An Efficient Algorithm based on Fibonacci Pattern Hound Packets for Detection of Wormhole Attack in DSR for Mobile Ad Hoc Networks

Krishna Kumar Joshi
Institute of Engineering and
Technology
Alwar (Raj.)
India

Neelam Khemariya
Poornima College of
Engineering
Jaipur (Raj.)
India

Deepak Chaudhary
Institute of Engineering and
Technology
Alwar (Raj.)
India

ABSTRACT

Wireless networks are playing very important role in the present world. Mobile Ad hoc Networks (MANET) are the extension of the wireless networks. These networks are playing crucial role in the each and every field of the human life. They are used in those places where a simple wireless network cannot use. They play a significant role in real time applications such as military applications, home applications wireless sensor applications etc. Due to their adaptive nature they are threatened by number of attacks such as Modification, Black Hole attack, Wormhole attack etc. Wormhole attack is one of the dangerous active attacks in the mobile Ad hoc Networks (MANET). In this paper a secure and efficient approach for the detection of the wormhole attack in the Mobile Ad Hoc Networks (MANET) is described. The algorithm is implemented in a very popular on demand routing protocol, called DSR (Dynamic Source Routing) protocol. In this approach the solution is provided by sending the Hound Packet in the order of Fibonacci series and also modifies the table entries in terms of storing them in sorted order, so that the processing of Route Discovery becomes faster.

General Terms

Mobile Adhoc Networks, Routing protocols, Security Threats, Active attacks, Passive attacks, Reactive Routing protocol, Algorithm.

Keywords

DSR, Fibonacci Series, Hound Packet, Proactive, Reactive, Table Entries, Wormhole Attack..

1. INTRODUCTION

Wireless Networks can be classified into two categories: **Infrastructure Wireless networks** and **Infrastructure less Wireless Networks**.

In **Infrastructure Wireless networks**, communication takes place between the Wireless nodes through the Access Point (AP) and the wireless nodes cannot communicate directly. The access point just not works as a control medium access, but acts as a bridge as well.

Infrastructure less Wireless Networks do not need any fixed infrastructure for the communication. These networks are also called Ad Hoc Networks. In these types of networks, each node can communicate directly with other node and thus there is no requirement of the access point. An important thing about these networks is that these networks do not have

routers, the wireless nodes work as routers. These networks don't have any fixed or static topology.

Mobile Ad hoc networks are collection of mobile nodes that use wireless transmission for communication. These networks have no fixed infrastructure, no fixed configuration and other controlling device such as router etc [1]. The setup or deployment of these networks is very easy because these networks don't have a fixed infrastructure or a fixed topology also they have a very less setup time. The routers are free to move randomly.

Fig 1: Mobile Ad hoc Networks

Wormhole attack is one of the most dangerous attacks in the mobile Ad Hoc Networks. In wormhole attack, two or more malicious nodes together make a tunnel in the network, in which the traffic enters from one end and passes through the tunnel and leaves from the other end [10]. Wormhole link or tunnel can be created by means of a high quality wireless link or a logical link. After building a wormhole link, one attacker is able to receive all the messages which travel from this route. This attacker node then copies packets from its neighbors, and forwards them to the other malicious attacker through the wormhole link. Then another malicious node which receives these packets, replays them into the network in its vicinity. Figure 2 showing the wormhole tunnel.

Fig 2: Wormhole Attack

2. ROUTING PROTOCOLS

Many protocols have been suggested for Mobile Adhoc Networks keeping applications and type of network in view. Routing protocols can be classified mainly into three categories, as defined below:

2.1 Proactive Routing Protocols

In Proactive routing protocols each node maintains one or more tables containing routing information about all other node in the network. All nodes keep on updating these tables to maintain latest view of the network. Some popular proactive protocols are: DSDV, WRP and ZRP [1].

2.2 Reactive Routing Protocols

In these protocols, the nodes don't maintain a routing table. Instead, they maintain a route cache. Routes are created only when a node want to communicate with another node. For this purpose source invokes the route discovery procedure. Some reactive routing protocols are: DSR, AODV and TORA [1].

