Reputation based Efficient Isolation of Wormhole Nodes

T.Padmavathy
Assistant Professor,
Sri Venkateswara College of Engineering,
Sriperumbudur, India,

G.Sumathi, PhD.
Professor,
Sri Venkateswara College of Engineering,
Sriperumbudur, India,

K.Srinivasan,
Assistant Professor,
Sri Venkateswara College of Engineering,
Sriperumbudur, India,

ABSTRACT
Mobile Adhoc Network (MANET) is infrastructure less as it does not require any specialized router to do the routing tasks. Instead, each and every node in MANET acts as a router as well to perform the routing tasks with the dependability on a routing protocol. This feature of MANET leads to serious security threats affecting the performance of the network. The attacks may be done at various layers of the network. Thus, security becomes the vital service for the success of MANET. Network Layer protocols extend connectivity from neighboring 1-hop nodes to all other nodes in MANET. A variety of attacks targeting the network layer have been identified. One such critical problem is wormhole attack. This paper proposes a reputation based isolation of wormhole node, which provides a trust computation to the Worm Hole Avoidance protocol (WARP), leaving the normal node without any support for additional hardware .It combines the advantages of WARP and the basic trust model.

General Terms
Mobile Adhoc Networks (MANET), AODV, Reputation, Trust, Security, Network Layer.

Keywords
Enhanced WARP, WORMDETECT, CALCTRUST.

1. INTRODUCTION
MANET comes under the hottest research area in the field of networking. With the advent of MANET, it becomes easier to form a group communication among a set of peer working group for knowledge sharing, confidential information sharing, medical diagnostics etc., without the need for any centralized coordinator to establish the communication between the peers of the group. Without a central coordinator establishing the proof of identity, authentication, the so formed network is vulnerable to a variety of security attacks. These attacks can be done at all layers of the protocol stack of the network reference model. The most concentrated layer will be the network layer with a variety of functions like path determination, path setup and switching.

Routing protocols available for adhoc networks concentrate on performance metrics like maximization of throughput, network lifetime, reducing network delay etc., rather than the security issues. Hence, in the recent years there has been substantial work done over these protocols to improve the proposed protocols in terms of security, energy efficiency and other criteria. Thus, the routing protocols available are to be updated to account for the various attacks. There are various updates that are done to the existing routing protocols as a countermeasure to various attacks. With various updates available, this paper focuses on implementing a trust based algorithm as proposed by Azad Amir Pirzada [2] to the wormhole avoidance routing protocol (WARP) [1], which is an extension to AODV protocol to secure against wormhole attack. We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

2. ISSUES IN PROVISIONING OF SECURITY
The following characteristics [3] of MANET makes it difficult to establish security among the node of the network.

Shared Broadcast Channel: Data transmitted by a node is received by all other nodes which are directly/indirectly connected by the transmission range of the network. So a malicious node can easily receive the data sent by other nodes of the network.

Mobile operational Environment: Nodes of the mobile adhoc network are roaming from one place to the other and are not stable. They are vulnerable to a variety of attacks from other mobile nodes.

No central Control: Since MANET is wireless and infrastructure less; there are no central nodes to authorize the nodes that are coming into the network, forwarding thepackets, performing routing activities etc., Hence there is a higher probability of a malicious node performing the routing decision and forwarding.

Lack of Authentication: MANET is dynamic and hence nodes come in and leave the network dynamically. This provides a way for the intruder to come into the network easily and perform various attacks on the network.

Scarce Resources: Resources such as bandwidth, battery power, and computational power are scarcely available which limits implementation of powerful security algorithms.

3. NETWORK LAYER ATTACKS
Listed below are a variety of network layer attacks which are to be considered with great care. These attacks when left unnoticed or ignored can lead to disastrous effects.Our interest is to propose a solution to detect the wormhole nodes by efficient detection and isolation.

