WORMHOLE ATTACK MITIGATION IN MANET: A CLUSTER BASED AVOIDANCE TECHNIQUE

Subhashis Banerjee[1] and Koushik Majumder[2]

Department of Computer Science & Engineering,
West Bengal University of Technology,
Kolkata, India

ABSTRACT

A Mobile Ad-Hoc Network (MANET) is a self configuring, infrastructure less network of mobile devices connected by wireless links. Loopholes like wireless medium, lack of a fixed infrastructure, dynamic topology, rapid deployment practices, and the hostile environments in which they may be deployed, make MANET vulnerable to a wide range of security attacks and Wormhole attack is one of them. During this attack a malicious node captures packets from one location in the network, and tunnels them to another colluding malicious node at a distant point, which replays them locally. This paper presents a cluster based Wormhole attack avoidance technique. The concept of hierarchical clustering with a novel hierarchical 32-bit node addressing scheme is used for avoiding the attacking path during the route discovery phase of the DSR protocol, which is considered as the under lying routing protocol. Pinpointing the location of the wormhole nodes in the case of exposed attack is also given by using this method.

KEYWORDS

MANET, Wormhole Attack, DSR, Hierarchical Clustering.

1. INTRODUCTION

Mobile Ad-hoc Networks (MANET) is a highly challenged network environment due to its special characteristics such as decentralization, dynamic topology and neighbour based routing. This type of network consists of nodes that are organized and maintained in a distributed manner without a fixed infrastructure. These nodes, such as laptop computers, PDAs and wireless phones, have a limited transmission range. Hence, routing is essentially multi-hop in case of mobile ad hoc networks. Since the transmission between two nodes has to rely on relay nodes, many routing protocols [1-4] have been proposed for ad hoc networks. Most of the routing protocols, however, do not consider the security and attack issues because they assume that other nodes are trustable. This lack of security mechanism provides many opportunities for the attackers to conduct attacks on the network. And also, the lack of infrastructure, open nature of wireless communication channels, rapid deployment practices, and the hostile environments in which they may be deployed, make them vulnerable to a wide range of security attacks described in [5-7].

In this paper we investigate a specific type of attack, known as Wormhole attack. It is a network layer attack which is relatively easy to mount, while being difficult to detect and prevent. During the attack a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally, this is illustrated in figure 1.

In the ad-hoc network in figure 1, we assume that S, A, B, C, E, F, D are the legitimate nodes and X and Yare the malicious nodes. S can communicate with D using the path S–A–B–C–E –F–D.

DOI : 10.5121/ijcnc.2014.6104

For conducting the wormhole attack successfully the attacker places the malicious nodes X and Y close to S and D. Then the attacker makes S and D think that they are neighbours of X and Y like this - X captures the packets sent by S, tunnel the packets to Y, Y replays the packets to D. From then on, S and D use the malicious link for communication. Thus, the attacker has successfully mounted the wormhole attack on the network.

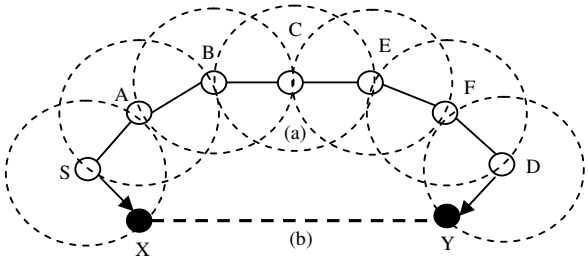

Figure 1. Wormhole attack in ad hoc networks: (a) Normal ink (b) Wormhole link

In this paper we have proposed a cluster based Wormhole attack avoidance mechanism. At first the hierarchical clusters are formed up to 3-level, and during the cluster formation a unique 32-bit hierarchical address is assigned to each nodes within the cluster boundaries. With the help of the hierarchical addressing scheme the receiver can compute the intermediate nodes address in a valid path on the receiving of a packet. So when it receives a route request packet from the sender it can check for all valid addresses in the packet. If some mismatch occurs it reports this path as an attacking path and avoids the path in case of further communication.

The remaining paper is organized as follows: in section 2 we give the literature review. In section 3 we give our proposed scheme with our assumptions and cluster formation technique and at the end of this section we give the data structures used by the proposed algorithm. Different types of wormhole attacks and there countermeasures have been given in section 4 and 5. The complete algorithm in pseudo code is present in section 6. And we finally conclude the paper in section 7.

2. RELATED WORKS

According to the literature survey we found that we can classify the proposed Wormhole attack detection and prevention techniques in 1) Location and Time Based Solutions 2) Hop-Count Analysis based Schemes 3) Special Hardware-based Solutions 4) Statistics- Based Solutions 5) Neighbour-Based solutions and 6) Clustering based solutions.

Y. Hu et al. in [8] introduced the first location and time based Wormhole detection and prevention scheme called the Temporal Leashes and Geographical Leashes. According to Temporal Leashes while sending a packet at local time ts, the sender needs to set the packet expiration time to $te = ts + L / c - \Delta$ (All nodes are time synchronized up to a maximum time synchronization error Δ and c is the propagation speed of wireless signal) in order to prevent the packet to travel further than distance L. When the receiver gets the packet at local time tr, it further processes the packet if the temporal leash is not expired (i.e., $tr < te$), otherwise it drops the packet. According to the Geographical Leashes while sending the sender includes in the packet its own location, ps, and the time at which it sent the packet, ts. After receiving the receiving node compares these values to its own location, pr, and the time at which it received the packet, tr. If v is an upper bound on the velocity of any node, then the receiver can compute an upper bound on the distance between the sender and itself, dsr like this: $dsr \leq \| ps - pr \| + 2v (tr - ts + \Delta) + \delta$ (Assume that the clocks of the sender and receiver are synchronized to within $\pm\Delta$). Though both of the Leashes are reliable and have a high detection rate Temporal Leashes suffers form need of tightly

synchronized clocks and the Geographical Leashes suffers from some hardware need like GPS information.

