A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks

V. Karthik Raju
Department of Computer Science and Engineering
National Institute of Technology, Surathkal
Mangalore, India.
vkarthik.1233@gmail.com

K. Vinay Kumar, Associate Professor
Department of Computer Science and Engineering
National Institute of Technology, Surathkal
Mangalore, India.
vinaykumarin2000@yahoo.com

Abstract— **Mobile ad hoc networks are vulnerable to many kinds of attacks since they have unique characteristics like limited bandwidth, limited battery power and dynamic network topology. Among the various attacks possible in mobile ad hoc networks wormhole attack is one which is treated as a very severe attack. In this attack a malicious node records packets at one location in the network and tunnels them to another malicious node which is present in the other end of the network. In this paper, we have proposed an algorithm which detects and avoids the wormhole attack in the routing phase itself. Our mechanism is based on the total round trip time (RTT) of the established route and the average round trip times of the sender one hop neighbors, which is considered as maximum one hop round trip time. Our solution works for both mobile ad hoc networks and wireless ad hoc networks.**

Keywords— **MANET, Wormhole attack, RTT, AOMDV, malicious node**

I. Introduction

Mobile ad hoc network (MANET) is a combination of several independent wireless nodes that acts as a host as well as a router. In MANET there is no need of any infrastructure or base stations due to this MANETs are used in many applications. Each node can directly communicate with other nodes if they are present in their communication else via other nodes. Since there is no need of any infrastructure in MANET these are used in many areas like military battlefield, emergency or rescue situations like floods, earthquake etc, and also in classrooms or colleges [1]. Though it has many advantages it also has some disadvantages, due to limited bandwidth, limited batter power of nodes and absence of infrastructure there are several chances for the attackers to break through the network and perform many attacks like Blackhole attack, Flooding attack, Link withholding attack, Link spoofing attack, Replay attack, Colluding misrelay attack and Wormhole attack, these are briefly described in [2][3][4].

There are several kinds of routing protocols which are classified into two types.

- Table driven routing protocols or Proactive routing protocols.
- On-Demand routing protocols or Reactive routing protocols.

In proactive routing protocols like Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Global State Routing, Fisheye State Routing, Hierarchical State Routing etc., the routes are calculated prior to the communication. All the nodes in the network maintain routing tables which contain routing information to all other nodes in the network and these tables are updated frequently in order to maintain consistency of the network. Whenever the network topology changes the nodes propagate update messages in the network to maintain consistent routing information about the network. In proactive routing protocols whenever a node wants to send data it sends data immediately by taking a route from the routing table without any delay. Proactive routing protocols work effectively in small networks only they are not suitable for large networks since every node has to maintain all the routing information of every other node in the network and these are only suitable for fixed networks and not for mobile ad hoc networks because in mobile ad hoc networks nodes have mobility and the network topology changes frequently.

In reactive routing protocols such as Ad hoc on-demand Distance Vector (AODV), Dynamic Source Routing Protocol, Cluster Based Routing protocol (CBRP), Temporally Ordered Routing Algorithm (TORA), Ad-hoc On-demand Multipath Distance Vector (AOMDV) etc., the routes are calculated dynamically only when they are required. In this whenever a source node wants to send packets to destination node it initiates the route discovery mechanism to find the path to the destination. In reactive routing protocols the source cannot send the packets immediately, it requires some time to establish the route to the destination only then it can send the packets.

Section II describes about wormhole attack and types of wormhole attacks, In section III we described related work proposed by various authors, In section IV we described our mechanism to detect and avoid wormhole attacks, In section V we present our results and in the section VI we conclude.

