Implementing Security algorithm to worm hole attack using AOMDV protocol & comparison using NS2 simulator

Richa Gulati[1], Savita Shivani[2]
[1]*M.Tech Research Scholar, Suresh Gyan Vihar University,Rajasthan,India*
[2]*Associate Professor,IT Dept.,Suresh Gyan Vihar University,Rajasthan,India*

Abstract: *In present era, where every person has become addicted to wireless networks, MANET'S has fulfilled the demand of the people by removing the dependency of fixed network. Mobile ad-hoc networks have extended the range of mobile nodes beyond their level. Now when we talk about wireless communication, routing is the backbone of any communication. Ad hoc on demand multipath distance vector routing algorithm (AOMDV) is a very reactive protocol in MANET's. We have selected AOMDV algorithm for routing purpose as there have already been done several work with AODV. Also, in AOMDV the end to end delay is reduced by utilising several parallel paths. Various routing attacks have been identified in single path routing but here we have introduced worm hole attack in multi path routing i.e. AOMDV routing algorithm. In this paper, we have studied the performance of AOMDV algorithm under worm hole attack. Also, we have provided security and authentication to each and every node by the use of public key and private key. Different metrics of the proposed protocol has been evaluated from simulation on NS2 on different scenarios i.e. with worm hole attack and without worm hole attack and there has been a noticeable improvement in the throughput and energy consumption is also reduced.*

Keywords: *AODV; AOMDV; Worm hole attack; black hole attack; security; authentication; protecting.*

I. Introduction

Mobile ad hoc network is a collection of wireless mobile nodes thus have multiple wireless communication devices that dynamically self configure and self organize and have distributed, mobile and multi hop network. In MANETs, nodes within each other wireless transmission ranges can communicate directly; however nodes outside each other's range have to rely on some other nodes to transfer messages. Due to this fact, we need a routing algorithm to route the packets from source to destination. As the router will find the optimum path and manage the data delivery with the help of routing protocol scheme. There are various types of routing protocol for various types of network. Here, we have used Ad-hoc on demand multipath distance vector (AOMDV) routing algorithm.

AOMDV is a reactive protocol to most researchers because of its ability to adapt effectively in dynamic network environment like MANET [2,3]. In AOMDV, the end to end delay is reduced by utilising several parallel paths. This algorithm tries to use large number of loop free and disjoint paths as possible to increase the reliability from one node and reduce shared resources, increase bandwidth and reduce latency from another node. Also, AOMDV algorithm performs better as it prefers to use node-disjoint paths. In node disjoint ad loop free paths, there is no node between two joint paths, which makes paths completely independent and they don't have any shared resources. But in present scenario, even the best ad hoc routing protocols do not have fullproof security mechanisms against threats and worm hole is one of such threat against the AOMDV routing protocol.

A wormhole attack is one of the severe attack on MANET routing where attacker record the wireless data he overhear, forward it to other, and replay the packets at the other end of the network. Once the wormhole attacker has control of a link he can drop the packets to be forwarded by the link. Basically, all packets are dropped, a random portion of packets, or specifically targeted packets are dropped. Attacker can also send packets out of order or on and off 'switch' of its link. By disturbing the routing of packets worm hole corrupt the whole path and hamper the transfer of data from source to destination. [3,4]

We have secured the worm hole attack by protecting it with the concept of pre shared keys. The benefit of pre shared key is that it will not only provide security to routing path but also authenticate each and every node. Pre shared keys includes the distribution of public key to each node inside the cluster and private key to cluster head.

II. Related Research

Many routing algorithms have been tested and proposed with different criterions like strong and feasible node security and authentication with lightweight cryptography. Many of them have applied cryptographic techniques to prevent worm hole from unauthorized access. The one of the worm hole prevention technique by Hu at el [1,5] is 'packet leashes'. He described two types of leashes – geographical leashes and temporal leashes. Geographical leashes should work fine when GPS systems are practical. But later, we identified that GPS systems are not flexible, as Global positioning system do not function well inside buildings, under water, in the presence of strong magnetic radiation, etc. Whereas in comparison to geographical leashes, temporal leashes needs much tighter clock synchronization, but do not depend on GPS information. This approach completely ignores the message processing time. [7]

Many of the researchers worked on the wormhole attack problem by taking a wormhole as a disorderly node. In such type of approach, a wormhole attack is not specifically identified. Baruch and Chigan [9] use node rating schemes to prevent wormhole attacks. This approach focuses towards locating and preventing only one kind of wormhole behavior that is packet loss.