W. Wang et al. proposed a more generic approach in [9] for end-to-end wormhole detection mechanism on a multi-hop route. In this mechanism all intermediate nodes will attach its timestamps and positions to the detection packets. After receiving a detection packet, the destination will check for the validation of the packet. If many consecutive detection packets are all lost or a wormhole is detected, then the destination node will broadcast a message which notifies the source to abort the current route and reinitiate the process.

Xia Wang et al. proposed another end-to-end detection of wormhole attack called EDWA [10]. EDWA is a simple comparison based method for wormhole detection and prevention. Based on the estimated shortest path and the actual shortest path and is used to determine whether there is a wormhole attack for each received route.

S. Jen et al. proposed simple Hop-Count Analysis based scheme [11] for avoiding Wormhole attacks in MANET called MHA. MHA uses the observation that the route under the wormhole attack has a smaller hop-count than normal. As a result, users who avoid routes with relatively small hop-counts can avoid most Wormhole attacks. MHA has two phases. In the first phase it examines the hop-count values of all routes. Then a safe set of routes is chosen for data transmission. Finally, it randomly transmits packets through safe routes. Even if the wormhole is not avoided in some severe cases, it can still minimize the rate of using the route path through the wormhole.

Delay per Hop Indication (DelPHI) [12] is another hop count analysis based solution that uses delay as a parameter for detecting Wormhole attack in MANET. The detection mechanism uses the delay/hop value for detecting wormhole attacks. The reason behind that under a wormhole attack, the delay that a packet experiences for propagating across false neighbours should be unreasonably high since there are in fact many hops between them. Therefore, we observe that if we compare the delay per hop of a legitimate path with the delay per hop of a path that is under wormhole attack, we should find that the delay/hop of the legitimate path is smaller. Therefore, if a path has a distinguishable high delay/hop value, it is likely to be subjected to a wormhole attack.

L. Hu et al. presents an analysis of wormhole attacks and proposes a countermeasure using directional antennas [13] based on the observation that an attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbour and its messages are ignored.

S. Capkun et al. proposed another wormhole prevention technique, called “Secure Tracking of Node Encounters in Multi-hop Wireless Networks” (SECTOR) somewhat similar to “packet leashes” [14]. In SECTOR node A can estimate the distance to a node B based on the speed of data transmitted between them. Each node uses a special hardware that enables fast sending of one-bit challenge messages without CPU involvement to minimize all possible processing delays. By using the time of flight, A detects whether or not B is a neighbour.

The hardware based solutions introduce minimal Communication overhead but need some special h/w support which is a major drawback. Some methods also need some cryptographic support.

N. Song et al. [15] proposed another detection technique for detection of the wormhole attacks called a simple scheme based on statistical analysis (SAM). They mainly consider the relative frequency of each link appearing in the set of all obtained routes. They calculate the difference between the most frequently appeared link and the second most frequently appeared link in the set of all obtained routes. The maximum relative frequency and the difference are much higher under

wormhole attack than that in normal system. The two values are used together to determine whether the routing protocol is under wormhole attack.

Two statistical approaches to detect wormhole attack in Wireless Ad Hoc Networks have been introduced in [16]. The first one, called Neighbour Number Test is based on a simple assumption that a wormhole will increase the number of neighbours of the nodes (fake neighbours) in its radius. The base station gets neighbourhood information from all sensor nodes, computes the hypothetical distribution of the number of neighbours and uses statistical test to decide if there is a wormhole or not. The second one called All Distance Test which detects wormhole by computing the distribution of the length of the shortest paths between all pairs of nodes. In these two algorithms, most of the workload is done in the base station to save sensor nodes' resources. However, one of the major drawbacks is that they cannot pinpoint the location of wormhole which is necessary for a successful defence.

The main drawback of the above statistical analysis based solutions is that it can detect routing anomaly as long as sufficient information of routes is available.

Wormhole Attack Prevention Algorithm (WAP) [17] is a neighbour monitoring based solution. In WAP all nodes monitor their neighbour's behaviour when they send RREQ messages to the destination, to detect neighbours that are not within the maximum transmission range but pretend to be neighbours. When a source node sends RREQ it starts a wormhole prevention timer (WPT). If it receives some RREP messages after the timer got expire it detects a route under wormhole attack among the routes. Once wormhole node is detected, source node records them in the Wormhole Node List.

In [18] authors proposed a routing protocol WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on AODV protocol. It can efficiently find wormhole in the network and also the nodes that were making the wormhole. For identifying a wormhole in the path, sender node creates Hound packet, which contains the identity of all nodes which have been used for forming route from source to destination node in recently identified path. Then the source sends the hound packet. Each node in the network forwards the hound packet instead of nodes whose ip address listed in the packet. After different hound packets are reached at the destination node, it calculates the hop difference between neighbours based on the received values of the hound packets and detects the wormhole if the hop difference exceeds the acceptable level.

All the neighbour monitoring based solutions are less energy efficient. Because at the link layer, it assumes that a node can always monitor ongoing transmissions even if the node itself is not the intended receiver that consumes more power from the node, and nodes are died out very quickly.