3.1 Wormhole Attack
An attacker receives packets at one location in the network and sends them to another location[4]. Routing is disrupted when routing control messages are tunneled. This tunnel between two malicious nodes acts as a wormhole

which poses a great threat to MANET routing protocols. When a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack always leads to the discovery of routes that includes the malicious wormhole node.

3.2 Black hole Attack

In black hole, the malicious node tries to advertise a route to the destination even though the malicious node does not have any valid route. Thus, the black hole attack tries to exploit the mobile ad hoc routing protocol, such as AODV, by advertising route replies to the source node. On grabbing the attention of the source node, the malicious node intercepts the forwarded packets and does not forward it to the destination since it does not have a valid route. Any malicious node suppresses or modifies packets originating only from some nodes but not from all the nodes, which limits others, nodes to know about the malicious behavior.

3.3 Byzantine Attack

Byzantine attack refers to a malicious node creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

3.4 Routing Attack

Routing attacks tend to disrupt the operation of the network by making overflow in the routing table, route cache poisoning, rushing attack etc.,

4. PREVIOUS WORK

There are various methods and algorithms to defend against or to recover from various security attacks. All the proposed methods either modify the existing proposed protocols for MANET like AODV, DSR, DSDV and the like, or make use of some additional hardware to improve the security.

One of the foremost solutions proposed is the Packet leashes [4], which adds up some more additional information called as leash to restrict the maximum transmission distance that a packet can travel through. The packet leash added may carry temporal or geographical information, which is used to detect and defense against wormhole attack. These two mechanisms require tightly synchronized clocks (temporal packet leashes) or special hardware for location (geographical packet leashes) which is expensive to use widely.

Chiu and Lui [5] proposed a two phase mechanism named as DeLPHI which made use of both per hop delay and hop count to give a solution to wormhole attack. Phase1 named as Data Collection involves collecting the delay and hop count metrics from the nodes of the network. Phase2 named as Data Analysis and detection involves analyzing the information collected in phase1 to detect the presence of wormhole nodes. DeLPHI does not work well when all paths are tunneled.

Van Phuong [6], proposed a method to detect wormhole in Wireless Ad Hoc Networks using AODV routing protocol by calculating & comparing the Round Trip Time between every two successive nodes along that route during route setup protocol. TTM is able to detect both hidden & exposed wormhole attacks, locating the wormhole, requiring no special hardware.

Watchdog and path rater [7] is a two phase mechanism based on Dynamic Source Routing. The two phases are termed as Watchdog and Path rater. Phase1, termed as Watchdog detects selfish nodes.Phase2, termed as path rater assigns ratings to the nodes. Whenever the node is in its promiscuous mode, it buffers every packet that it receives for some duration to know its transmission by the neighboring node.

Ming Yang Su [1], has proposed Wormhole avoidance routing protocol (WARP). The principle of WARP is to allow neighboring nodes of a wormhole node to notice that the wormhole node has an extreme capacity of competition in path discovery. Two main limitations of WARP are identified. One, Although a normal node may be located at a key position of connectivity in a network, and hence, be isolated due to a high route-building rate, which may be recovered later.. Two, in the design of WARP, if one isolated node behaves normally, it may be recovered from isolation which makes it possible to recover the wormhole node too.

The proposed work is an extension to Wormhole avoidance routing protocol, which overcomes the first limitation of Wormhole avoidance routing protocol (i.e.,), the key node will not be removed from the network even for a minimum amount of time.

5. RELATED WORK

The proposed work is an extension to Adhoc on-demand Routing protocol (AODV) and Wormhole Avoidance Routing Protocol (WARP).The details of AODV is discussed in the following sections.

5.1 Adhoc on Demand Distance Vector (AODV) Routing Protocol

AODV is one of the on-demand routing protocol, which finds and establishes the route to the destination when a route is needed widely. AODV protocol is the most widely adopted MANET routing protocol with its dynamic route capture androute building capability. In order to keep track of the dynamic routes AODV uses routing table to keep track of the reverse paths.

