Securing MANET against Wormhole Attack using Neighbor Node Analysis

Sweety Goyal
M.Tech. Scholar
Dept. of Computer Sc. & Applications
Chaudhary Devi Lal University, Sirsa-125055
(India)

Harish Rohil
Asst. Professor
Dept. of Computer Sc. & Applications
Chaudhary Devi Lal University, Sirsa-125055
(India)

ABSTRACT
In mobile ad hoc networks (MANETs) security is of major concern because of its inherent liabilities. The characteristics of MANETs like infrastructure less network with dynamic topology pose a number of challenges to security design. There is an increasing threat of attacks in MANET. Wormhole attack is one of the security attacks on mobile ad hoc networks in which a pair of colluding nodes make a tunnel using a high speed network. This paper focuses on providing a solution for secure transmission through the network and proposes a neighbor node analysis approach to identify wormhole attack and removes wormhole link in MANET. The proposed work is simulated using NS-2 and is analyzed using certain parameters such as throughput, loss rate, delay rate.

Keywords
Wormhole Attack, AODV, Routing, Network Security, MANET

1. INTRODUCTION
Due to technological advances in laptop computers and wireless communication devices such as wireless phone and wireless LANs, wireless communication between the mobile users is becoming more popular than ever.

An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. There is an increasing trend to adopt ad hoc networking for commercial usage. However, their main applications lie in military, tactical and other security-sensitive operations. In these and other applications of ad hoc networking, secure routing is an important issue. Designing a foolproof security for ad hoc network is a challenging task due to its unique characteristics such as, lack of central authority, frequent topology changes, rapid node mobility, shared radio channel and limited availability of resources.

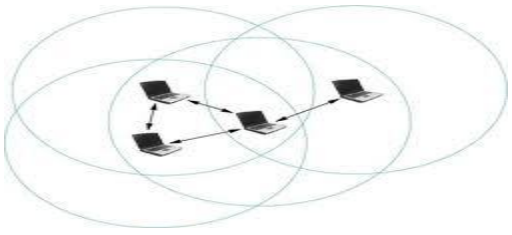

Figure 1: Mobile Ad hoc Network

Wireless ad hoc networks can be classified into three sub networks wireless sensor networks, wireless mesh networks and mobile ad hoc networks. Mobile ad hoc networks consist of auto configuring nodes such as laptop computers, PDAs and wireless phones that use wireless communication with each other. A mobile ad hoc network with four nodes is shown in Figure 1. The nodes at the same time may act as both host and router i.e. each node participates in routing by forwarding data for other nodes and deciding to which node data must be forwarded next, based on network connectivity. The routers are to move randomly and organize themselves without any centralized administration. Thus the network topology may change rapidly and unpredictably. Such a network may be an independent network or may be connected to internet. Applications of ad hoc networks range from military operations and emergency disaster relief to commercial usage such as community networking and communication between attendees at a meeting or students during a lecture. In wireless mesh network each node communicates with other nodes via radio waves to transmit its own data and also collaborates to relay other node's data. The Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors and a gateway or base station, which communicate with other wireless sensors by a radio link. The collected data such as temperature, sound, pressure etc. via the wireless sensor node is compressed and transmitted to the gateway directly. WSN are used to monitor physical or environmental conditions.

2. ROUTING
Routing is the selection of source destination pairs and the delivery of messages to correct destination. The routing protocol is needed because a packet may be required to hop several hops due to the limited transmission range of nodes before it reaches the destination. Routing protocol can be categorized into three categories [1] i.e. Proactive, Reactive and Hybrid.Proactive protocols are table driven protocols because of consistent maintenance, up to date routing information between every pair of nodes in the network by propagating routing information at fixed intervals. These protocols: Destination Sequenced Distance Vector (DSDV), Cluster Gateway Switch Routing (CGSR) and Optimized Link state Routing (OLSR).

i) Reactive Protocols are on demand protocols to create routes only when demanded by source nodes. It establishes a route to a destination through discovery process within the network, whenever there is a demand by source node. The discovered and established route is maintained by the route maintenance procedure until either the destination becomes inaccessible along each and every path from source or route is no longer needed. These Protocols are: Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR).

ii) Hybrid protocols are combination of both reactive and proactive protocols i.e table driven & on demand approaches such as Zone Routing Protocol (ZRP).

3. AODV

AODV is an on-demand routing protocol for ad hoc networks. AODV uses hop-by-hop routing by maintaining routing table entries at intermediate nodes. It involves three main procedures for communication between nodes: path discovery, path establishment, path maintenance [1].