D. B. Roy et al. proposed the first cluster base Wormhole attack detection method [19]. They divided the entire network in clusters. Each cluster has a cluster head and there is a guard node in the intersection of two overlapping clusters. Guard node has the responsibility to monitor the communication between the clusters that are adjacent to the guard node, and if malicious activity is found the guard node reports to the cluster head of the respective layer. A cluster head in the inner layer detects a malicious activity and informs the cluster head of the outer layer, and then the outer layer cluster head has the responsibility to inform the other nodes in the network about the malicious nodes.

The proposed cluster based organization reduces the load of processing on each node because it uses guard nodes for monitoring purpose and the cluster heads for the Wormhole detection purpose. The cluster head also has the responsibility to inform the other node about the wormhole nodes. D. B. Roy et al. did not provide a practical method for cluster formation, the cluster head selection and the guard node selection. Also the method cannot pin point the location of the

wormhole nodes and needs a separate phase for Wormhole attack detection after the guard node observes a malicious activity. Their method can only detect the single Wormhole attack multiple Wormhole attack cannot be detected by this method.

This paper presents a cluster based Wormhole attack avoidance technique. We only use the cluster heads for the monitoring purpose and also select the cluster heads dynamically based on some parameters, that distributes the lodes among all the nodes within the cluster. Our method does not require an extra phase for the wormhole detection during the DSR route discovery the receiver can detects the wormhole if there is any. Our method is also capable to avoid multiple Wormhole attack, and in the case of exposed attack it also pinpoints the location of the wormhole nodes.

3. PROPOSED SCHEME

In this paper we have proposed a cluster based Wormhole attack avoidance mechanism. Where the receiver can identify whether there is a wormhole in the routing path during the route discovery phase in DSR, the routing protocol we use. As a result the sender and the receiver can avoid the compromised path during the path setup step, and no further checking for Wormhole attack is required during communication.

3.1. Assumptions

In this section we outline the assumptions that we make regarding the properties of the physical and the network layer and the organization of the ad-hoc network. The assumptions are:

1. We consider a hierarchical cluster model (up to level-3), where the entire network is geographically divided into disjoint or overlapping level-0 clusters. The upper layers are used for organizing the cluster heads of the layer below it.
2. The destination node should wait until a RREQ packet with a valid routing path has been received. A path is valid if it contains all the cluster heads ids. According to the characteristic of the Wormhole attack the attackers are communicating using some low latency link, so packets that are coming through a wormhole link will reach the destination fast than other packets which are coming through valid long paths. So for validation and identification of the Wormhole attack the destination needs some packets which are coming through some valid path.
3. Though we are using the conventions of the DSR routing protocol, the destination does not sends the RREP through the path that has minimum hop count value like DSR. We do this because in case of a wormhole attack the malicious nodes always try to advertise a path which has low hop count value. So in order to avoid this we will select a valid path which avoids the malicious nodes, but as a consequence it may reflect in a large hop count value.
4. In the proposed cluster based model every cluster is monitor by a power full node called the cluster head of this cluster. So we assume that some of the mobile nodes have more capacity (like more remaining power, low mobility) than other nodes in the network.
5. We assume that the nodes are communicating by using the proposed 4 byte hierarchical addressing, in the format X.Y.Z.W where X is the level-2 cluster head id, Y is the level-1 head id, Z is the level-0 head id and W is the node id (will be described in detail in the cluster formation section).
6. Cluster head selection is the crucial part of our method, and it should be selected according to the criteria described in the cluster formation section, such that a malicious node cannot be selected as a cluster head.

In this paper we propose a cluster based hierarchical mobile ad-hoc network model shown in figure 2, for avoiding the Wormhole attack. The cluster formation technique is described in the section bellow.

