International Journal Of Engineering Research & Management Technology ISSN: 2348-4039

May- 2014 Volume 1, Issue 3

Email: editor@ijermt.org Website: ijermt.org

WORMHOLE ATTACK MITIGATION IN MOBILE ADHOC NETWORKS using NS2

Ajay Kumar,Mandeep Singh
Department of Computer Science & Engineering
Shree Siddhivinayak Group Of Institutions,
Bilaspur, Yamuna Nagar, Haryana, India

Abstract
Mobile Adhoc Networks is an autonomous collection of mobile nodes and there is no fixed infrastructure, so, the open and dynamic nature of MANET makes it more vulnerable to attacks and also suffers from lot of problems related to congestion, routing etc. Security is one of the most challenging problems as the nodes are utilizing open air medium to communicate and the operation environment of such network is usually unpredictable. One of such type of attack is Wormhole attack which is most difficult to prevent. This attack results in information stealing, transfer delay or consumes bandwidth of the network. In this paper, a mechanism has been presented to prevent the network from this attack in which a secret key has been used and encryption is done at each level to provide secure delivery of the packet.

Keywords: MANET, AODV, RREQ, RREP, Wormhole Attack.

Introduction

Mobile Ad Hoc Networks is a collection of set of nods or stations that communicate with each other over a wireless channel. A wireless network uses radio waves or micro waves to connect the devices such as laptops to any business network or internet without the use of physical wired network between sender and receiver. The nodes in an Adhoc networks do not rely on existing infrastructure and the functioning of such network is dependent on the trust and cooperation between the nodes.Hence, each mobile node does the function of routing and share the responsibility of managing the network [2]. Such mobile Ad Hoc Networks have many attractive features including self-maintenance, automatic self configuration, inexpensive and quick deployment, and the lack of the centralized administration or infrastructure [3].
Wireless ad-hoc network helps in challenging many real-world problems, for example, communication in military field operation, emergency response operations, oil drilling and mining operation. The proliferation of wireless devices also stimulates the emergent applications in a wide range of areas covering from health to environmental control. However, the realization and wide deployment of such network face many challenges in the network [12]. Security is one of the most challenging problems in this network.

A particularly severe security threat, called the wormhole attack, has been introduced in the context of ad hoc networks [10]. In this attack, the attacker captures the packets from one location in the network and tunnels them to another malicious node at a distant point which replays them locally. The tunnel can be established in many ways e.g. out-of-band and in-band channel. This makes the tunneled packet arrive with a lesser number of hops and faster compared to the packets transmitted over normal route. This creates the illusion that the two end points of the tunnel are very close to each other. However, it is used by malicious nodes to disrupt the correct operation of ad hoc routing protocols. They can then launch a variety of attacks

against the data traffic flow such as selective dropping, eavesdropping, replay attack etc. Wormhole can be formed using, first, in-band channel where malicious node m1 transmits the received route request packet to another malicious node m2 using encapsulation through the pre-built path made by these malicious nodes [11], even though there is one or more nodes between two malicious nodes, the nodes following m2 nodes believe that there is no node between m1 and m2. And in out-of-band channel [15], the malicious node uses a physical channel that could be either long range wireless link or dedicated wired link between them. When the wormhole is made, the malicious nodes can hide or reveal themselves in the routing path. The former is known as the hidden attack and the latter is known as the exposed or open attack. They can lunch many types or varieties of attack like replay attack, selective dropping and eavesdropping etc.

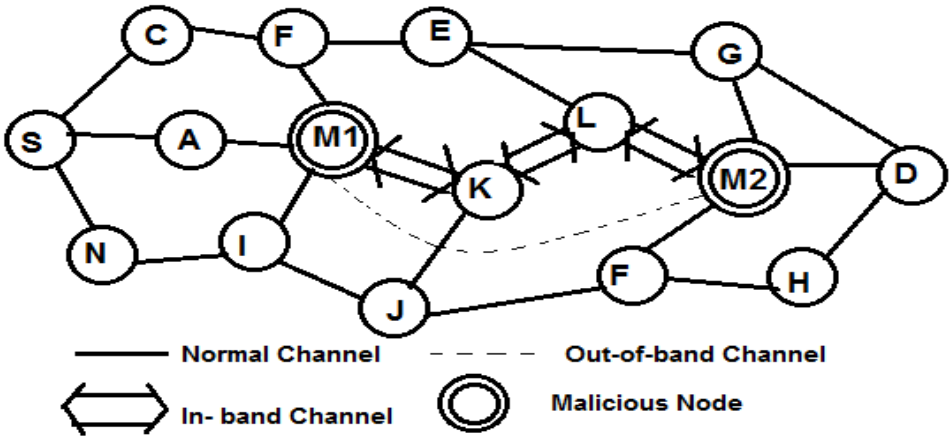

FIGURE 1 MODES OF WORMHOLE ATTACK

Types of Wormhole Attack[4]