2.3 Hybrid Routing Protocols

This type of protocols contains the best features of proactive and reactive routing protocols. In case of the intra-domain routing, these protocols uses the proactive approach, while in case of inter-domain routing these protocols uses the reactive approach. For example, Zone Routing Protocol (ZRP) etc.

3. DYNAMIC SOURCE ROUTING (DSR) PROTOCOL

3.1 Overview

DSR protocol is popular Reactive routing protocols. There are two important mechanisms in DSR: **Route discovery mechanism** and **Route maintenance mechanism**.

Route discovery mechanism is used to find the route between the sender and the receiver. Figure 3 shows the frame format of the route request option.

Option Type	Opt Data Len	Identification
Target Address		
Address1		
.....		
Address n		

Fig 3: Route Request Option

Figure 4 is showing the frame format of the route reply option.

	Option Type	Opt Data Len	L	Reserved
Address1				
Address2				
.....				
Address n				

Fig 4: Route Reply Option

Route Maintenance mechanism helps source node to detect that the communication route is OK or it is broken. It can detect that a route is broken by checking that there is no communication since a long time

Figure 5 is showing the frame format of the route error option.

Option Type	Opt Data Len	Error Type	Reserved	Salvage
Errored Source Address				
Errored Destination Address				
.....				
Type Specific Information				
.....				

Fig 5: Route Error Option

3.2 Security Threats in DSR

Mobile Ad Hoc Networks are unwired network with continuous changing topology (dynamic topology). So, they are very vulnerable to security threats. In protocol stack, Physical layer, which is the first layer is provide the functions like forming the network topology, synchronization, medium access control and flow control etc. this layer has security issues like Denial of Service (DoS) attacks and preventing signal jamming.

Network layer is the second layer that provides one of the important the function called routing and logical addressing. Network layer has to deal with security of ad-hoc routing protocol and related parameters. Some dangerous attacks occur in network layer are black hole attack, wormhole attack, gray hole attack and message altering etc. transport layer is the third layer in the p[protocol stack. Transport layer is responsible for end to end communication, segmentation and reassembly, flow and error control etc. Transport layer has issues with end to end data security with encryption

methods and Authentication. Session hijacking is one kind of attack that can be occurring in the transport layer.

The last layer in the protocol stack is Application layer. Application layer deals with the user. It contains different types of protocols for providing different type of services for user. The application layer has security concerns with prevention from worms, malicious codes, as well as virus detection. Repudiation is one kind of attack that can occur in the application layer. Some other dangerous threats for Mobile Ad Hoc Networks are Fabrication, Denial of Service attack etc. There can be two kinds of attacks: active and passive.

3.2.1 Active Attacks

Active attacks are the kind of attack in which the attacker can see the information of a user and can modify it too. These attacks contain some modification on the actual data or a false data. In these attacks, the attacker injects arbitrary packets into the network. The goal may be to attract packets destined to other nodes to the attacker for analysis or just to disable the network. Active attacks sometimes are detected. This makes active attacks a less inviting option for most attackers. These attacks can be subdivided into four categories: replay, modification of message, masquerade and denial of service. An active attack may be internal or external.

Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a big security concern for DSR.

3.2.2 Passive Attacks

In a passive attack the attacker can learn or use the information of a user but does not modify nor change it. In a passive attack, the attacker does not change or alter the operation of a routing protocol but only attempts to discover valuable information. Defending against such attacks is very difficult. Two important passive attacks are the traffic analysis and the release of the message contents.

These attacks are very difficult to detect because they do not involve in any modification of the data. Routing information contains the relationships among nodes and also information about the nodes such as their IP addresses, hardware addresses etc. so if attacker is able to find the routing information, he can easily extract the information about the nodes and about the relationship among the nodes.