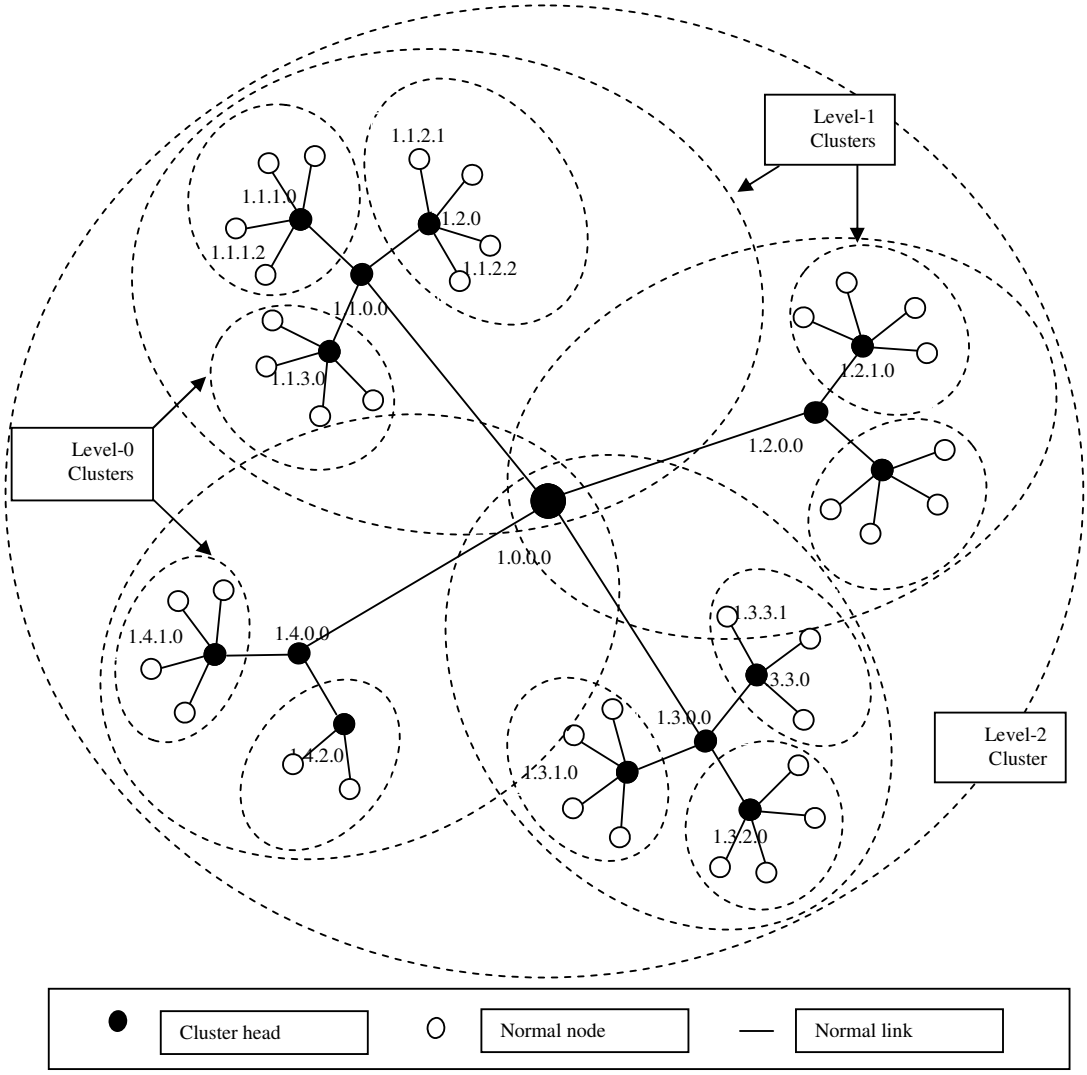

Figure 2. Hierarchical cluster formation and addressing

3.2. Cluster formation

3.2.1. Hierarchy Definition

Here we consider a hierarchical (up to level-3) cluster model as described in [20]. All mobile nodes are first grouped into few disjoint level-0 clusters, and among them one node is selected as the cluster head (we will describe the cluster head selection criteria in "3 Cluster head selection"). All nodes in the cluster are in the direct communication range from the cluster head. All the level-0 clusters are grouped into few overlapping level-1 clusters and in every level-1 cluster a node is selected as the cluster head of that cluster. The same procedure as level-0 is applied for selecting the level-1 cluster heads. Then the level-1 clusters are grouped into level-2 clusters, where one of

the nodes from the level-1 clusters that qualify the cluster head selection criteria is selected as the level-2 cluster head.

3.2.2. Hierarchical Node Addressing

Here we introduce a novel hierarchical addressing scheme for the nodes in the network. In the next section we will use the addressing scheme for detecting and preventing the Wormhole attack. All cluster heads at level-2 will get the address in this format X.0.0.0. The level-1 cluster heads will get the address like X.Y.0.0. The level-0 cluster head address is in the format X.Y.Z.0. And finally the nodes in the level-0 cluster will get the address in the format X.Y.Z.W where X, Y, Z, and W are any integer from 0 to 255. So if a level-1 cluster head has the address 1.25.0.0, then the level-0 cluster heads which are under the level-1 cluster head have the address like 1.25.Z.0, where Z is any integer from 0 to 255. The first byte in the address specifies the level-2 cluster head id; second byte represents the level--1cluster head id; third byte represents level-0 cluster head id and fourth byte represents the node id.

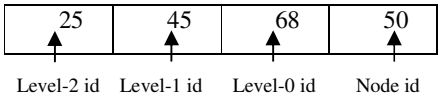

Figure 3. Hierarchical address format

3.2.3. Cluster Head Selection

The cluster heads at level-0 are selected according to the following criteria:

1. *Remaining Power:* In order to ensure event dissipation of power by all the nodes and for increasing the overall network life time we need to select the cluster heads from among the nodes periodically on the basis of the maximum remaining power of a node power.
2. *Reliability:* A node is a reliable one if other nodes in the network previously route the packet through it. As we are considering the DSR as the underlying routing protocol, the sender get the intermediate nodes ids in the route path from the Address[i] field in the RREP packet described in section 4.3. In our approach each node should maintains a Neighbour_Reliability table (described in section 4.3) that stores the node id and the reliability value i.e., how many times it route packet via this node by using the RREP path information. During the cluster head selection all nodes in the cluster exchange the Neighbour_Reliability table among them and the node that satisfy the 'maximum remaining power' and the 'low node mobility' constraints and has the maximum reliability value will be selected as the cluster head.
3. *Node Mobility:* Node with the low mobility is selected as the cluster head. If the cluster head change its link to other nodes very frequently then we have to select a new cluster head. To select the new cluster head nodes should run the cluster head selection procedure, which introduces some computational overhead as well as some communicational overhead due to exchanging the Neighbour_Reliability table described in section 4.3.

3.2.4. Cluster Creation

Once the cluster head has been selected it creates the HELLO packet, and set its TTL value to 1. Then flood the packet to discover all 1-hop neighbours. Then it creates a level-0 cluster. To organize the level-0 clusters level-1 clusters are created. At first the cluster head has been selected

then it discover its one hop adjacent level-0 cluster heads using the same HELLO packet flooding described above. After level-1 clusters have been created they create the level-2 clusters using the same technique described above.

Now we describe the data structures which will be used by the Wormhole attack avoidance algorithm described in section VI.

3.3. Data Structures

Before presenting the algorithm for avoiding the Wormhole attack, we first describe the data structures that we use for efficient implementation of the algorithm.

1. *Neighbour_Reliability table:*

   It has two columns, 1) The node id and 2) The reliability value.