- **Open wormhole attack:** In the open wormhole attack, the attackers include themselves in the RREQ packet header in the route discovery stage. Other authentic nodes are aware that the two colluding parties lie on the path but they would think that they are direct neighbors.
- **Closed wormhole attack:** The attackers do not modify the content of the packet in a route discovery. Instead they simply tunnel the packet from one side of the wormhole to another side and it rebroadcasts the packet. The path includes both the attackers and send the data too the destination.
- **Half open wormhole attack**: One side of the wormhole does not modify the packet and only another side modifies the packet while following the route discovery procedure. Thereby, generating the path S-M -D for the packets sent by S for D [4].

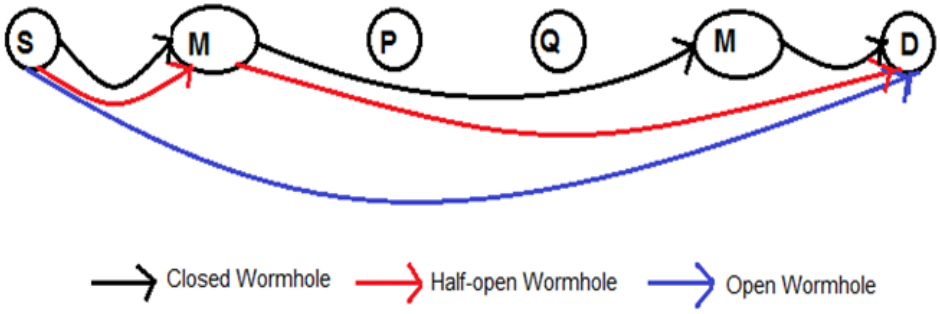

FIGURE 2 TYPES OF WORMHOLE ATTACK

In this paper, we present a mechanism to detect the wormhole node and to prevent the wormhole attack by encrypting the packet at each levels by sharing the Secret Key with the neighboring nodes and ensuring secured delivery via decrypting the packet at the neighbor node and matching the distributed Secret Key in MANET in AODV protocol environment. This paper is organized in 5 sections. In section 2, reviews starts by relating the work to other surveys in the literature. In section 3, AODV routing protocol is described and then in section 4, the proposed algorithm is presented. In section 5, analysis and results are reported to support the advocacy of the introduced algorithm.

1. LITERATURE SURVEY

The concept of threads [5] between the mobile nodes has been used to defend the network against the wormhole attack. Then source node estimates the minimum path to the destination during the route discovery. Wormhole node will create tunnel between any two of nodes in network, which will be detected by using some appropriate criteria as network traffic etc. Finally, those nodes will be detected and a normal route is selected for the data communication.

According to the author [6], every node shares its public key with the help of HELLO message with its neighbors during neighbor discovery Phase. In response to it, HELLO reply is generated.The source of Reply packet is verified by the encryption of hash value with the private key of source. The data Transmitted by node is also in encrypted form. Routing table in this technique will hold public key of destination node, next node and delay. This eliminates the fake identity of neighbor node completely. If node receives data with false digest value then it declares that the packet is received through the wormhole node and discards that packet. It also discards the routing entry for that node.

The author[7] has used the RSA technique for encryption and decryption purposes. It uses the 2Ack scheme to check that data is reached to the authentic node. This scheme can take acknowledgment from one hope and two hop nodes and finds the misbehaving node. If attacker does not forward the received message to the next node and tries to drop them into another location. This scheme prevents this by taking the acknowledgments from the next two nodes.

The authors present a graph theoretic framework [8] for modeling the wormhole attack. They provide a necessary and sufficient condition that any solution to the wormhole problem needs to satisfy. In addition, the authors also propose the use of local broadcast keys whereby the keys in different geographic regions are different. As a result, an encrypted message replayed via the wormhole in a different location cannot be decrypted by the receivers in that region.

The authors have worked upon the hound packets [9] to detect the wormhole node. They presented a protocol without the use of any special hardware such as synchronized clock or directional antenna. After the route discovery, wormhole detection process is initiated by the source. It counts the hop difference between the neighbors of the nodes that exceeds the acceptable level.