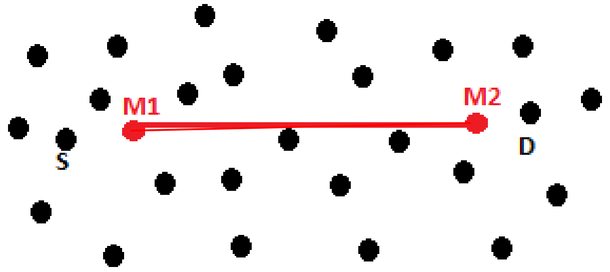
II. WORMHOLE ATTACK

In this paper we are focusing on a particular kind of attack called wormhole attack which is considered as a severe attack in MANET. Minimum two malicious nodes are required to perform this attack; more than two malicious nodes are also used to perform this attack. In this attack the two malicious nodes resides in the two ends of the network and they form a

978-0-7695-4817-3/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCS.2012.4

link between them using an out-of-band hidden channel like wired link, packet encapsulation or high power radio transmission range[5]. After they form a tunnel between them as shown in figure 1, whenever a malicious node receives packets it tunnels them to the other malicious node and in turn it broadcasts the packet there. Since the packet is travelling through the tunnel it reaches the destination speeder than other route and moreover the hop count through this path is going to be less so this path is established between the source and the destination [6]. Once the path is established between the source and the destination through wormhole link they can misbehave in many ways in the network like continuously dropping the packets, selective dropping the packets, analyzing the traffic and performing Denial of Service attack.

Wormhole attacks are divided into two types based on the behaviour of the malicious nodes; they are hidden attacks and exposed attacks. In the former one the malicious nodes do not update the packet header with their identities like MAC address, this keeps the malicious nodes invisible to the outside world but where as in the later one the malicious nodes update the packet header with their identities this makes them look like normal nodes in the network.



S Source
D Destination
M1 Malicious node 1
M2 Malicious node 2
▬ Wormhole tunnel

Fig. 1. Mobile ad hoc network with wormhole link.

III. RELATED WORK

In this section we discuss some of the existing solutions to wormhole attacks in wireless ad hoc networks and mobile ad hoc networks. One of the solutions provided to wormhole attacks in wireless ad hoc network is packet leashes [7]. This solution is based on the packet's maximum allowed transmission distance. The author has described two types of leashes they are geographical leashes and temporal leashes. In the former one the sender node has to include its own location and sending time into the packet, when the corresponding packet is received by the receiver node it compares those values with its receiving time of the packet and its location values. Based on that if the distance between them is very high it restricts the path to establish. In the later one when the sender sends a packet it includes its sending time in the packet, and when this packet is received it note downs the receiving time of the packet and it computes the time taken for the packet to travel from source to destination, based on this time it comes to know how far the packet has travelled, if it has travelled too far then it restricts the communication. In temporal leashes the expiration time is also used instead of noting the times to restrict the packet transmission distance. But these require special hardware like GPS to find the location in case of geographical leashes and tightly synchronized clocks in case of temporal leashes which are expensive to adopt.

Another approach to defend against wormhole attacks in MANET is based on hop count analysis [8]. In this hop counts of all the available routes to a destination is taken and compared. Normal routes have higher hop count when compared to routes which have wormhole so the routes which have very less hop count are avoided and a set of safe routes are selected based on the hop count, now the packets are send through these selected routes. But this works for only hidden wormhole attacks and it may not work all the time in the case of exposed wormhole attacks.

Another approach to defend against wormhole attacks in ad hoc networks is using location based keys [9]. In this the author has proposed this solution for designing compromise tolerant security mechanisms for sensor networks. In this they developed a node to node authentication scheme and the establishment of pair wise keys between neighbouring nodes. In this the packets of authenticated nodes are only accepted.

In [10] the author proposed a mechanism to detect wormhole attacks in wireless ad hoc networks which is based on the round trip time. In this when a route is established between a source and destination the round trip times between each and every two successive nodes is calculated. The round trip time of the wormhole link is higher than the round trip time between normal nodes, so the two successive nodes which have higher round trip time are considered as the wormhole link. But this does not work all the time for example when the malicious node enters incorrect sending time and receiving time of the packet.

In [11] the author proposed a statistical based solution called Statistical Analysis of Multipath (SAM) for wormhole attacks in wireless ad hoc networks. SAM method is based on the observation that certain statistics of the discovered routes by routing protocols will change dramatically under wormhole attacks. Examining such statistics is possible and hence the wormhole attacks can be detected and can pinpoint the attackers if enough routing information is available which can be obtained by multi-path routing.