When a node receives an RREP packet it extracts all the intermediate node ids from it, then stores the node id in the node id column if not present in the table. Then it initializes all the new nodes reliability value to 1, and increments previously stored nodes reliability by 1.

2. *Direct_Neighbour list*: Each cluster heads sores a list that contains the id of all it direct neighbouring cluster heads. The cluster heads periodically updates the list by broadcasting the HELLO packet with hop count =1.

3. *Hierarchical addressing structure:* Each nodes address consists of three fields: Node id, Level-0 id, Level-1 id and Level-2 id. The size of an address is 4 bytes. Each field can take any value from 0 to 255. Figure 4 represents a hierarchical address.

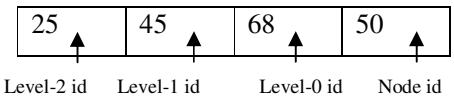

Figure 4. Hierarchical address format

4. *DSR packet format:*

IP Header	Transport Layer Data

Figure 5. Standard IP Header

Version	IHL	Type of Service	Total Length			
Identification				DF	MF	Fragmentation offset
Time to Live		Protocol	Header Checksum			
Source Address						
Destination Address						

Figure 6. IP Header Format

IP Header	DSR Header	DSR Option	Transport Layer Data

Figure 7. IP packet with DSR information

Option Type	Opt Data Len	Identification
Target Address		
Address[1]		
…		
Address[n]		

Figure 8. DSR Route Request Option (RREQ) format

	Option Type	Option Data Length	L	Reserved
Address[1]				
Address[2]				
…				
Address[n]				

Figure 9. DSR Route Reply Option (RREP) format

4. DIFFERENT TYPES OF WORMHOLE ATTACKS ON THE PROPOSED CLUSTER BASED MODEL

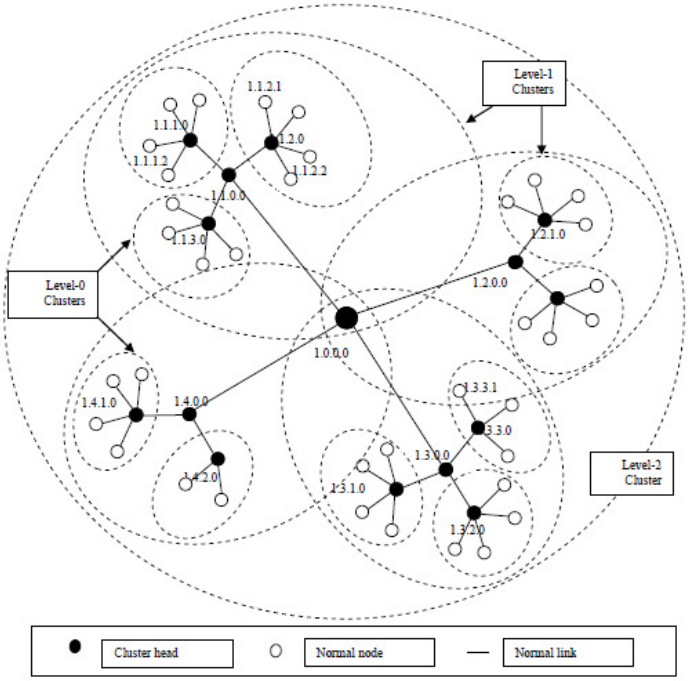

Figure 10. Different type of Wormhole attacks on the proposed model.

Our proposed hierarchical cluster based mobile ad-hoc network model is susceptible of the following four types of attacks:

1. *Intra cluster Wormhole attack*
2. *Inter level-0 Intra level-1 cluster Wormhole attack*
3. *Inter level-0Inter level-1 Wormhole attack*
4. *Inter level Wormhole attack*

All the 4 types of attacks are shown in figure10.

4.1. Intra Level Intra Cluster Wormhole Attack

In intra level intra cluster the two malicious nodes belongs to the same cluster and they establish wormhole link between them.

Example: In figure 11, two malicious nodes X and X' create wormhole link between them within the cluster. When the sender 1.1.2.1 wants to communicate with the destination 1.1.2.2, it broadcasts RREQ packet. The RREQ packet is received by both the cluster head 1.1.2.0 and the malicious node X. After that X encapsulates it and tunnels it to the other malicious node X'. X' then forwards it to the destination 1.1.2.2. The encapsulation is done by X so that hop count of the packet does not increase and destination node thinks the source to its closed neighbour. For this the route through the malicious node seems to be low hop count path. Afterwards the malicious nodes either drop the packets or spying on the content of the packets going through them.

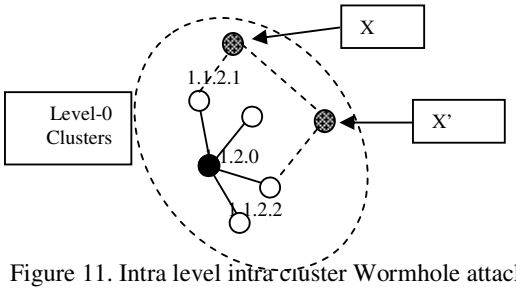

Figure 11. Intra level intra cluster Wormhole attack

4.2. Inter Level-0 Intra Level-1 Cluster Wormhole Attack

In this attack the wormhole link is created between two malicious nodes that are in two different level-0 clusters but within same level-1 cluster.

