CSWD - Clustering with Seek Packet for Wormhole Attack Detection and Elimination

Authors

Srishti Parashar¹, Pradeep Kumar²

¹M. Tech Student, CSE Department, JSS Academy of Technical Education, Noida (U.P.), India
²Assistant Professor, CSE Department, JSS Academy of Technical Education, Noida (U.P.), India

Email: innovationthroughout@gmail.com¹, pradeep8984@jssaten.com²

ABSTRACT

A Mobile Ad-hoc Network (MANET) is a collection of independent wireless mobile nodes for communication without any established infrastructure. Due to unique characteristics such as dynamic topology, limited bandwidth, and limited battery power make them vulnerable to security attacks. One of the routing protocol attacks, wormhole attack is hard to catch but easy to implement in network with help of tunnelling. This attack can launch a variety of attacks against the data traffic flow such as selective dropping, replay attack, denial of service, packet modification once launched in the network. In this paper, we present an algorithm CSWD for detection and elimination of wormhole attack from the network. A concept called seek packet is used to detect and clustering will eliminate wormhole attack from the network. The algorithm will be implemented in base protocol ZRP (zone routing protocol) which has not been done so far. ZRP will reduce overhead of cluster formation simply with help of zone radius. The algorithm would be implemented using ns2 (network simulator) on Ubuntu OS.

Keywords- MANET, Wormhole Attack, Seek packet, ZRP, Clustering

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is an autonomous group of mobile users that form temporary network architecture for communication without any established infrastructure or centralized mechanism. Mobile nodes are distributed and communicate via radio waves quickly, dynamically and spontaneously shown in Fig 1.

In a MANET, nodes are free to move anywhere in the network or out of the network and organize themselves into a network. MANET does not require any centralized controlling mechanism such as base stations therefore it is a striking networking option for connecting mobile devices quickly, dynamically and spontaneously. The network topology may vary rapidly and unpredictably, because the nodes are mobile. The network is decentralized in nature, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality has to be incorporated into the mobile nodes. There are three types of routing protocols in MANETs Proactive, Reactive and Hybrid.

Fig 1: Basic infrastructure of MANETs

Ad-hoc network are more vulnerable to the safety attacks as compared to wired network or infrastructure based wireless network due to their distributive nature. Security Attacks on the ad-hoc
network can be classified into two broad categories:

**Passive Attacks** – These attacks don't disrupt the conventional operation of the network, the attacker sleuth the data changed within the network while not altering it. Here the need of confidentiality gets violated. Traffic analysis, eavesdropping are some passive attacks.

**Active Attacks** – Active attacks makes an attempt to alter or destroy the data being changed inside the network there by disrupting the traditional functioning of the network. Active attacks, whether or not administrated by an external advisory or an internal compromised node involve actions such as interception, modification, fabrication and duplication.

Wormhole attack is one of the active attacks is finished by two or a lot of malicious nodes with conspiracy. Just in case of wormhole attack, two malicious nodes at totally different locations communicate to every alternative via a secrete channel. Thus the two malicious nodes are settled far from one another and that they initiate to be among one-hop count communication range. Primarily this secret tunnel is incredibly long as compared to traditional root from supply to destination however it's logically suppose united hop count shown in Fig 2.

![Fig 2: Wormhole attack in network](image_url)

The Wormhole attack can be classified in two main types: Hidden attacks and Exposed attacks, depending on whether wormhole attacker nodes put their identity into packets headers when tunnelling & replaying packets.

**Hidden Attacks** - Wormhole attacker nodes do not update packets headers so other nodes do not realize the existence of them. In this kind of attack, a path from S to D via wormhole attacker link will be:

$$S \rightarrow E \rightarrow K \rightarrow D$$

**Exposed Attacks** - In exposed attacks, wormhole nodes do not change the content of packets but they include their identities in the packet header as trustworthy nodes do.

In case of exposed attacks, the path from S to D via wormhole will be:

$$S \rightarrow E \rightarrow W1 \rightarrow W2 \rightarrow K \rightarrow D$$

If the wormhole can solely peacefully transport all the traffic from one location within the network to a different location that's isolated, then it may be helpful for the network operation because it will improve the network connectivity. Unfortunately if once the traffic is routed through the wormhole, the attacker can gain full management over the traffic. Then he will begin his malicious actions by selection dropping data packets which is able to lower the network throughput or store all the traffic and later perform cryptanalysis attacks.

The remaining paper is organized in sections. Section - II briefs about related work done and techniques used for detection of wormhole attack moreover the proposed architecture and algorithm is discussed in section – III followed by Conclusion and future aspects mentioned in section – IV. References included in section – V that’s used in end of this paper.

### 2. LITERATURE SURVEY

Various solutions have been proposed by researchers to detect and analyse the impact of wormhole attack.

Hu et al. in his paper [14] introduced a concept of Packet Leashes method to defend against the
wormhole attack. Leash is basically a additional information which is added with the packet for detection. Two types of leash information were used Geographical Leash and Temporal Leash. To implement temporal leashes, an efficient protocol, called TIK was presented which also provides instant authentication of received packets. The drawback of paper was that packet leashes do not identify malicious nodes.