Unauthorized nodes are the main problem with the wormholes which transmit valid network messages. In certain cases, technical solutions based on nodes performance may be suitable, but they do not identify the wormhole problem completely.

III. Proposed Methodology

Our main objective is to secure the worm hole attack by providing authentication criterion using concept of pre shared keys that is using public and private key. We have taken following assumptions regarding the organization of MANTE which consist of cluster of nodes:

1.1 Assumptions

The following assumptions are taken in order to design the proposed system algorithm:

i. The entire network is divided into two clusters, each having its individual cluster head.
ii. Every node has assigned a unique id numbered from 0-24 in cluster 1 and 25-49 in cluster-2.
iii. Two types of communication will take place: intra cluster i.e. internal communication and inter cluster i.e. external communication.
iv. A cluster head of cluster-1 is represented by 12 and that of cluster-2 by 37.

1.2 Cluster Formation

In this paper, we have used AOMDV routing protocol as the underlying network topology. In the proposed algorithm, worm hole attack has been introduced in a cluster after that security algorithm is defined to prevent the cluster from worm hole. The network is divided into two clusters, each having its own cluster head. Every node has assigned a unique id numbered from 0-24 in cluster 1 and 25-49 in cluster-2. Two types of communication will take place: intra cluster i.e. internal communication and inter cluster i.e. external communication. A cluster head of cluster-1 is represented by 12 and that of cluster-2 by 37. Internal communication occurs when source node shares information only to its cluster head and cluster head forwards the information to its destination node. External communication occurs when cluster head of cluster-1 communicates with cluster head of cluster-2.

3.3 Introducing Worm Hole To Cluster Head

The main purpose of our paper is to provide security to worm hole attack node for which firstly we have introduced worm hole on node 37 i.e. cluster head of cluster-2 during external communication. We have set 90 sec time limit for simulation on NS2. At 2 sec data communication will start within cluster which will end at 35 sec. (shown in figure 1).

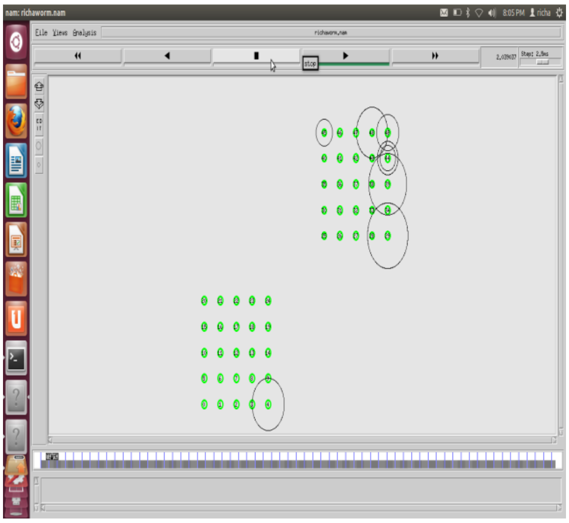

Figure 1. Simulation environment at 2 sec

After that all the cluster nodes will move from their positions and make tunnel shape through which cluster heads of both the clusters move towards each other and then at 50 sec external communication will start. Tunnel shape is introduced as worm hole make use of tunnel to transfer packets from one point in a network and replays it to the network from another point. We have introduced worm hole attack at 55_{th} sec at node 37. After 55_{th} sec communication will stop as worm hole attack has started and data packets will start dropping which is shown through NS2 simulator in figure-2.