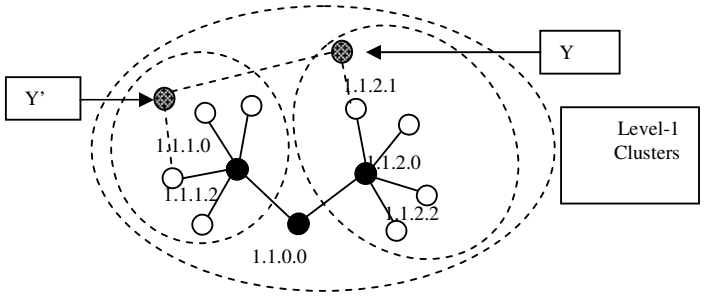

Figure 12. Inter level-0 Intra level-1 cluster Wormhole attack

Example: In figure 12, 1.1.2.1 and 1.1.1.2 are sender and receiver respectively (which are in the same level-1 cluster but belong to two different level-0 clusters). The wormhole link is created

between them by using two malicious nodes Y and Y'. The sender 1.1.2.1 floods RREQ packet to initiate route discovery. After receiving the packet Y encapsulates it so that hop count remains same and sends it to Y'. Then Y' forwards it to destination 1.1.1.2. As the path seems to have lesser hop count it may be selected. In this way the attack is successfully launched.

4.3. Inter Level-0 Inter Level-1 Wormhole Attack

In this type of attack the sender and receiver node not only belongs to two level-0 clusters but also belongs to different level-1 clusters.

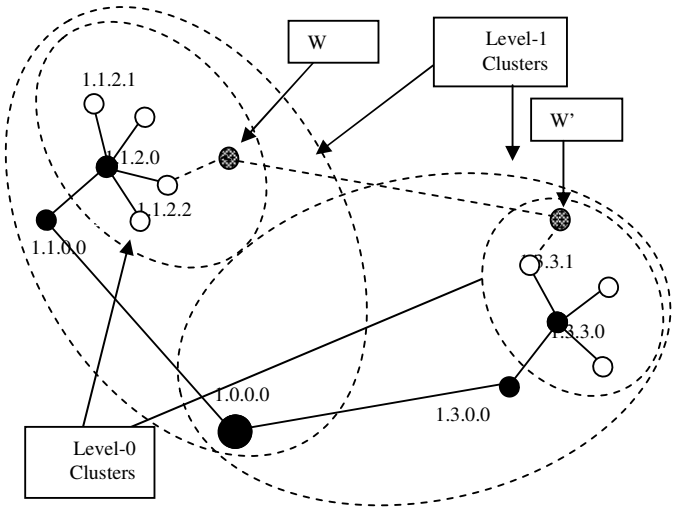

Figure 13. Inter level-0Inter level-1 Wormhole attack

Example: In Figure 13, sender node 1.1.2.2 and receiver node 1.3.3.1 belongs to two different level-1 cluster and a wormhole is created between them by two malicious node W and W' in the previously discussed way.

4.4 Inter Level Inter Cluster Wormhole Attack

Inter Level Inter cluster wormhole attack is conducted by creating wormhole link between two malicious node placed in two different level clusters

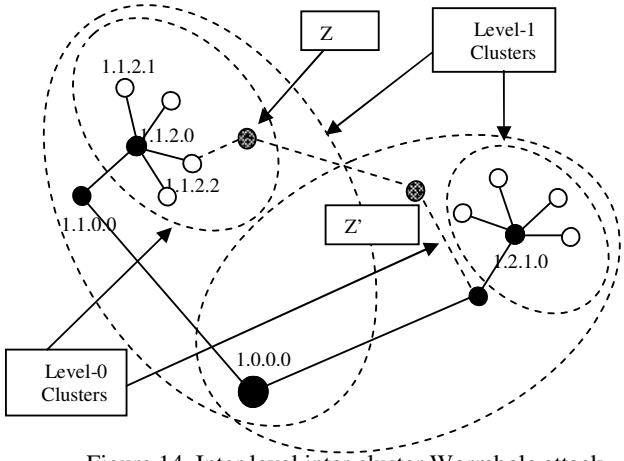

Figure 14. Inter level inter cluster Wormhole attack

Example: In Figure 14, the two nodes 1.1.2.2 and 1.2.0.0 (which are in two different level clusters) are affected by two wormhole creator nodes Z and Z'. Z captures the packet from sender 1.1.2.2 and tunnels it to Z' after encapsulating it. The wormhole link is created in similar fashion.

5. PROCEDURES FOR WORMHOLE ATTACK AVOIDANCE

Now we will give the avoidance techniques for our previously discussed four types of Wormhole attacks on the cluster model. As the underlying technique is DSR protocol, when any node has data to send route discovery phase is initiated first by flooding the RREQ packets. The receiver after receiving all the RREQ packets extract the sender and receiver address from the packet and calculate the intermediate cluster head address. Then the receiver search for the intermediate cluster address in the packet, if not found it detects that it came from a Wormhole link and reject that packet, otherwise accept the packet and sends a RREP via the reverse path that contained in the packet. After that a route has been established between the sender and the receiver via the cluster head.

In the next section we will explain all the countermeasures with example.

5.1. Intra Level Intra Cluster Wormhole Attack Avoidance

In figure 11 it is depicted that that two malicious nodes X and X' creates wormhole link between the sender 1.1.2.1 and receiver 1.1.2.2. Sender node floods RREQ packet to initiate route discovery. After getting RREQ packet cluster head 1.1.2.0 and node X both will send the packet to the destination. But malicious node X uses wormhole link to send the packet. Therefore, the receiver node will get two RREQ packets- one from malicious node X' and another from cluster head 1.1.2.0. Then the receiver node extracts the address of sender and receiver contained in the RREQ packet. And then to calculate the intermediate cluster head address it first checks the level-2 id of those two addresses, if it matches then it checks level-1 id and then level-0 id. In this example the destination node finds that only node id differs in those two addresses. That means both the sender and receiver node belongs to same cluster. And only one path is there between sender and receiver i.e. via cluster head. After this calculation the destination node only accepts that RREQ packet that contain valid path i.e. 1.1.2.1→1.1.2.0→1.1.2.2 and rejects the packet which doesn't contain the valid path. If this is an exposed Wormhole attack then the attackers should put their identity in the packet and the destination mark this path as a compromised one and in future it does not accept any requests coming from this path.