The path discovery process is initiated when a source needs a route to a destination and it does not have a route in its routing table. Figure 2 shows routing process in AODV. To initiate path discovery, the source floods the network with a route request (RREQ) packet specifying the destination for which the route is requested.

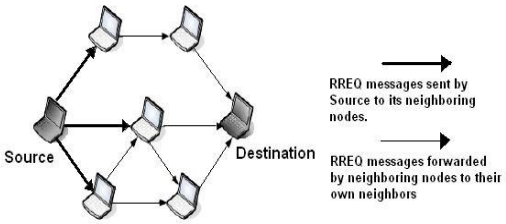

Figure 2: Routing in AODV

When a node receives an RREQ packet, it checks to see whether it is the destination or whether it has a route to the destination. If either case is true, the node generates a route reply (RREP) packet, which is sent back to the source along the reverse path. When the source node receives the first RREP, it can begin sending data to the destination. When a node detects a broken link while attempting to forward a packet to the next hop, it generates a RERR packet that is sent to all sources using the broken link. The RERR packet erases all routes using the link along the way. If a source receives a RERR packet and a route to the destination is still required, it initiates a new route discovery process. Routes are also deleted from the routing table if they are unused for a certain amount of time.

4. WORMHOLE ATTACK

Wormhole is a particularly severe attack and has been introduced in ad hoc networks. It is a kind of active attack and is hard to defend against. In this attack, two colluding nodes that are far apart are connected by a tunnel and give an illusion that they are neighbors [3]. Each of these malicious node captures route request messages, topology control messages and data packets from the network and send it to the other malicious node by tunnel which replays them into the network from there [5]. By using this additional tunnel these malicious nodes are able to advertise that they have the shortest path through them. So the tunnelled packet arrive either sooner or later with the lesser number of hops compared to the packets transmitted over normal multihop routes. The tunnel is used by malicious nodes to disrupt the correct operation of ad hoc routing protocols such as AODV. They can also launch some other attacks against the data traffic such as Selective Dropping, Replay Attack and Eavesdropping etc. Wormhole can be formed in two ways i.e. In-Band Channel and Out-of-Band Channel. In in-band channel malicious node n1 tunnelled the received route request packet to another malicious node n2 using encapsulation even though there are one or more nodes between two malicious nodes. The nodes following n2 node believes that there is no node between n1 and n2. In out-of-band channel two malicious nodes n1 and n2 establish a physical channel between them by either dedicated wired link or long range wireless link.

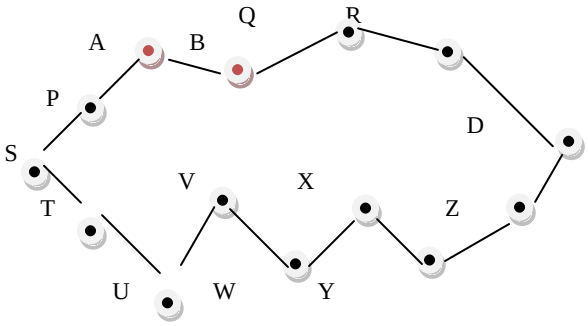

Figure 3: Wormhole Attack

In Figure 3, source node S broadcasts an RREQ message to find its way to the destination node D. Node P and T receives RREQ message from S. Now when A receives RREQ (forwarded by P) it records and tunnels the RREQ to B. Now B forwards it to Q, Q forwards it to R and finally RREQ reaches D. Again RREQ reached D through another route S-T-U-V-W-X-Y-Z-D but the RREQ reaching D through the other path reaches faster. So D ignores the message received through S-T-U-V-W-X-Y-Z-D route. Now D unicasts RREP through the route S-P-A-B-Q-R-D. Thus all the data packets pass through the wormhole tunnel between the malicious nodes A and B [6].

The malicious nodes can also transmit the eavesdropped packets to some other channel available to the attackers. The wormhole attack can also be combined with Message Dropping attack to prevent destination nodes from receiving packets meant for them. As a result securing AODV against wormhole attack is a big challenge.

4.1 Classification of Wormhole Attack

There are several ways to classify the wormhole attack. Wormhole can be classified into two classes- Hidden Attack and Exposed Attack, depending on whether malicious nodes show their identity into packet's header when tunnelling and replaying packets [7].

4.1.1 Hidden Attack

Each participating node on the path updates packet's header before forwarding it to the subsequent node by putting their identity (MAC address) to allow receivers know the packet directly comes from,. In hidden attack, wormhole nodes do not put their identity into the packet's header so that do not realize the existence of them. For example, in this kind of attack a path from S to D via wormhole link A, B will be S-P-Q-R-D as shown in Figure 3. In this way Q seems to get the packets directly from P so it considers P its neighbour although P is Out of radio range from Q. In general in hidden attack nodes within A's vicinity are fake neighbours of nodes within B's vicinity and vice versa.