5.1.1 AODV Message Types

AODV basically has two types of messages namely, Route request and route reply. It also has one more additional message named as “Hello” message. A “Hello” message is nothing but a Route Request message with TTL=1.Any node that wishes to make a communication with the destination node for which the route is not available makes a RouteRequest. The source node waits for the Route reply for specified wait time. If the node does not receive any reply within the specified time, the node retransmits the Route reply for specified number of times and waits for the route reply.

5.1.2 Processing Of AODV Messages

Initially, when a node wishes to transmits packets to a destination node it checks to see whether it has a route to the destination node. If the source node has a fresh route to the destination as determined from the sequence number, it uses the available route. If a fresh route does not exist, it sends outa route request packet to all its neighbors. Any neighbor that has got a route replies to the route querying node. If none of the neighbors got a fresh route in their routing table, they flood the packet to its neighbors till a route is found or the reply is made by the destination node. The source node may receive multiple path replies, but ultimately considers only one among them.

As shown in the Fig.1, the source node sends the route request to its entire neighbor. The intermediate nodes on receiving the route request packets first checks to see if there exists a latest route to the destination in its routing table. If so, it replies with the route reply packet. If it does not have a route to the destination, it simply forwards it to its neighbor. This process continues until an intermediate node replies with a route reply packet or the destination node replies with the route reply packet.

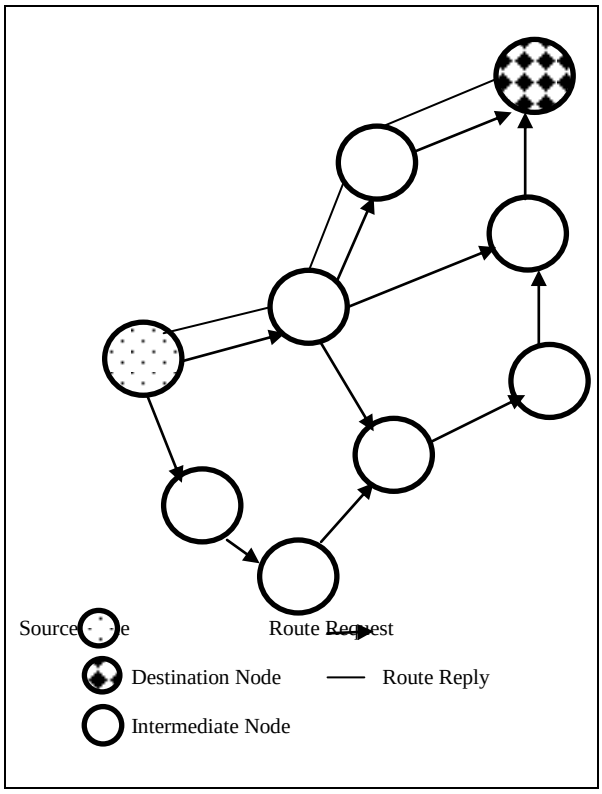

Fig.1: AODV Processing

6. PROPOSED WORK

The proposed work is an extension to Wormhole avoidance routing protocol (WARP) which determines whether the node that captures the route most of the time is really a wormhole node or is a true hot node. This is achieved by establishing a reputation on the node by all the neighboring nodes. The reputation is based on the trust value that is being established by the basic trust model.

6.1 Application of Trust Model

The trust model as described by Pirzada [6] is applied to the WARP protocol to overcome the limitation that the hot node which is treated as malicious node. On application of the trust model as proposed by Pirzada [6] to the Route Reply Decision Message of WARP and the basic RREP message of AODV helps in differentiating the hot node from the malicious node. The application of trust model to WARP applied to the Route ReplyDecision enables the network to arrive at a trust value that gives the reputation of the misbehaving node.

6.2 Algorithm for processing RREP

The algorithm for processing the route reply is an extension to the RREP processing of WARP, Worm Hole Avoidance Routing Protocol.

The proposed algorithm extends the RREP processing by adding the trust computation in order to establish the probability that a given node may be malicious. This is done by calculating the trust of a given node by its neighbor based on the behavior of the node. The behavior of any node, x is calculated for different categories such as acknowledgements received, number of route reply decision packets forwarded and route reply decision that are received, number of hello packets received, number of Destination unreachable messages received.