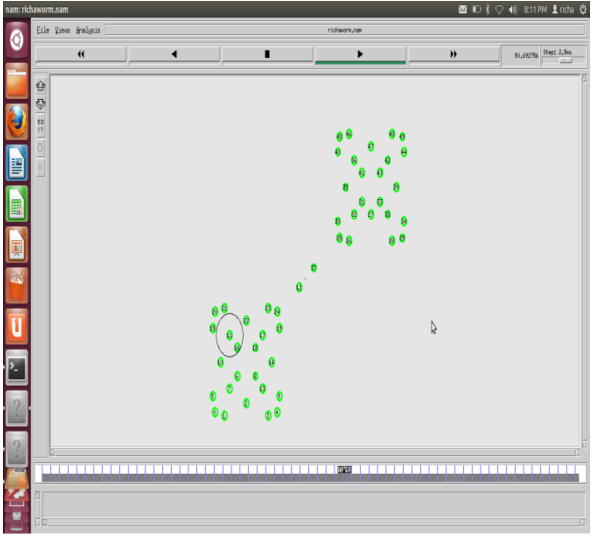

Figure 2. External Communication started at 50 sec and at 55 sec worm hole is introduced which results in packet loss

3.4 Implementing Security Algorithm To Worm Hole

Here we will present the security algorithm that provides authentication and protection to each and every node such that no worm hole can further attack to the routing nodes. Our work is based over Pre-shared key distribution that is using public and private key. The concept of pre-shared key distribution is used in which two nodes can only communicate when their key matches with each other's key and will behave as an isolator. Hence, there is no prior knowledge of keys to any of the node. They have information only about their own key. So, here we have introduced zero knowledge algorithm. In zero knowledge algorithm, A (or prover) can prove to B (or verifier) that the given condition is true. No other information is exchanged among them and no knowledge is gained by prover. Hence, it is called zero knowledge algorithm. After proving the condition true by A (or prover), B (or verifier) would gain the additional information that the prover has knowledge of the required secret information and after which communication can take place between them.

3.5 Procedure Of Working Of Zero Knowledge Algorithm

Begin
Step 1: We have generated a pair of public and private keys.
Step 2: Private Key (numbered 5) is assigned to cluster head of both the clusters i.e. node 12 and 37.
Step 3: Each Public key (numbered 1,2,3,4,5) are assigned to rest of the nodes of both the clusters.
Step 4: Before the communication starts between the nodes, keys are matched among them.
Step 5: In internal communication i.e. within the cluster, public key of one of the node (suppose 9) is matched with private key of the cluster head (suppose 12). If the key is matched, therefore, isolator value becomes true and further communication can take place. If key is not matched, the node is considered to be malicious and hence value of malicious becomes true and packets starts dropping.
Step 6: In external communication i.e. among two clusters, private key of one cluster head (12) is matched with private key of another cluster head (37). Again the similar concept as above is applied here.
End

In our simulation environment, in case of worm hole attack, at 55^{th} sec we introduced a worm hole. Here, in isolator case, at same time i.e. at 55^{th} sec isolator is implemented which shows we have protected the node against worm hole by using the concept of Pre Shared key.

IV. Simulation Environment For Attack Analysis With Worm Hole And Without Worm Hole

The simulation study has been done in NS 2 simulator which is an event driven simulation tool to simulate wireless packet mode communication. It is an object oriented discrete event simulator for studying the dynamic nature of communication networks. It provides a comprehensive environment for designing network protocol, creating and visualizing the scenarios under specific condition and analyzing their performance. We have worked with 50 nodes in the network; simulation duration was 90 sec, rest parameters are listed below in table:

Table 1: Simulator Parameters

Parameter	Value
Simulator	NS2
Simulation Duration	90 sec
Topology	2500m X, 2500m Y
No. of Nodes	50
Max segment size	512 bytes
Traffic Type	FTP
Routing Protocol	AOMDV

4.1 Parameters Used For Comparison

1. Throughput: is the average rate of successful message delivery over a communication channel. The throughput is measured in kilo bits per second (kbps or kbit/s). Greater the value of throughput means better the performance of the protocol.