4. LITERATURE REVIEW

Wormhole attack is one of the most dangerous attacks. Many researchers did their work on this attack and try to provide the solution for this attack. The researchers provide a lot of solution based on different technologies, concepts and terms. Some important approaches are described below

Marianne et al [2] proposed an algorithm based on the theory of diffusion of innovations. The algorithm is divided into five phases: Normal network routing, wormhole parameters measurement, actor's network formation, route selection using penalties and intrusion detection. In the normal network routing phase AODV protocol find the route on the basis of minimum hop count. Also a counter is added to check how many times a particular node participated in routing. In wormhole parameter phase some parameters such as arrival

speed are measured for malicious node identification. In the actor's network formation phase, when a node receives the RREQ/RREP packet, compares how many hops offered by the incoming packet and by the routing table entries. Then it selects a node which has minimum hop count and has a recent route to the destination. Then it checks how many times this selected nodes participated in routing for a particular destination and if it has greater value than the threshold then this node is treated as a malicious node.

Kuldeep Sharma et al [3] proposed an approach which is based on the MHA (Multiple hop count analysis) .in this approach they use a general concept that the route contains the hop count 5 or 6, but the route under a wormhole has a hop count value 2. So, if the users avoid the route with the small hop count can easily avoid most of the wormhole attacks. In this approach, they calculate the hop count value for all the routes and then select a safe set of routes for the transmission of the data. And then send the packet in a random order by these safe routes. They implemented their approach in the AODV routing protocol. Then they assign a unique ID to each and every node so that we can easily differentiate between the simple node and the attacker malicious node.

Yih chun hu et al [4] propose an approach, called packet leashes. The lease contains timing and global positioning system information about each packet on the basis of hop by hop. So a node can easily detect that whether the packet which he received has travelled a distance larger than the physically possible by using the information stored in a packet leash. There are two types of the leashes: geographical and temporal. Geographic leash requires loose clock synchronization. Temporal leases works on tighter clock synchronization and also they are not dependent on GPS.

Khalil et al [5] propose a protocol, called LiteWorp for wormhole attack discovery, basically for the static networks. In this LiteWorp approach, all the nodes of the mobile ad hoc networks obtain the complete routing information about their neighbour nodes. In comparison to the normal routing protocols where the nodes finds the information about their neighbouring nodes by using the route discovery process, in LiteWorp approach the nodes actually knows who is their neighbour and who is the neighbour of the neighbour because LiteWorp approach uses two hop routing approach to find the information about the neighbouring nodes rather than the one hop approach This information is very useful to detects the Wormhole attack because nodes can easily analyze the behaviour of their nodes and detect that which node is the malicious node and by this they can easily avoid the wormhole attack.

Pirzada et al [6] proposed an algorithm which does not need any special hardware. This approach is mainly works on the round trip time mechanism. Basically, the round trip time is the total time to send the message to the destination plus the time to receive the acknowledgement receiving time. Generally, the round trip time is twice of the propagation time. In this approach the round trip time is calculated as the total time to send the route request message from the source to the destination node plus the time to receive the route reply message from the destination. The round trip time between the two real neighbour nodes is always less than the round trip time between the two malicious (fake) nodes. By this theory, a node can easily differentiate between a real node and a malicious fake node. In this approach, every node do this work, means every node calculates the round trip time

between itself and all of its neighbour node and thus easily detects the malicious node.

Hubaux et al [7] proposed another solution for detection of the wormhole attack by using the directional antennas. In this approach node uses the specific sectors of their antennas to communicate each other. So every node has the information about the location of its neighbor when it receives a message from its neighbor. So this extra information about the location of the nodes is very useful in case of detection of the wormhole attack.

S. Capkun et.al. [8] Proposed a secure scheme for the detection of the wormhole attack in wireless sensor networks. This scheme is based on an authenticated distance bounding technique, called MAD. This approach is similar to the packet leashes approach at a particular, but has some significance differences. This approach does not require the information about the location and clock synchronization, which are needed in the packet leashes. In this scheme to find the distance for secure location verification ultrasound is used. This helps to relax the timing requirements. Also for the verification of the true neighbor, means it is not a fake neighbor, this scheme is used. The main problem with this scheme is that it needs an additional hardware and also it still remains unclear that how the realistic timing analysis will be done at the lower cost for the wireless sensor networks.