The existing RREP processing is enhanced with two algorithms WORMDETECT and CALCTRUST given in section 6.2.1 and 6.2.2 respectively. Section 6.2.1 is used to identify the nodes that are suspected as malicious node. Section 6.2.2 establishes the trust of any given node based on the basic trust model.

6.2.1 Algorithm WORMDETECT (i, j)

Let the intermediate Node i receives forwarded packet from node j. Let the source node be 'S' and the destination node be 'D'. Then the algorithm to detect the given node as a wormhole node is given as follows:

Step 1: Increment Route Reply count (RTE (j)) of node j in node I's routing table.

Step2:
If (RTE (j).RREP_DEC_COUNT/RTE (j).RREP_COUNT)>threshold then,
Node j may or may not be wormhole node
Go to step 3.
Else
Node is definitely not a wormhole node.
Go to step 6.

Step 3: Calculate the Trust worthiness of node j as determined by node I to determine if the node is really wormhole or a true node.
Calculate Ret=CALCTRUST (i, j)
If (Ret>mintrust)
Trust node j and keep forwarding packets
Else
Do not forward any further packets to node j.
Advertise Node j as malicious Node to all neighbor nodes.

Step 4: If RTE (D) does not exist, then create entry for D elsego to step 6.

Step 5: Check if hop count of Route reply<Available Hop count. If true, update the Hop count of destination with the new count.
RTE (D).hop count = RREP.Hopcount
RTE (D).Next hop=j;
Else
Drop Route reply packet.

Step 6: Select a neighbor node 'k' that has got a lesser hop count and node k's anomaly value< threshold value and T_i (k) is greater than threshold.

Step 7: Forward RREP to node k towards source node.

Step 8: Drop RREP and return

6.2.2 Algorithm CALCTRUST (i, j)

Equation (1) calculates the trust of a given node based on the Route reply decision messages received as follows by modifying the basic trust algorithm [2]:

$$T_i(j) = W_i(R_{RD}) * R_{RD} + W_i(B_L) \times T_i(B_L) + W_i(H_M) * H_M \quad \ldots\ldots\ldots (1)$$

Where,

W_i represents the weight assigned to a trust category by i and T_i is the situational trust of node i on node j in that trust category.

B_L tells whether the node belongs to the black list category as determined by AODV. B_L may take a value of zero or one. H_M is the number of Hello messages received. R_{RD} is the quantized value of the route reply decision messages and is given by the equation

$$Rrd = \begin{cases} \frac{Rrds - Rrdf}{Rrds + Rrdf}, & Rrds + Rrdf \neq 0 \\ 0, & otherwise \end{cases} \quad \ldots\ldots\ldots\ldots (2)$$

Where Rrds is the number of successful Route Reply Decision messages and Rrdf is the number of failure Route Reply Decision messages.

7. Simulation Results

The simulation is done using network simulator version2 (NS2).IEEE 802.11 is used as the MAC layer protocol. The network was set up with 10 nodes and the wormhole attack was performed on the so formed network which uses AODV as the routing protocol. The same network was simulated with the wormhole attack with the basic AODV protocol modified with the proposed solution and the results were analyzed. The trace files generated by both the simulations were used for analysis. The trace files so generated were loaded into XGraph tool for windows and the graphs were generated. The graphs generated proved the efficiency of our algorithm in terms of the number of packet losses.

The simulation started with the network being attacked by the wormhole nodes. The performance of the network was monitored. The results indicated the packet losses due to the wormhole attack. The same network was then simulated with the proposed algorithm as a countermeasure to the wormhole attack, which showed considerable improvement leading to reduction in the packet loss.

8. Performance Analysis

Fig.2 shows the packet drops by the wormhole nodes. The wormhole nodes are shown in red circles and they form a tunnel between them. Fig.3 shows the packet drops under AODV protocol and the proposed algorithm. The throughputs of the dropped packets were compared. Although the packet losses were high during the early stages of simulation, the proposed algorithm tends to show better performance than the AODV protocol throughout the simulation, except for the early stages.