4.1.2 Exposed Attack

In exposed attacks, wormhole nodes include their identities in the packet's header as other authenticated nodes do. Therefore, other nodes are aware of the existence of wormhole nodes but they do not know wormhole nodes are malicious. In case of exposed attacks, the path from S to D via wormhole will be S-P-A-B-Q-R-D. In hidden attacks, there are many fake neighbours created by wormhole link but there is no fake neighbour except (A, B) in exposed attacks.

5. RELATED WORK

To detect malicious nodes and avoid routing from these nodes robust secure routing has been proposed by K. Sivakumar and Dr. G. Selvaraj [4]. In this technique called Robust Secure Routing (RSR), the concept of FR packets was introduced which inform nodes along a path that they should expect specified data flow within a given time frame. The path elements can therefore be on the lookout for the given data flow, and in the event that they do not receive the traffic flow, they can transmit info to the source informing it that the data flow they expected did not arrive. A path tracing algorithm for detection and prevention of wormhole attack has been proposed by P. Anitha and M. Sivaganesh [11]. The PT algorithm runs on each node in a path during the AODV route discovery process. It calculates per hop distance based on the RTT value and wormhole link using frequency appearance count. The corresponding node detects the wormhole if per hop distance exceeds the maximum threshold range.

An effort return based trust model to detect and evade wormhole attack is proposed by Shalini Jain and Dr.Satbir Jain in [12] where each node executing the trust model, measures the accuracy and sincerity of the immediate neighboring nodes by monitoring their participation in the packet forwarding mechanism. The sending node verifies the different fields in the forwarded IP packet for requisite modifications through a sequence of integrity checks. If the integrity checks succeed, it confirms that the node has acted in a benevolent manner and so its direct trust counter is incremented. Similarly, if the integrity checks fail or the forwarding node does not transmit the packet at all, its corresponding direct trust measure is decremented. This derived trust is then used to influence the routing decisions, which in turn guide a node to avoid communication through the wormholes.

For detection and prevention of attack in MANET an efficient multipath algorithm was proposed by Waseem Ahad and Manju Sharma [10]. This algorithm will randomly generate a number in between 0 to maximum number of nodes and make the node with same number as transmitter node as wormhole attack is done by transmitter and receiver so have to decide the transmitter and receiver. Then generate the route from selected transmitting node to any destination node with specified average route length. After this it will send packet according to selected destination and start timer to count hops and delay. By repeating the whole process up to this point will be required as to store routes and their hops and delay. Now for detection of malicious node, if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker. Algorithm will check the delay of all previous routes which involve any on node of the suspicious route. The node not encounter previously should be malicious.

An end-to-end detection of wormhole attack (EDWA) in wireless ad hoc networks is proposed by Xia Wang and Johnny Wong [8]. Authors first presented the wormhole detection which is based on the smallest hop count estimation between source and destination. If the hop count of a received shortest route is much smaller than the estimated value an alert of wormhole attack is raised at the source node. Then the source node will start a wormhole tracing procedure to identify the two end points of the wormhole. Finally, a legitimate route is selected for data communication.

An Approach to Defend against Wormhole Attack in Ad hoc Network Using Digital Signature is proposed by Pallavi Sharma and Aditya Trivedi [9]. This paper presented a mechanism which is helpful in prevention of wormhole attack in ad hoc network is verification of digital signatures of sending nodes by receiving node because each legitimate node in the network contains the digital signature of every other legitimate nodes of same network. In proposed solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

6. PROPOSED WORK

We are presenting a novel approach to secure AODV against wormhole attack in MANET using neighbor node analysis. In our work, neighbor node analysis approach analyze the neighboring nodes so as to check the authenticity of the nodes for secure transmission of data over the network. According to this approach a node will request to its neighboring nodes and perform a request and response mechanism. The node will maintain the table to track the timeout. If the reply time is not accurate there is an attack in the network. All the intermediate nodes are analyzed to detect the presence of wormhole attack using AODV protocol in MANET. The steps of proposed algorithm are:

Step 1: As transmission initiates, source node search for the neighbor nodes and form a neighbor list.

Step 2: Source node then generates RREQ packet and encrypt it using the public keys of neighboring nodes and distribute it all around.

Step 3: If the neighboring node receiving RREQ packet, decrypt it using their private key then the node is authenticated otherwise, remove the node from neighbor list and report node as bad node.