The author [17] has proposed the mitigation of wormhole in Adhoc networks. The scheme relies on the idea that usually the wormhole nodes attract most of the traffic by participating in the routing in a repeated way. Therefore, a cost will be assigned to each node depending on its participation in the routing. Besides preventing the network from the wormhole attack, the scheme also provides a load balancing among the nodes to avoid the nodes that are cooperative in routing.

2. ADHOC ON DEMAND DISTANCE VECTOR (AODV)

AdhocOn Demand Distance Vector (AODV) is a routing protocol for mobile Adhoc networks and other wireless Adhoc networks. AODV is capable of both unicast and multicast routing. It is an on demand distance vector routing protocol, which means a route is established by AODV to destination only on

demand. It keeps the records for the active routes only. Here, the sequence numbers are used by the AODV to ensure the freshness of routes. AODV is self starting, loop free and scales to large numbers of nodes which can be mobile.

When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this RREQ packet update their information for the source node and set up a backward pointer to the source node in route tables. In addition to the source node's address, the RREQ packet also contains the broadcast ID [16], the most recent sequence number for the destination of which the source node is aware. The intermediate node getting the RREQ may send a route reply (RREP) [2] if it is having the route to the destination with the corresponding sequence number greater than or equal to the sequence number contained in the RREQ or it can also be generated by the destination. If this is the case, it sends a RREP back to the source. Otherwise, the node will rebroadcast the RREQ [12]. Nodes keep the track of the RREQ's source IP address and broadcast ID. If the nodes receive a RREQ which they have already sent, they discard that RREQ and do not forward it. When the RREP is propagating back to the source, the nodes will set up the forward pointer to the destination. When the source receives the RREP, it starts forwarding the data packets to the destination. If the source node receives the RREP that contains the same sequence number with a smaller hop count or the greater sequence number, it may update its routing information for that destination and begin using the new route to send the packets. As long as the route remains active, the node will maintain the route entry. A route is active as long as the data packets are traveling from that path. When the source stops sending the data packets, the links will get time out and eventually it will be discarded from the immediate routing tables.

The existing mechanisms such as routing protocols assume a trusted environment so; any malicious node could disrupt the normal operation of such networks. Hence, these networks face acute security problems as compared to the wired medium.

3. PROPOSED ALGORITHM

The proposed work is about the prevention of the network from the wormhole attack. In this research, a mechanism is presented to secure the communication between source and destination. As the node has to start the communication, it first starts with the neighbor discovery from the neighbor list. It first generates the "Hello" message and encrypts it using the secret key. The encryption technique is used to prevent the network from the wormhole attack. As the neighboring node receives this message, the node will decrypt it using the same secret key and send the acknowledgement back to the sender. If the node is not authentic, it will remove its entry from the neighbor list. After the neighbor discovery if sends the RREQ to its immediate neighbors from the neighbors list to have the route to the destination. As the RREQ reaches the destination, it will generate a RREP message and unicast it to the source node.

To check the authentication of the node, it will also check the response time of the node. If the response time is greater than the threshold then also it excludes the node from the list. The complete process is repeated node by node till the destination node is achieved. The algorithm is analyzed on ns2 network simulator. Here the exact algorithm is presented.

Algorithm

Algorithm: Wormhole Attack Prevention
INPUT: Encrypted Message.
OUTPUT: Path to destination excluding wormhole Nodes.
Intermediate Nodes: i, j
Source Node: S

Destination Node: D

This algorithm is divided into two modules: Neighbor Discovery Mechanism and Route Discovery Mechanism. In first module, the secure neighbors are discovered and then, in the second module, the route is discovered from the source to the destination to transmit the data packets.

Neighbor Discovery Mechanism

Step1: Message Transmission begins for finding the neighboring node.
Step2: Generate HELLO message at each current node i and encrypt it by Secret key and forward to every other neighboring Node j in the network also based upon distance within transmission range.
Step3: While (i! = D)
Step4: If j is in neighboring list.
Then,
If (Secret key (Encrypted Message) == "Hello")
Then

Add Node j to the list of Node i.
Else
I. Originator i Removes j from its One Hop Neighbor.
II. Update Table and report the node j is a **Wormhole node**.
Endif
i = i + 1;
j = j + 1;
End if
End While
Step5: End

Route Discovery Mechanism

Step1: For New Path discovery Source S sends RREQ to j.
Step2: While (j! = D)
Step3: If (Secret key (Encrypted Message) == "RREQ" && Response Time < Threshold)
Then
Each Node j Forwards Encrypted RREQ.
Until the RREQ is received by D.
Else
The RREQ packet is dropped at j.
Endif
EndWhile
Step4: The Node D sends the Encrypted RREP to S while j is TRUE.
Step5: END

4. SIMULATION RESULTS

We have used the following simulation parameters to analyze our proposed algorithm in ns2 network simulator.