Saurabh gupta et al [9] proposed an approach, called WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on the AODV protocol. In this approach a Hound packet is sent after the route discovery process, means after the route has been discovered. This hound packet is processed by all the nodes, except that nodes which are involved in the path setup process. Basically the path discovery is done by the help of the two types of packet, called RREQ and RREP. When the sender gets the message, it creates a hound packet and computes its message digest and signed this message digest with its own private key and attached all this information with the hound packet.

5. PROPOSED WORK

In the previous section we described a lot of approaches for the detection of wormhole attack in Mobile ad hoc Networks. Even though these approaches are very good but some of them have limitations also. In this paper a secure and very efficient approach for the detection of the Wormhole nodes is described. We implement this work in a popular reactive routing protocol, called DSR protocol. In our work, the Hound packets are sent in the Fibonacci series pattern. This approach will help to reduce the processing delay. Also, the table entries are always stored in the sorted form. So this will improve the speed of the searching. The algorithm is described below:

Algorithm:

(i). Initialization Process:

Source node s starts the route discovery process.

(ii). At source Node :

Initially $S3_{src}=1$, $S2_{src}=1$, $S1_{src}=0$;

Initially $Pcount_{src}=0$;

$Pcount_{src} = Pcount_{src} + 1$

If ($Pcount_{src} == S3_{src}$)

{Source node creates a Modified Root Reply packet which contains all nodes identity of recent path, And MD of packet signed by its private key.

And then send this Packet to its all neighbor node.}

$S1_{src}=S2_{src}$;

$S2_{src}=S3_{src}$;

$S3_{src}=S1_{src}+S2_{src}$;

(iii). All Network Nodes:

Each node periodically sends its public key to its one hop neighbor. Nodes who receive MRR packet first increments the CRNH field for the first node entry whose P.B is 0.

If (Any of the nodes listed in the MRR packet is its neighbor)

{Set all P.B in the packet till node entry to which it is a neighbor.}

Otherwise

Forward it.

(iv). At Destination Node:

Destination node create table for each entry of special RR packet.

This table contains three fields "Node id", "Process bit" and "count to reach next hop".

(v). Calculate difference of each row:

If (difference > 4)

{Node and its previous node in the path may form wormhole link and it is wormhole node.}

6. IMPLEMENTATION AND RESULTS

The proposed work is implemented in NS-2 (ns 2.34) simulator and executed on a Pentium (Core i3) processor with 3 GB of RAM, running at 2.40 GHz under Red Hat Enterprise Linux (RHEL) 5.0.

6.1 Parameters

The effectiveness of work to detect the Wormhole attack is evaluated in this subsection using the simulations performed in a very popular simulator, called Network Simulator (NS)-2 with the 50 mobile nodes. The graphical representation of this simulation is shown in the popular animator, called Network Animator (NAM). The traffic type is Continuous Bit Rate (CBR), the channel used is a wireless channel, the Ad hoc routing protocol used is Dynamic Source routing (DSR) and the network interface is wireless physical. The parameters are defined in the table 1 below:

Table 1 Simulation Parameters

Parameter	Value
Number of Nodes	50
Topography Dimension	670 m x 670 m
Traffic Type	CBR
Signal Prop. Model	Two Ray Ground model
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni directional
Routing Protocol	DSR
Interface Queue	Drop Tail/Priority Queue
Max pkts in IFqueue	50
Channel	Wireless Channel
Link Layer Type	LL
Network Interface Type	Wireless Phy

6.2 Simulation Results

Figure 6 is showing the simulation scenario of the 50 mobile wireless nodes. This figure is used to show the initial position of these nodes.

Fig 6: Simulation of 50 Mobile Nodes Implementing DSR Protocol

Figure 7 is showing the movement of the scenario file contains the location of the mobile nodes

Fig 7: Movement Scenario file showing Nodes Position

Figure 8 is showing the movement of the scenario file showing the route and link changes.

Fig 8: Movement Scenario file showing the route and link changes

Figure 9 is showing the movement of the trace file showing the traffic generator script.