IV. PROPOSED MECHANISM TO DETECT AND AVOID WORMHOLE ATTACK

In AOMDV routing protocol whenever a node wants to communicate with another node first it checks in the route table whether a route is present or not, if the route is not present then it broadcasts the RREQ packet to its neighbours which in turn checks whether a route is present to the required destination or not, if present it gives the routing information else it broadcasts the packet. Whenever the destination receives the RREQ packet it sends RREP packet to the source along the same path through which the RREQ packet has arrived. For all the consequent RREQ packets which have arrived through other routes the RREP packets are sent along the same path. At the source node all these paths are stored in routing table. In this way the routes are established. The advantage of AOMDV routing protocol is, whenever a link failure occur due to unavailability of intermediate nodes it immediately fetches another route from the routing table, this saves time of route establishment.

In the proposed mechanism the detection of wormhole attack is done in the routing phase itself, in the following way. When the source node broadcasts a RREQ packet note the time (t_1) and when the corresponding RREP packet is received by the source, again note the received time of the packet, If there are multiple RREP packets received, that means there are more than one route available to the destination node then note the corresponding times (t_{2_i}) of each RREP packet. By using the above two values one can calculate the total round trip time (t_{3_i}) of the established route or routes. In the next step calculate the round trip times for all the one hop neighbors of the source, for this first fetch all the neighbors of the source node from the neighbor list of the source then broadcast hello packets to all the neighbors of the source. While broadcasting the hello packet note the time (t_s) and similarly while receiving the reply for hello packets note the times (t_{r_i}) for corresponding hello packets, from this calculate the round trip times (t_{rt_i}) taken for each hello packet to travel from source node to neighbor nodes and back to source node. Now calculate the average of all the times that noted in the above step. Since all the round trip times of the one hop neighbors of the source are considered, by averaging them one can get the exact time taken for a packet to travel one hop distance, this time is considered as the maximum time taken for a packet to travel one hop distance and this time is noted as the maximum round trip time (t_{max}) for one hop. Now multiply the maximum round trip time (t_{max}) with the hop count (h) of the established route, this gives the maximum time taken for a packet to travel along the established route, this is considered as estimated round trip time (t_e). Now compare the total round trip time (t_{3_i}) with the estimated round trip time (t_e), if the total round trip time (t_{3_i}) is less than or equal to estimated round trip time (t_e) then there is no wormhole link present in the established route and one can continue with that route else wormhole link is present in that route. Since wormhole link is detected in that route, that route is no more used and it is blocked and that route is kept in the blocking list at the source node. So that, from next time onwards whenever a source node needs a route to that destination, first it checks in the routing table in the route establishment phase for a route and it will come to know that that route is having wormhole link and it will not take that route instead it will take another route from the routing list of the source node which is free from wormhole link if available. The proposed mechanism has less overhead and also does not require any additional hardware. Since AOMDV routing protocol is used the end to end delay is less because even when a route is failed another route is fetched immediately from the routing table and the time taken for route establishment is saved by this.

Algorithm:

```
1.  When the source node broadcasts RREQ packet
    note the time $t_1$.
2.  For each RREP packet received by the source
    node
        a. Note the time $t_{2\_i}$
        b. Calculate the round trip time for all
           routes using this formula
                $t_{3\_i} = t_{2\_i} - t_1$.
3.  End For
4.  Fetch the neighbors from the neighbor list.
5.  Broadcast the hello packet to neighbors of the
    source node and note the time $t_s$
6.  For each hello packet received by the source
    node.
        a. Note the time $t_{r\_i}$
        b. Calculate the round trip times ($t_{rt}$) using
           this formula
                $t_{rt\_i}=t_{r\_i} - t_s$
7.  End For
8.  Calculate the average round trip time for one hop
    neighbors, from the round trip times taken in the
    step 6.
9.  Note this time as the Maximum round trip time
    ($t_{max}$) for one hop distance.
10. Fetch the hop count (h)
11. Calculate the estimated round trip time ($t_e$) using
    this formula
        $t_e= t_{max} * h$
12. If ($t_{3\_i} <= t_e$) then
        a. No wormhole link is present in that
           route
        b. Continue with that route
13. Else
        a. Wormhole link is present in that route
        b. Block that route and update it in the
           routing table
        c. Fetch another route from the routing
           table $r_i$
        d. If (route is present && not in the
           wormhole blocked list)
                perform the process from step 10
           Else
                Stop
        End If
End If
```

V. RESULTS

In this section, we have shown the simulation results for detection rate of wormhole attacks and throughput of the packets at the destination in normal network (without wormhole), under wormhole attack and using our algorithm against wormhole attack. The mobile ad hoc network environment is created using CPP language and AOMDV routing protocol [12] is used for routing purpose.