PARAMETER	VALUE
Traffic Type	CBR
Number of Nodes	36
Area Covered	800 X 800
Routing Approaches	AODV
Mobility Type	Critical Mobility
Threshold Energy of Node's	1.42681E-12
Maximum packets in Queue	50
Channel Type	Wireless channel

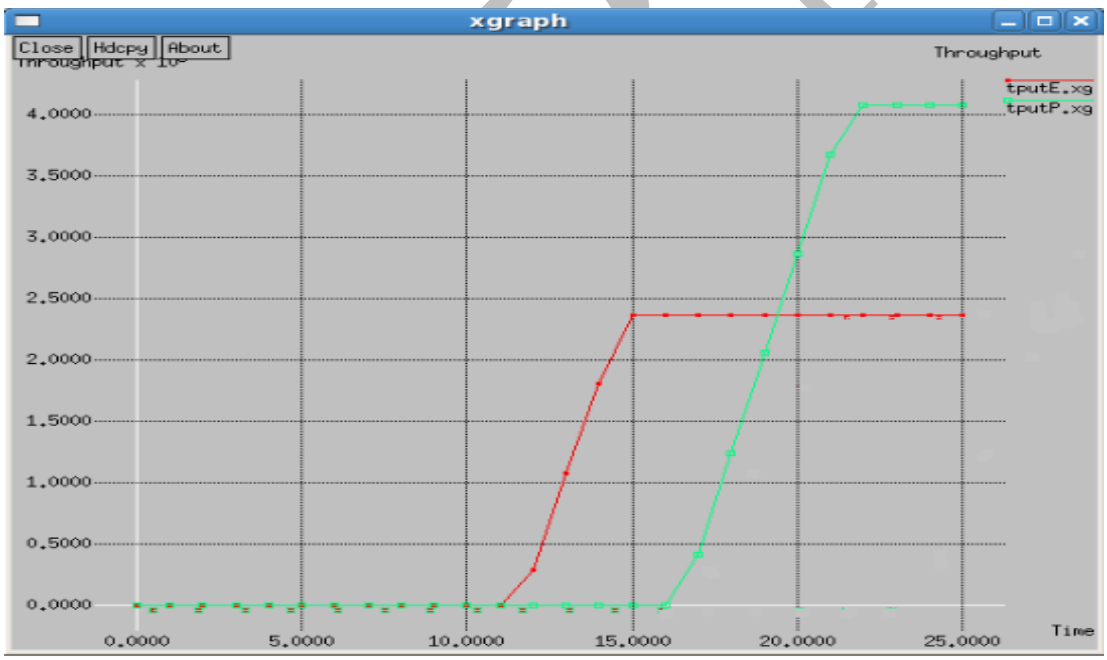

FIGURE 1.3 THROUGHPUT COMPARISONS

The above compared throughput are of the scenario's when there is no wormhole node present in the network which is represented in green while the red curve represents the throughput after the intrusion in the network i.e. the packet losses during the wormhole attack decreases the throughput of the network which is caused by the packet losses incurred on the wormhole nodes.