5.2. Inter Level-0 Intra Level-1 Wormhole Attack Avoidance

In figure 12 a wormhole link is created between sender 1.1.2.1 and receiver 1.1.1.2 by two malicious nodes Y and Y'. RREQ packet is broadcasted by the sender node to find route to destination. The destination node will get RREQ packets from both Y' and cluster head 1.1.2.0. After receiving RREQ packet the destination node uses the sender and receiver addresses (1.1.1.2 and 1.1.2.1 respectively) contained in the RREQ packet to calculate intermediate cluster head address. After comparing the level id of those two addresses destination node finds that the level-0 id is different means sender and receiver belong to two different level-0 clusters. So the sender must send the packet through level-1 cluster head 1.1.0.0. And then the intermediate nodes addresses in that packet are checked whether they are legitimate or not. If any one of the nodes address in that packet is not valid then the packet is rejected. RREP is sent back by destination through the valid reverse path 1.1.1.2 –> 1.1.1.0 –> 1.1.0.0 –> 1.1.2.0 –> 1.1.2.1.

5.3. Inter Level-0 Inter Level-1 Wormhole Attack Avoidance

In figure 13 W and W' these two malicious nodes establish wormhole link between sender 1.3.3.1 and receiver 1.1.2.2. The destination node calculates the intermediate cluster head address form the extracted sender and receiver addresses from the received RREQ packet in the same way as discussed above. In this case sender and receiver belong two different level-1 clusters and packet delivery between them must be done via level-2 cluster head 1.0.0.0. If the RREQ packet does not contain cluster head address 1.0.0.0, the packet is rejected otherwise it is accepted and RREP is sent back through that path in reverse direction 1.1.2.2 –> 1.1.2.0 –> 1.1.0.0 –> 1.0.0.0 –> 1.3.0.0 –> 1.3.3.0 –> 1.3.3.1.

5.4. Inter Level Inter Cluster Wormhole Attack Avoidance

In figure 14 Z and Z' create wormhole link between 1.1.2.2, the sender and 1.2.0.0, the receiver. After receiving RREQ it first extracts the sender and receiver address from the received packet and then calculates intermediate cluster head address 1.0.0.0 by comparing the level id of those two addresses. In the same way discussed above. Now it checks the valid path in the packet. If the packet contains valid path packet is accepted otherwise rejected.

In the next section we are giving the pseudo code for avoiding the Wormhole attack by selectively dropping the RREQ packets that are routed via the Wormhole link during the route discovery phase in the DSR protocol.

6. PROPOSED ALGORITHM

Algorithm: RREQ packet forwarding and Wormhole attack avoidance

Step 1. The sender node initiates a route discovery by flooding the RREQ packets within the cluster.

Step 2. The cluster head of this cluster that the sender belongs to, receives the packet.

Step 3. The Cluster head extracts the source and destination addresses from the packet, and identify the mode of communication – *a) Intra cluster b) Inter cluster c) Intra level or d) Inter level* and also sets the Next_Hop address like follows:

3.1. The cluster head starts matching the receiver address with its own address from the MSB (during the matching the cluster head considers only the non zero bits of the addresses).

3.2. If (*mismatch occurs*) then

3.2.1. Set the Next_Hop address value = Current cluster head address.

3.2.2. Replace the first right most non zero bit of Next_Hop address value with zero.

Else

3.2.3. Set the Next_Hop address value = Current cluster head address.

3.2.4. Replace the first left most zero bit value of Next_Hop address with the corresponding receiver address value.

End if

Step 4. The cluster head sends the packet to the address specified in the Next_Hop address.

Step 5. Repeat step – 3 to 4 until the packet reaches the destination.

Step 6. After the destination receives a RREQ packets, it can drop the packets if it came through a Wormhole link as follows:

6.1. It first extracts the source and the destination address from the packet.

6.2. Starts matching the two addresses and take the decision as follows:

Step 7.

7.1. If (the level-1 id mismatches) then

/*sender and receiver belongs to two different level-1 clusters*/

7.1.1. Case 1: both the level-0 id and node id are non zero

/*both of them are non cluster head nodes*/

The receiver calculates the level-2 and level-1 and level-0 cluster heads ids addresses from the source address. As a legal RREQ packet is suppose to pass through all the determined cluster heads, therefore, the destination node searches the entire routing path recorded in the RREQ packet for the respective cluster heads ids. Even if a single cluster head id is missing from the routing path in the packet, it means that the packet has come through some compromised path. In that case the packet is rejected by the receiver.

7.1.2. Case 2: only the node id is zero

/*sender is a level-0 cluster head*/

The receiver calculates the level-1 and level-2 cluster heads ids, and validates the route information stored in the packet using the procedure described in Case1. If the validation is successful then the receiver keeps the packet, otherwise it rejects it.

7.1.3. Case 3: both the level-0 id and node id are zero

/*sender is a level-1 cluster head*/

The receiver only calculates the level-2 cluster head id and validates the route information stored in the packet using the procedure described in Case1. If the validation is successful then the receiver keeps the packet, otherwise it rejects it.

7.2. Else if (the level-0 id mismatches AND the node id is non zero) then

/*sender and receiver belongs to two different level-0 clusters*/

Then the sender calculates only the level-1 cluster head id and validates the route information stored in the packet using the procedure described in Case1. If the validation is successful then the receiver keeps the packet, otherwise it rejects it.