Step 4: If node is authenticated it will send the RREP message to the source node.

Step 5: Source node will record the response time of RREP message.

Step 6: Compare the response time of RREP message with response time of actual message sent.

If $\text{Response Time}_{(\text{Actual Message})} > \text{Response Time}_{(\text{RREP})} + \text{Threshold}$

Then

a) Wormhole link is present in that route.
b) Block that route and update it in routing table.
c) Fetch another route from the routing table.

Step 7: The process is repeated for each node in the neighbor list till the destination is reached.

7. SIMULATION BASED PERFORMANCE ANALYSIS

In our experiment we simulated 50 nodes distributed over 670m x 670m terrain on NS-2. The initial positions of nodes are random. The implementation used 802.11 MAC layer and CBR traffic type. The AODV protocol is used which is an on demand routing protocol and is given in Table 1.

Table 1: Simulation Parameters

PARAMETER	VALUE
Number of nodes	50
Topography Dimension	670 m x 670 m
Traffic Type	CBR
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11.Mac Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	AODV

In Figure 4, the comparison between the existing (with wormhole attack) and proposed approach (without wormhole attack) was made on basis of throughput. Here the simulation is carried out for 10 seconds. The given graph shows the throughput for both the scenarios (existing and proposed). Initially the throughput was zero at the time of start. After the TCP (Transmission Control Protocol) connection was build, we can see that the throughput increased in the proposed system.

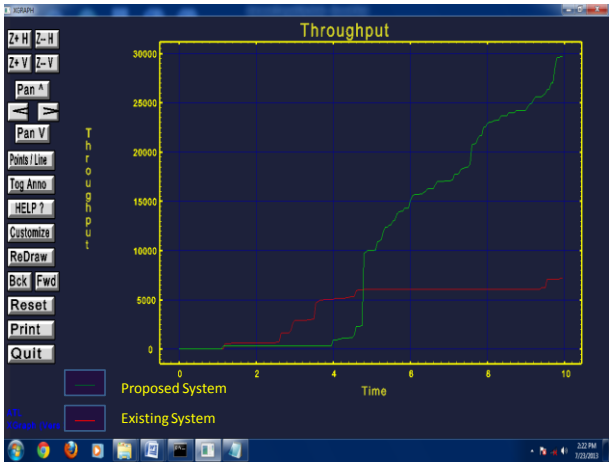

Figure 4: Throughput Comparison between Proposed and Existing Approach

Figure 5: Loss Rate Comparison between Proposed and Existing Approach

The existing approach defines the loss with wormhole and proposed approach is the solution with neighbor node analysis approach. In Figure 5, the loss rate is presented. As we can see the loss rate is less in the proposed system indicated by a green line.

The graph in Figure 6 gives the number of bytes transferred when the simulation is carried out for 10 seconds. We can see that the bytes transferred are increased after the implementation of proposed algorithm.

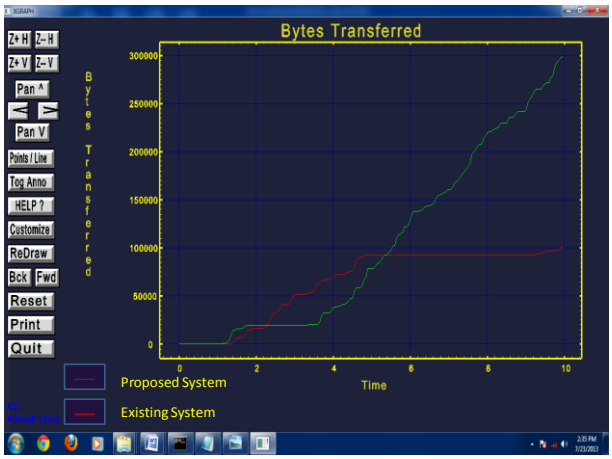

Figure 6: Bytes Transferred Comparison between Proposed and Existing Approach

The packet delay is the delay rate when packets are sent through the network from source to destination. In Figure 7, we can see the delay rate for the both systems. The delay for the proposed system decreases with time and after a few seconds it gets constant.