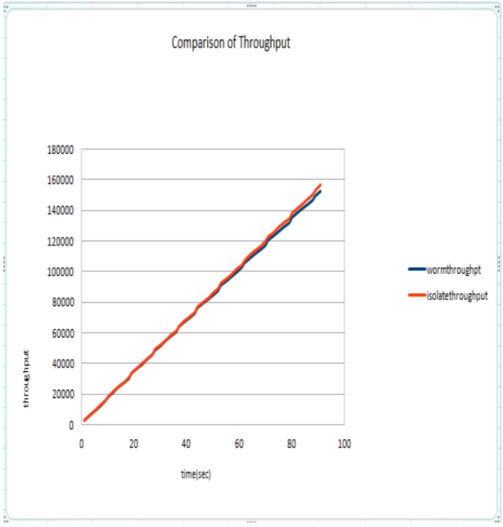

Figure 3. Comparison of Throughput with wormhole and with isolator

2. Energy Consumption: is the utilization of energy in the form of heat or electricity. The less the energy is utilized the more the better the performance of the protocol.

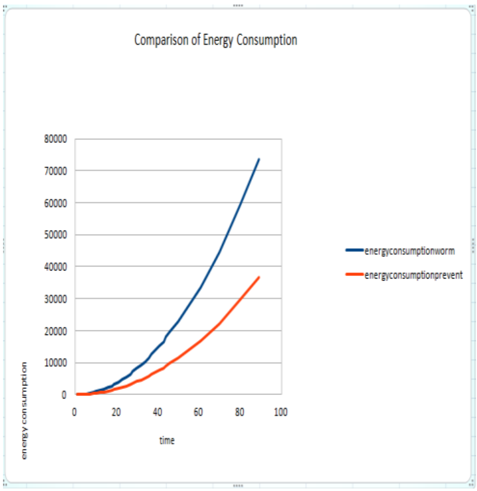

Figure 4. Comparison of Energy Consumption with worm hole and with isolator

V. Conclusion

In our research work, a new security algorithm is proposed which not only protect but also provide authentication to communicating nodes. The routing algorithms are exposed to many security threats one of them we have used in our work is worm hole. We have studied many researches regarding this threat. Our proposed work is free of number of hardware support which not only increases the cost but also much complicated to implement. The simulation of 50 nodes in our work proved the effectiveness of the proposed algorithm at the security level. Further studies are being done on this concept in presence of different attacks.

References

[1]. Y.-C. Hu, A. Perrig, D. B. Johnson; "Wormhole Attacks in Wireless Networks"; IEEE Journal on Selected Areas of Communications, vol. 24, numb. 2, pp. 370-380, 2006

[2]. Debdutta Barman Roy, Rituparna chaki, Nabendu chaki; "A new cluster based wormhole intrusion detection algorithm for mobile adhoc networks"; IJNSA, Vol 1, No 1, April 2009

[3]. Reshmi Maulik, Nabendu chaki; "A study on worm hole attacks in MANET"; International Journal of computer Information systems and Industrial Management applications, ISSN 2150-7988 Vol 3 (2011)

[4]. Bhavneet Kaur, Sandeep Singh Kang;" A distance based scheme for defending against Wormhole attack in Wireless sensor networks"; IJCNWMC ISSN 2250-1568 Vol-3 (2013)

[5]. Y-C Hu, A. Perrig, D. Johnson; "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols"; Proc. of WISE 2003, September 19, San Diego, California, USA, 2003

[6]. Y.-C. Hu, A. Perrig, D. B. Johnson; "Packet leashes: a defense against wormhole attacks in wireless networks"; INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, pp. 1976-1986, 2003

[7]. S. Capkun, L. Buttyan, J.-P. Hubaux; "SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks"; Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks; 2003

[8]. C. Chigan, R. Bandaru; "Secure Node Misbehaviors in Mobile Ad Hoc Networks"; Proc. of IEEE Conf. on Vehicular Technology Conference, VTC 2004, Vol. 7, pp. 4730-4734, 2004