to 2 hops based on the no of data packets transmitted

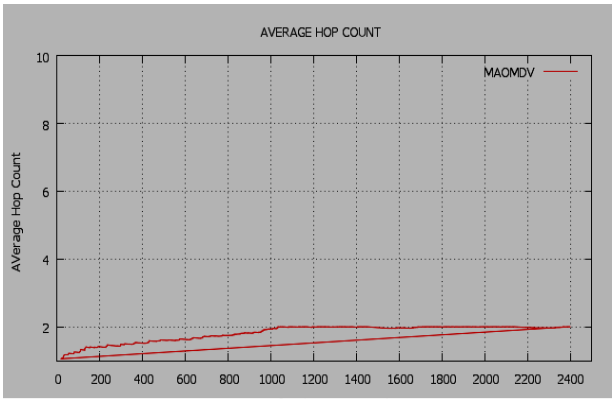

Fig. 3: Average Hop count

Fig. 4 shows the packet loss ratio in the presence of the Black hole node. The Packet loss ratio varies from 0.1 to 0.3 % for the variation of the data packets transmitted.

Fig. 5 depicts the Average Throughput of the network with 43 nodes, 15 sender nodes. The throughput remains from with the variation of 92 to 100% based on the no of data packets

transmitted. Fig. 6 illustrates the average end to end delay based on the run time .The delay time varies from 0 to 20 % for the network with 15 senders. Fig. 7 illustrates the routing overhead for the network scenario. The Routing overhead seems to be more due to the route discovery process for selecting alternative path which is tolerable.

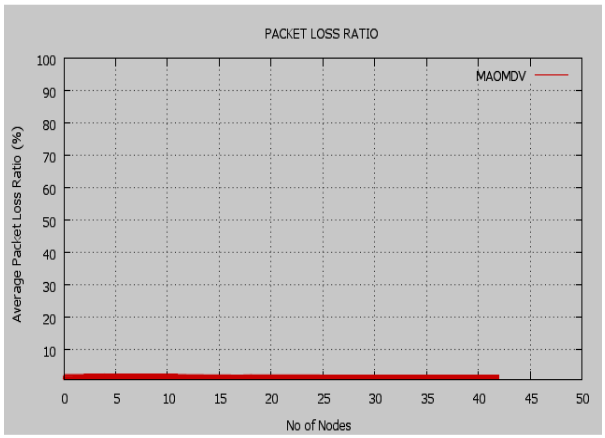

Fig. 4: Packet Loss Ratio

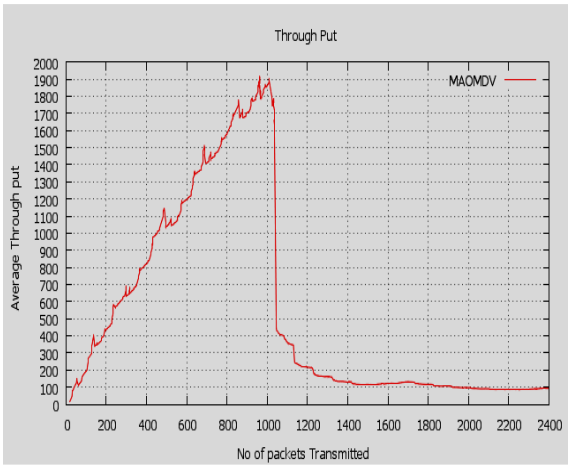

Fig. 5: Average Throughput

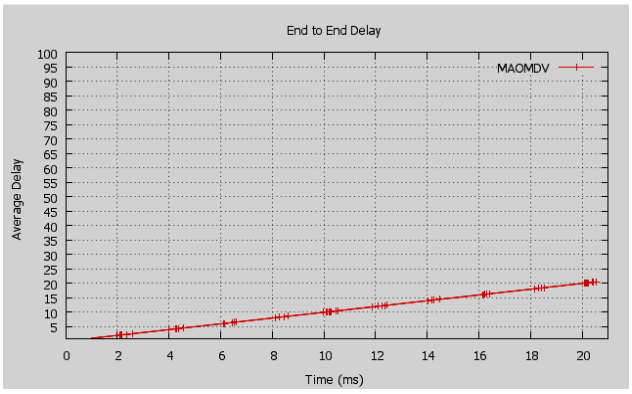

Fig. 6: Average End- to-End Delay

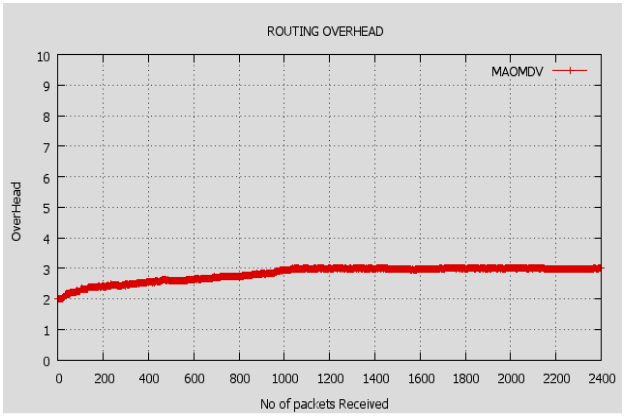

Fig. 7: Routing Overhead

V. CONCLUSION

The Simulation results shows that MAOMDV protocol with secret sharing scheme performs better in detecting and preventing the Black hole nodes in MANET. Packet loss is very much reduced, proving the reliable data delivery. The results shows that message overheads during route discovery due to increased flooding is also tolerable one because the protocol searches for alternate paths if the current route breaks by flooding the network with RREQ packets instead of dropping all the packets.

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, 2005.

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

[4] 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.

[5] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

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

[7] Sukla Banerjee, Dectection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-hoc Networks. Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008,San Francisco, USA373-377-

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

[9] 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.

[10] Wenjing lou. "Secure protocol for reliable data delivery", 2003.