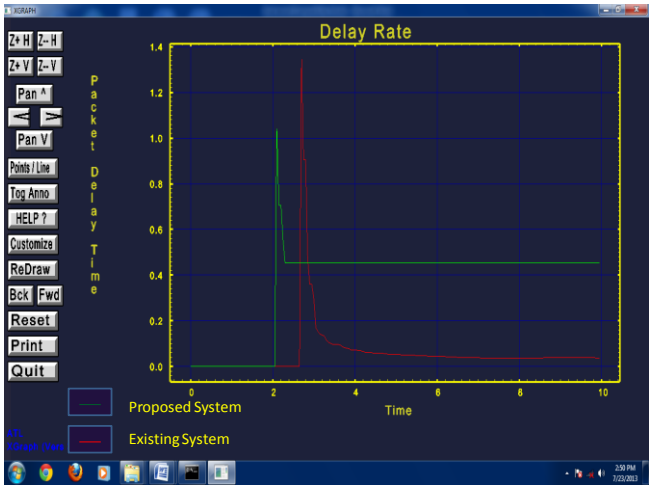

Figure 7: Delay Rate Comparison between Proposed and Existing Approach

8. CONCLUSION

Wormhole attack is one of the most serious attacks in MANETs. Many solutions have been proposed to detect and remove the attack but are not perfect in terms of efficiency or any special hardware, the proposed approach is based on neighbor node analysis and provides a solution for detection of wormhole attack and removal of wormhole link from the network. The proposed technique gives a better solution for wormhole attack in the network. The proposed work with respect to four parameters throughput, loss rate, bytes transferred and delay rate has been simulated. Simulation results shows that the proposed approach is successful in detecting wormhole attack and

locating wormhole link thus avoiding wormhole link in route discovery process providing better efficiency.

9. REFERENCES

[1] Achint Gupta, Priyanka V J, Saurabh Upadhyay, "Analysis of wormhole Attack inAODV based MANET Using Opnet Simulator", International Journal of Computing, Communications and Networking Vol. 1, October 2012.

[2] Jatin D. Parmar, Ashish D. Patel, Rutvij H. Jhaveri1, Bhavin I. Shah, " MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, Vol. 10, No.4, April 2010.

[3] Reshmi Maulik, Nabendu Chaki, "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Vol. 3, pp. 271-279, 2011.

[4] K. Sivakumar, Dr. G. Selvaraj, "Analysis of Worm Hole Attack In MANET And Avoidance Using Robust Secure Routing Method", International Journal of Advanced Research in Computer Science and Software Engineering Vol. 3, No. 1, January 2013.

[5] Yashpalsinh Gohil, Sumegha Sakhreliya, Sumitra Menaria, " A Review on Detection and Prevention of Wormhole Attcaks in MANET", International Journal of Scientific and Research Publications, Vol. 3, No. 2, February 2013.

[6] Abari Bhattacharya, Himadri Nath Saha, " A Study of Secure Routing in MANET various attacks and their countermeasures", IEMCON organized in collaboration with IEEE in January 2011.

[7] Susheel Kumar, Vishal Pahal, Sachin Garg, " Wormhole Attack in Mobile Ad Hoc Networks: A Review", IRACST, Vol. 2, April 2012.

[8] Xia Wang, Johnny Wong, "An End-to-end Detection of Wormhole Attack in Wireless Ad hoc Networks", 31st Annual International Computer Software and Applications Conference IEEE, 2007.

[9] Pallavi Sharma, Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", IEEE, 2011.

[10] Waseem Ahad, Manju Sharma, "Efficient Multipath Algorithm in MANETs to Prevent Wormhole Attack", CT International Journal of Information &Communication Technology Vol. 1, No. 1, 2013.

[11] P. Anitha, M. Sivaganesh, "Detection And Prevention Of Wormhole Attacks In Manets Using Path Tracing", International Journal of Communications Networking System, Vol. 01, No. 02, December 2012.

[12] Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks" , International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

10. AUTHOR'S PROFILE

Er. Sweety Goyal received her Bachelor of Technology degree in Computer Science & Engineering in 2008 from Ch. Devi Lal Memorial Engineering College Panniwala Mota, Sirsa, India. She is pursuing M.Tech. in Computer Science and Engineering from Chaudhary Devi Lal University, Sirsa India. At present she is engaged as lecturer in M.M. University, Mullana. She has published 3 Research Papers in International/National level reputed Journals/Conferences. Her area of interest is Ad hoc Networks, Mobile Ad Hoc Network (MANETs) & Sensor Networks.

Dr. Harish Rohil received his Ph. D. in Computer Science from Department of Computer Sc. & Applications, Kurukshetra University, Kurukshetra- 136119 (India). He is working as Asst. Professor in Department of Computer Sc. & Applications, Chaudhary Devi Lal University, Sirsa-125055 (India) since July 2004. He is member of IEEE and LIFE member of IDES (Institute of Doctors Engineers and Scientists). His area of interest includes software reuse, data mining and computer networks.