Nicklas Beijar presented a hybrid protocol ZRP (zone routing protocol) in his paper [15] which combines two different routing methods proactive and reactive protocol approach into one protocol. The proactive component IARP (intra-routing protocol) maintains up-to-date routing tables within the routing zone. Outside the routing zone routes are discovered using reactive component IERP (inter-routing protocol) using route requests and replies. Using border casting, query detection, ZRP reduces the traffic amount compared to pure proactive or reactive routing. The advantage is routes to nodes within the zone are immediately available and ZRP is able to identify multiple routes to a destination, which provides increased reliability and efficiency and ensures that the routes are free from loops. It is a flat protocol which handles traffic well reduces congestion, overhead and is usually targeted for large networks. ZRP performs better than any single proactive or reactive protocol.

Debdutta Barman Roy et.al in his paper for mobile ad-hoc network [10] proposed an algorithm where intrusion detection has been done in a cluster based manner to detect wormhole attack in network. The AODV routing protocol is used as the underlying topology. They used a two layer approach which was introduced to reduce the load of processing on each cluster heads for detection of wormhole. Also from security point of view, this will reduce the risk of a cluster head being compromised. The proposed solution unlike some of its predecessors does not require any special hardware components like directional antennas, etc. for detecting the attackers. The drawback of this paper was it could not identify the exact nodes which were making wormhole in the network.

Saurabh Gupta et.al in paper [8] proposed a routing protocol WHOP (Wormhole Attack Detection Protocol using Hound Packet), based on AODV protocol. The protocol can efficiently find wormhole in the network and also the nodes that were making the wormhole. The Principal working of WHOP is to take the help of others nodes who were not involved in RREQ path after the path has been discovered to found worm hole in the network. After the source node receives RREP packet, it creates an additional packet called Hound Packet, before forwarding this packet source computes its Message Digest and signed the MD with own private key and attached this information with hound packet. At destination it calculates the hop difference based on processing bit and CRNH (count to reach next hop) field. If it exceeds the acceptable level wormhole is detected in the path. The paper presents an excellent approach to detect wormhole nodes, the only drawback was high processing delay due to hound packet calculation at each and every node.

Yahya Ghanbarzadeh et.al [7] has proposed a method that can avoid against wormhole attack on ad hoc networks. For avoiding wormhole attack in these networks, they proposed special packet with name WADP packet. When a particular node suspect any route, will send a WADP packet to his cluster head node and that cluster head will further broadcast that packet to all neighbour cluster heads and their cluster members. Member nodes that receive WADP packet updates their routing table by dropping wormhole route from their table. In this way they can avoid from wormhole attack. Also for security they used the concept of sending a private key to destination from a route that is bigger than the shortest route and reduce cost of sending packets. The proposed method detects unsecure routes that can be created by malicious nodes.

In paper [1] a more efficient Routing Protocol named Wormhole attack Detection Protocol using
Time Stamp with Security Packet. W-TSP allows to the receiver to check whether there are any malicious nodes sitting along its paths from sender to receiver and try to launch wormhole attacks. We obtain the average delay time and total hop count details of paths between the sender and the receiver and use this information to indicate that wormhole attack is subjected in this selected path among. The advantages of W-TSP are that it does not require any special hardware and clock synchronization.

3. PROPOSED WORK

Our proposed work will detect and eliminate wormhole attack if it exists in the network using a concept of Seek packet and clustering in ZRP. Our proposed work is divided in mainly three main modules:

3.1 Module 1- Path Discovery using Centrality

In path discovery process Source will send RREQ and search for destination using IARP and IERP component of ZRP. Shortest path will be calculated based on centrality [6] and RREP will be sent back to source node.

Computation of Centrality: Source node S sends a RREQ message including the size of its routing table as its centrality:

$$E_1 = \text{size (rtable(S))}$$

Upon receipt of this message, neighbor node V1, not knowing a route to the solicited destination, acquires $$p(n) = p(1)$$ and $$n=1$$ from the received RREQ message and diffuses a modified replica with the novel average centrality:

$$E_2 = \frac{1}{2} E_1 + \frac{1}{2} \text{Size of (rtable(X1))}$$

Iteratively, for an nth intermediate node, the novel average eccentricity:

$$E_{n+1} = \frac{n}{n+1} E_n + \frac{1}{n+1} \text{Size of (rtable(Xn))}$$

Finally, when destination node D receives messages from various possible paths to S, it simply chooses the route having smallest average centrality. Centrality will find the shortest path efficiently and effectively by minimizing the process of broadcasting by each node.