Fig 9: Traffic Generator Script for 50 Mobile Nodes

6.3 Simulation Graphs

Three graphs end to end delay, throughput and packet delivery ratio are described here to show the simulation results. Every graph contains three sub graphs. The first graph is for the simple DSR protocol, when there is no attacker node presented. This graph is shown by the Dark blue color. Second graph is for the case where there are the attacker nodes and no prevention algorithm is presented. This graph is shown by the red color. And the last graph is for the case when we implemented our algorithm to identify the attacker nodes. This graph is shown by the green color. Basically the graph is drawn between the time and the number of mobile nodes presented in the network (in our case, there is 50 nodes). The next subsections are used to describe these graphs.

6.3.1 Average End to End Delay Graph

This metric is basically used to describe the average time to send a packet from source to the destination. It is always measured in seconds.

Fig 10: A Screenshot of Average End to End Delay (in msec.) Graph

6.3.2 Throughput Graph

This metric is basically used to describe the total number of bits send to the physical layer per second. So it is always measured in kbps.

Fig 11: A Screenshot of Throughput Graph

6.3.2 Packet delivery Ratio Graph

Basically this graph is used to describe the Packet delivery ratio which is the ratio of the total incoming packets and the actual received packets by the destination.

Fig 12: A Screenshot of Packet Delivery Ratio Graph

7. CONCLUSION AND FUTURE SCOPE

In this paper a secure efficient approach for the detection of the wormhole attack in the Mobile Ad Hoc Networks is described. The algorithm is implemented in DSR protocol. In the proposed approach a solution is provided which is based on the Hound packet with the two modifications. First modification is to send hound packet in the Fibonacci series order and another modification is to always store the table entries in a sorted form. These two modifications made the approach very secure and efficient.

The comparison graphs show the results in the three cases- when there is no attacker node, when there are attacker nodes and when algorithm is implemented.

For the future work, it may be worthwhile to merge other solution improvement methods to improve the performance of the proposed approach, so that we can get good results when the number of mobile nodes is large and also the number of attacker nodes is much more.

8. ACKNOWLEDGMENTS

It is with deep sense of gratitude and reverence to **Prof (Dr.) A. K. Srivastava, Prof (Dr.) Neelam Sharma, and Mr. Bipin Kumar Rai** for providing all the facilities and working environment in the institute.

We want to express our deep sense of obligation to our family and God for their blessings and encouragement.

9. REFERENCES

- [1] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010 ISSN: 2010-0248
- [2] . Marianne A. Azer, , IEEE, Sherif M. El-Kassas, and Magdy S. El-Soudani, " An Innovative Approach for the Wormhole Attack Detection and Prevention In Wireless Ad Hoc Networks", in IEEE Conference, 2008.
- [3] Kuldeep Sharma, Dr.G.Mahadevan, "Advance Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Int. J. on Recent Trends in Engineering & Technology, Vol. 05, No. 01, Mar 2011.
- [4] Sun Choi, Doo-Young Kim, Do-Hyem Lee, "WAP:Wormhole Attack Prevention Algorithm in Mobile AD-HOC network", Sensor network, Ubiquitous and Trustworthy Computing 2008, SUTC'08
- [5] Vih-chun-hu, Adrian Perrig, David B.Johnson, "Packet Leashes: A defense against Wormhole Attack in Wireless Mobile AD-HOC network", Rice University Department of computer science.Technical Report TRO1-384 December 17, 2001
- [6] A. A. Pirzada and C. McDonald, "Detecting and evading wormholes in mobile ad-hoc wireless networks", International Journal of Network Security, 3(2):191C202, Sept.2006.
- [7] S. Capkun, J.-P. Hubaux, and L. Buttyan, "Mobility helps security in ad hoc networks", Proceedings of MobiHoc, 2003.
- [8] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations", Proceedings of the 25th IEEE International Conference on Computer Communications Societies (INFOCOM '06), Barcelona, Spain, April 2006.
- [9] Saurabh Gupta, Subrat Kar, S Dharmaraja, WHOP: Wormhole Attack Detection Protocol using Hound Packet, 2011 International conference on innovations in information technology.
- [10] Ritesh Maheshwari, Jie Gao, Samir R Das, "Detecting Wormhole Attacks in Wireless Networks using Connectivity Information", in IEEE INFOCOM 2007, Alaska..