A. *Figures and Tables*

Table 1. Simulation parameters

Simulation area	1000m X 1000m
Routing protocol	AOMDV
Packet size	512 bytes
Traffic model	CBR
No. of nodes	10,20,30,40,50
Transmission range	100m
Simulation Time	10s
Traffic Model	Random

Figure 2 shows the detection rate of hidden wormhole attacks for different lengths of wormhole tunnel. If the wormhole tunnel length is greater than 1 (here the length 1 means the distance covered by a normal node in the mobile ad-hoc network, if the length is 2 that means the distance between the two malicious nodes is the twice the distance covered by a normal node) then the detection rate is higher. X axis shows the different lengths of wormhole tunnel and Y axis shows the percentage of detection rate. If the wormhole tunnel distance is less than 1 then the detection rate is less but however in real time scenario the wormhole tunnel will not be less than 1 because the main aim of wormhole attack is to attract more traffic through the wormhole tunnel established by the two malicious nodes and if the wormhole tunnel is less than 1 its main objective will be missed since if the distance is less, it cannot cover more number of nodes and there is also no guarantee that the path will be established through them because the distance covered by this malicious nodes is less, the normal nodes may find route directly to the destination via other routes which gives a better path which has less hop count, so obviously the distance of the wormhole tunnel will be kept as large as possible by the attacker.

The detection rate of hidden wormhole attacks is higher than the detection rate of exposed wormhole attacks because in hidden wormhole attacks the malicious nodes do not include their parameters such as MAC address, hop count in the packet header so when a path is established through them the hop count will be less and when the estimated round trip time is calculated it will give less time and the round trip time of the established route will be more so it is easy to detect the hidden wormhole attacks with the proposed solution.

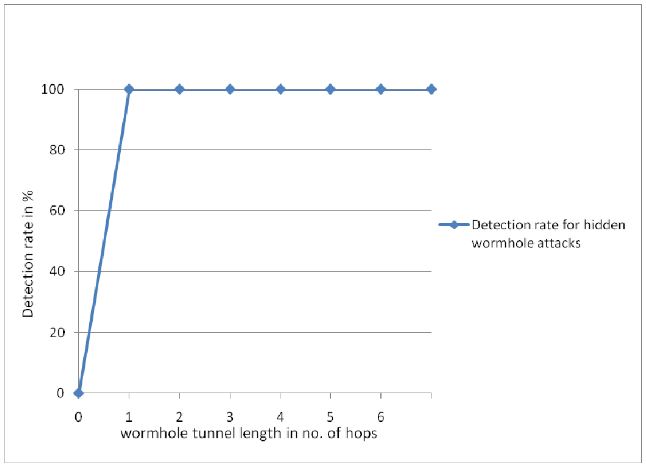


Fig. 2. Detection rate Vs length of Wormhole tunnel (Hidden wormhole attacks).

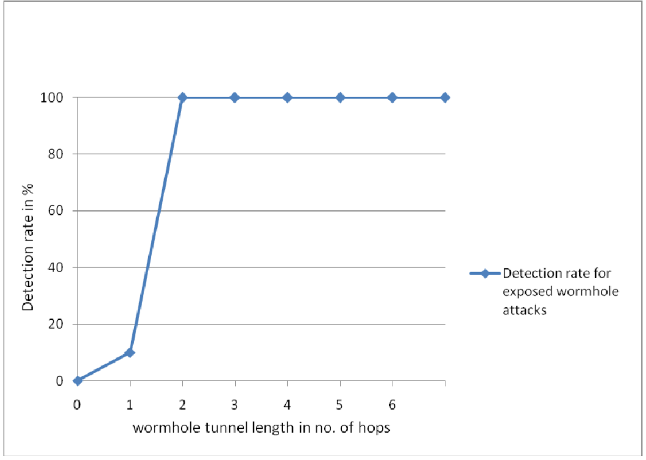


Fig. 3. Detection rate Vs length of Wormhole tunnel (Exposed wormhole attacks).