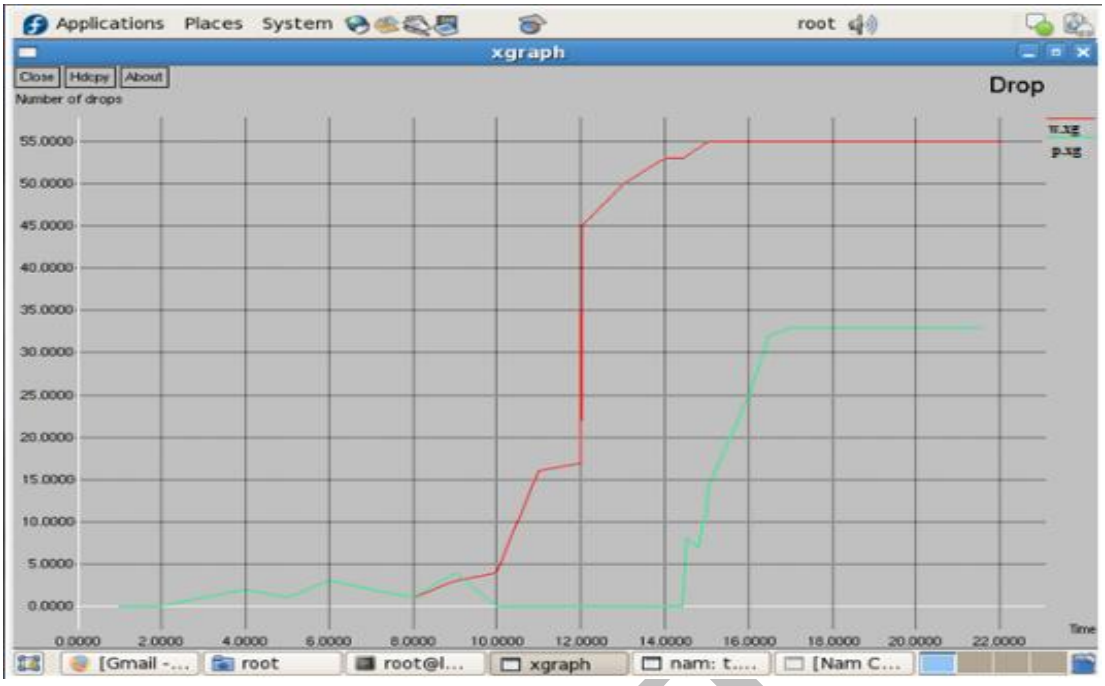

FIGURE 1.4 PACKET DROP COMPARISONS

The above graph shows the number of packets dropped during the wormhole attack which is represented in red and the drop which is during the prevention mechanism applied on the network. The other losses in the network are very less and negligible as compared to the wormhole packet losses thus they are represented in green.

5. CONCLUSION

In this paper, we presented an approach to prevent the network from the wormhole attack. The system is implemented in the mobile Adhoc networks on AODV protocol. In this approach, a secret key is used to encrypt the data packets in the network. It means only authenticated node will get the request packet and can reply. In this way, the mechanism is providing better throughput and less packet drop over the network. The implementation is performed on ns2 and the analysis is done using the xgraph.

REFERENCES

1. C. Siva Ram Murthy and B. S Manoj, Ad Hoc Wireless Networks, Architecture And Protocols (Prentice Hall PTR, 2004).
2. LathaTamilselvan, Dr. V Sankaranarayanan, Prevention ofWormhole Attack in MANET.
3. Anil Kumar Fatehpuria, SandeepRaghuwanshi, "An Efficient Wormhole Prevention in MANET Through Digital Signature", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 3, March 2013.
4. DharaBuch and DeveshJinwala, "PREVENTION OF WORMHOLE ATTACK INWIRELESS SENSOR NETWORK", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.
5. Nidhi Nigam, Vishal Sharma, "A comprehension on Wormhole Attack prevention technique using THREADS in MANET",Nidhi Nigam et al , International Journal of Computer Science & Communication Networks,Vol 2(4), 531-535.
6. PradnyaPatange, S.P.Medhane, "PUBLIC KEY BASED APPROACH TO MITIGATE WORMHOLE ATTACK", International Journal of Computer Science Engineering Research and Development (IJCSERD).
7. PravinKhandare, Prof. N. P. Kulkarni, "Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack", International Journal of Computer Trends and Technology- volume4Issue3- 2013.

8. L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.
9. Saurabh Gupta, SubratKar, S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", International Conference on Innovations in Information Technology, 2011.
10. YashpalsinhGohil, SumeghaSakhreliya, SumitraMenaria,"A Review On: Detection and Prevention of Wormhole Attacks in MANET", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.
11. A.VANI, D.SreenivasaRao, "A Simple Algorithm for Detection andRemoval of Wormhole Attacks for SecureRouting In Ad Hoc Wireless Networks", A.Vani et al. / International Journal on Computer Science and Engineering (IJCSE).
12. ReshmiMaulik and NabenduChaki, " A Study on Wormhole Attacks in MANET" International Journal of Computer Information Systems and Industrial Management Applications.
13. Vishal Pahal, Susheel Kumar , "A Cryptographic Handshaking Approach to Prevent Wormhole Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 50 – No.2, July 2012 .
14. Yih-Chun Hu, Adrian Perrigm, David B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, IEEE INFOCOM 2003.
15. Sana ulHaq, Faisal B Hussain"OUT-OF-BAND WORMHOLE ATTACK DETECTION IN MANETS" in proceedings of 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia,5th -7th December, 2011.
16. Rutvij H. Jhaveri,Ashish D. Patel, Jatin D. Parmar,Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV" in proceedings of IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010 12 Manuscript received April 5, 2010 Manuscript revised April 20, 2010
17. Mariannne. A. Azer, "Wormhole Attacks Mitigation", Sixth International Confernece on Availability, Reliability and Security, 2011.
18. Ajay PrakashRai**,** VineetSrivastava, Rinkoo Bhatia, "Wormhole Attack Detection in Mobile Ad Hoc Networks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.
19.