7.3. Else if (the node id mismatches) then

/*sender and receiver belongs to same level-0 cluster*/

Then the sender calculates only the level-0 cluster head id using the procedure previously described. Then it rejects the RREQ packet that does not contain that id.

Step 8. After this the receiver sends a RREP packet through the valid reverse path contained in the packet which has come through the valid path.

Step 9. After the sender receives the RREP packet, a link is established between the sender and the receiver through the path contained in the RREP packet and then the data transmission continuous using the path.

Step 10. End.

---

7. CONCLUSIONS

The main advantage of our proposed method is that it is an avoidance technique and the receiver can detect that a packet has come through some compromised (Wormhole) path during the route discovery phase of the DSR protocol. So, it does not need another phase or a periodically checking for the existence of the Wormhole in the path during data transmission. Our proposed countermeasure unlike of its predecessors neither requires any special H/W nor tightly synchronized clocks. It also does not use any statistical analysis or data. It detects if there is a Wormhole during the route discovery phase of the DSR protocol and avoids this path during further communication. So, nodes do not need to monitor its neighbour behavior during the data transmission, and also the detection process is carried out in the route discovery phase of the DSR so it does not require a separate phase for it.

REFERENCES

[1] C. Perkins, E. Belding-Royer & S. Das, (2003) "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561.

[2] D. Johnson & D. Maltz, (1996) "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, T. Imielinski and H. Korth, Ed., Kluwer.

[3] D. A. Maltz, D. B. Johnson & Y. Hu, (2007) "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4", RFC 4728, The Internet Engineering Task Force, Network Working Group. http://www.ietf.org/ rfc/rfc4728.txt.

[4] E. Royer & C.-K. Toh, (1999) "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Pers. Commun., Vol. 6, No. 2, pp. 46–55.

[5] H. L. Nguyen & U. T. Nguyen, (2008) "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Networks, Volume 6, Issue 1, pp. 32-46.

[6] P. Karmore & S. Bodkhe, (2011) "A Survey on Intrusion in Ad Hoc Networks and its Detection Measures", International Journal on Computer Science and Engineering (IJCSE), Chennai, India.

[7] A. K. Rai, R. R. Tewari, & S. K. Upadhyay, (2010) "Different Types of Attacks on Integrated MANET", Internet Communication. International Journal of Computer Science and Security (IJCSS), Vol. 4, Issue 3

[8] Y.-C. Hu, A. Perrig & D. B. Johnson, (2003) "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", Proc. of INFOCOM 2003, pp.1976-1986.

[9] W. Wang, B. Bhargava, Y. Lu & X. Wu, (2006) "Defending against Wormhole Attacks in Mobile Ad Hoc Networks". Wireless Communication and Mobile Computing.

[10] X. Wang & J. Wong, (2007) "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks", 31st Annual International Computer Software and Applications Conference - Vol. 1 - (COMPSAC 2007), pp. 39-48.

[11] S. Jen, C. Laih & W. Kuo, (2009) "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Sensors. Vol. 9, No. 6, pp. 5022-5039.

[12] H. S. Chiu & K. S. Lui, (2006) "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", Proc. of International Symposium on Wireless Pervasive Computing, pp-6-pp.

[13] L. Hu & D. Evans, (2004) "Using Directional Antennas to Prevent Wormhole Attacks", Network and Distributed System Security Symposium (NDSS).

[14] S. Capkun, L. Buttyan & J. Hubaux, (2003) "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks", ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pp.1-12.

[15] N. Song, L. Qian & X. Li, (2005) "Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach". in proceeding of the 19th International Parallel and Distributed Processing Symposium (IPDPS'05).

[16] L. Buttyán, L. Dóra & I. Vajda, (2005) "Statistical Wormhole Detection in Sensor Networks", Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS) Visegrád, Hungary, pp. 128-141.

[17] C. Sun, K. Doo-young, L. Do-hyeon & J. Jae-il, (2008) "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," Proc. of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008), pp. 343-348.

[18] S. Gupta & S. Dharmaraja, (2011) "WHOP: Wormhole Attack Detection Protocol using Hound Packet", in International Conference of Innovations in Information Technology, pp. 226 to 231.

[19] D. B. Roy, R. Chaki & N. Chaki, (2009) "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1.

[20] J. Sucec & I. Marsic, (2002) "Clustering overhead for hierarchical routing in mobile ad hoc networks", in Proceedings of INFOCOM, New York, NY, pp. 1698-1706.

Authors

Subhashis Banerjee has received his B. Sc. (Honours) and M. Sc. degrees in Computer Science in the year 2009 and 2011 respectively. He has obtained M. Tech. degree in Software Engineering in the year 2013 from West Bengal University of Technology, Kolkata, India. He is presently working as a researcher at Machine Intelligence Unit, Indian Statistical Institute, Kolkata, India. He has published several papers in International journals and conferences.

Koushik Majumder has received his B.Tech and M.Tech degrees in Computer Science and Engineering and Information Technology in the year 2003 and 2005 respectively from University of Calcutta, Kolkata, India. He obtained his PhD degree in the field of Mobile Ad Hoc Networking in 2012 from Jadavpur University, Kolkata, India. Before coming to the teaching profession he has worked in reputed international software organizations like Tata Consultancy Services and Cognizant Technology Solutions. He is presently working as an Assistant Professor in the Dept. of Computer Science & Engineering in West Bengal University of Technology, Kolkata, India. He has published several papers in International and National level journals and conferences. He is a senior Member of IEEE.