Figure 4 shows the throughput at the destination node under three scenarios they are throughput at destination node without attack, with attack and throughput at destination node using proposed algorithm against the wormhole attacks. The throughput at the destination node under without attack is good that means packets are reaching the destination node. Figure shows that the throughput at the destination node under wormhole attacks is zero which means the data packets are not reaching the destination node, they are dropped in between by the malicious nodes. By applying the proposed solution against the wormhole attack the throughput at the destination node is normal since the source node will take only the route which is free from wormhole tunnel, it will not take the route which has wormhole tunnel, so the throughput is same as when it is under without attack.

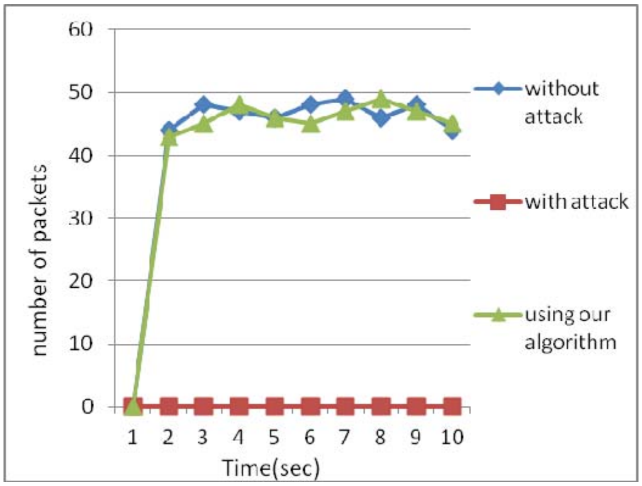


Fig. 4. Throughput at destination

VI. Conclusion

In this paper, we proposed a simple and efficient mechanism to detect and avoid wormhole attacks in mobile ad hoc networks. In our mechanism there is no need of any special hardware, just by calculating the round trip time of the established route and the average one hop round trip time of the source node, which is considered as maximum one hop round trip time we detect the wormhole link and we avoid the wormhole by blocking that route and selecting another route from the available routes in the routing list. Our solution works in both mobile ad hoc networks and wireless ad hoc networks.

References

[1] Jun-Zhao Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", IEEE 2001.

[2] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato "A Survey of Routing attacks in mobile ad hoc networks" IEEE Wireless Communications October 2007.

[3] Preeti Nagrath, Bhawna Gupta "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey" IEEE 2011.

[4] Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F.Hassan, Magdy S. El-Soudani "Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a Proposed Decentralized Scheme" IEEE 2008.

[5] Azer, M.A., El-Kassas S.M., Hassan, A.W.F., El-Soudani M.S., "Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a proposed Decentralized Scheme Marianne " IEEE Third International conference on Availability, Reliability and Security, 2008.

[6]Reshmi Maulik, Nabendu Chaki "A comprehensive review on wormhole attacks in MANET" International Conference on Computer Information Systems and Industrail Management Applications(CISIM) 2010.

[7] Yih-Chun Hu, Adrian Perrig, David B. Johnson "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks" IEEE 2003.

[8] Shang Ming Jen, Chi Sung Laih and Wen Chung Kuo "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET" Sensors 2009.

[9] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang "Securing Sensor Networks with Location-Based Keys" 2005 IEEE Wireless Communications and Networking Conference (WCNC)

[10] T. Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee, "Transmission Time-based mechanism to Detect Wormhole attacks," 2007 IEEE Asia-Pacific Services Computing Conference.

[11] Ning Song and Lijun Qian, Xiangfang Li "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach" Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05).

[12] Mahesh K. Marina, Samir R. Das "Ad hoc on-demand multipath distance vector routing" wireless communications and mobile computing 2006.