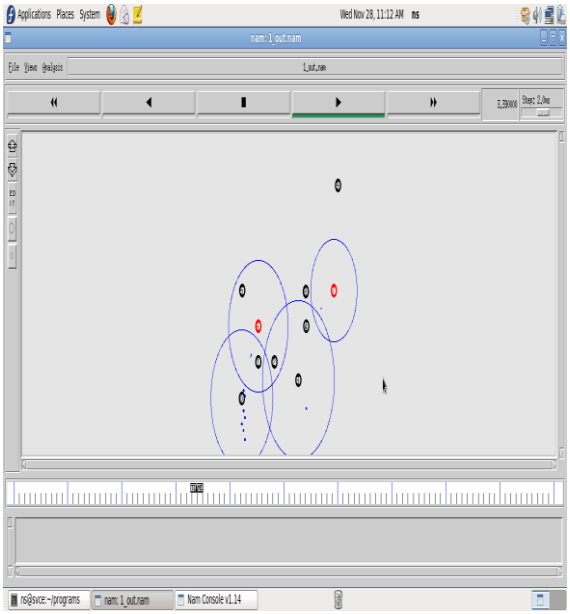

Fig.2: Simulation of Wormhole Attack

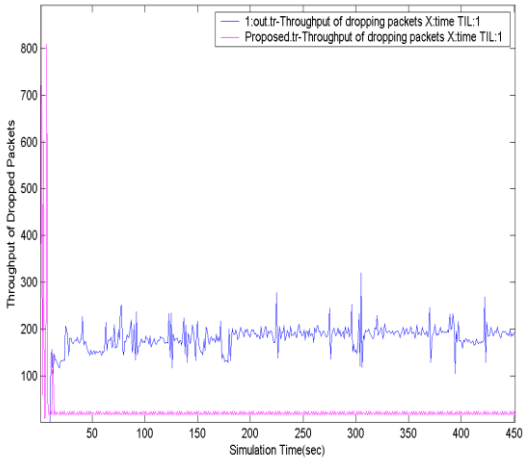

Fig.3: Simulation Time vs. Throughput

9. Conclusion and Future Work

As shown in the Fig.3, the number of packet drops is considerably reduced by the proposed algorithm despite of the fact that the numbers of packet losses were high initially. The proposed algorithm has to be enhanced to reduce this penalty of packet losses in the future.

10. References

[1] Ming Yang Su, WARP: Worm Hole Avoidance Routing protocol by anomaly detection in mobile adhoc networks in Computers and Security 29(2010).pp.208-224.

[2] Asad Amir Pirzada and Chris McDonald,Establishing Trust in Pure Adhoc Networks in 27th Australian Computer Science Conference, The University of Otago, Dunedin, New Zealand.

[3] C. Siva Ram Murthy and B.S.Manoj," Adhoc Wireless Networks Architectures and Protocols", Prentice Hall, 2004.

[4] Y. Hu, A. Perrig, and D. Johnson: Packet leashes: a defense againstwormhole attacks in Wireless Ad Hoc Networks. In Proceedings of theIEEE Conference on Computer Communications (Infocom), 2003.

[5] H.S. Chiu and K.S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," In Proc. International Symposium on Wireless Pervasive Computing, Phuket, Thailand, Jan. 2006.

[6] Tran Van Phuong, Ngo TrongCanh, Young-Koo Lee, SungyoungLee, and Heejo Lee. Transmission time based mechanism to detect wormhole attacks. In the proceedings of the IEEE Asia-Pacific service computing conference; 2007. pp. 172–8

[7] S.Marti, T. J. Giuli, K. Lai, M. Baker, "Mitigating Routing Misbehavior in Mobile Ad HocNetworks," Proc. of MobiCom 2000, Boston, August 2000.

[8] Network Simulator: http://www.isi.edu/nsnam/ns