3.2 Module 2- Seek packet for wormhole attack detection

For wormhole attack detection we have introduced a concept of Seek packet sent from source to destination after the path discovery. At destination seek packet is calculated based on some fields and comparison is done and informed to respective cluster head if presence of wormhole is detected. The structure of Seek packet is shown in Table I. Additional fields used are:

- **R/W FLAG**: R/W flag is added to check if any node in the path tries to modify or write something this field will get cleared.
- **TIMESTAMP**: If Seek_ack is not received from destination to source within given time period source has to send seek packet again.
- **EXPECTED RTT**: Source will calculate the value and put the value in Seek packet so that destination can check the presence of wormhole in the respective path.
- **LAST HOP**: Last hop field will let us know the last neighbour who sent the packet.

**Table I: Seek Packet Structure**

<table>
<thead>
<tr>
<th>Type</th>
<th>R/W Flag</th>
<th>Reserved</th>
<th>Timestamp</th>
<th>Total hop count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source sequence no</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination sequence no</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address[n-1]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address[n]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expected RTT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Hop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dummy Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.3 Module 3 - Clusters and cluster-head selection for wormhole node elimination

From security point of view Clustering plays an important role in MANET. A better way to support the increasing number of nodes in MANET is to subdivide the whole network into clusters giving the network a hierarchical organization. In our paper clustering is done with the help of ZRP (zone routing protocol). The
clusters are taken with respect to zones radius which is initially taken as two. So number of clusters defined will be two. It can be extended to three, four with respect to zone radius.

Since there is no central administrative control of MANET Cluster head play an important role as it is responsible for managing and controlling each cluster. The responsibility of the cluster head (CH) is to communicate with all the nodes of its own cluster. However CH must be able to communicate with the nodes of other clusters as well, which can be directly or through the respective CH or through gateways. Communication is done in three steps. First of all the cluster head receives the data sent by its members, secondly it compresses the data, and finally transmits the data to the base station or other CH. Electing a specific node as a cluster head is a very important but sophisticated job. Various factors can be considered for electing the best node as a cluster head. Some of these factors include location of the node with respect to other nodes, mobility, energy, lowest id basis, highest id basis trust, and throughput of the node. One cluster head per cluster must be selected during an election process, because multiple cluster heads within a single cluster can give rise to cluster reformation, Quality of Service and routing management issues.

Cluster head election initially in our paper will be done on the basis of minimum node id. Cluster head maintains a cluster head detection table (CHD) for wormhole detection. When destination informs the presence of wormhole in the path respective CH will add the path in its detection table. When the threshold exceeds the limit wormhole is detected. CH will inform other CH and their respective member nodes to drop that particular node from their routing table.

Fig 4: Block Diagram for Detection and Elimination Algorithm of Wormhole in MANET

Algorithm description of wormhole detection and elimination

1. Initially clusters are defined for whole network based on zone radius of the zone routing protocol. Cluster may contain arbitrary number of nodes.
2. After the network is defined in form of clusters path discovery is done by sending route request packet by source node which will be broadcasted by all the intermediate nodes. Various nodes will send route reply packet back to source node.
3. From all the route replies shortest path will be discovered using the concept of centrality in which each node will add its size of routing table and previous node’s routing table size. At destination all the paths are processed and path which has shortest centrality is chosen.
4. When path is selected hello packet is sent from source to destination to initiate communication process and source starts timer T1. Destination will send acknowledgement to source using time T2. Expected RTT (round trip time) of hello packet is calculated at source as: EXP-RTT = T2-T1
5. Source will send seek packet to destination. At destination seek packet is processed and actual RTT is calculated. If actual RTT>EXP-RTT then wormhole exists in path and an ACK is sent to source.
6. Source will select second shortest path based on centrality and step 4 and 5 are repeated. If again
wormhole exists in path then detection of nodes are done which are making wormhole
7. Wormhole nodes are detected based on cluster head detection table maintained by cluster head shown in Table II. After second path when threshold exceeds cluster head declares the node as wormhole node.
8. After node detection cluster head will inform its member nodes to delete that node’s id from their routing table. In this way wormhole nodes will be eliminated.

Table II: Cluster head – Detection Table
Considering No of wormhole nodes and Th value= 2

<table>
<thead>
<tr>
<th>NODE ID’S</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2(wormhole)</td>
</tr>
<tr>
<td>4</td>
<td>2(wormhole)</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

4. CONCLUSION AND FUTURE SCOPE
Our proposed work for wormhole attack detection and elimination is based on concept of Seek packet and clustering. The theoretical analysis of our proposed algorithm would provide attack detection with lesser processing delay as compared to the earlier work. Clustering will be used for making clusters in base protocol and drawback of hound packet will be eliminated using Seek packet. The algorithm would be implemented using ns2 (network simulator) on Ubuntu OS. Aim of our algorithm is detection and elimination of wormhole so that the effectiveness and efficiency of network can be improved. As future work, we intend to optimize the Seek packet and make it more efficient and effective in tracking the movement of dropping packets. We also plan to analyse the proposed algorithm in our base protocol ZRP which has not been done so far.

5. ACKNOWLEDGEMENT
The author would like to thank the faculty of Compute Science and Engineering Department, JSSATEN for their valuable guidelines and support.

REFERENCES


