Wormhole Detection and Removal Algorithm in Mobile Ad-hoc Networks using Enhanced Cluster based Technique

Ankur Ratmele
Assistant Professor
IES IPS Academy Indore, M.P.

ABSTRACT
Mobile Ad-hoc Networks (MANETs) are the collection of mobile devices which communicate through the wireless medium and do not have the central infrastructure. In unsecured MANETs, malicious nodes can form a private tunnel. Source sends packets to the destination and these packets follow the path through this tunnel, so the packets are captured by malicious nodes and do not reach the destination node. This is known as wormhole attack which is one of the well known security threat. The emphasis of my work is to detect wormhole attack, when there is more number of malicious nodes than non malicious nodes and develop a technique to prevent network from this wormhole attack. In this work, malicious nodes are detected on the basis of Packet Delivery Ratio (PDR). Packet Delivery Ratio is the ratio of number of packets sent to the number of packets received by the destination node. For performing the simulation of the various scenarios and analyzing the results we have used Ns-2 simulator.

Keywords
Wormhole Detection, Ad-hoc Networks

1. INTRODUCTION
Mobile Wireless Ad-hoc Networks are different from wired networks because MANETs uses the wireless medium to communicate that do not rely on fixed infrastructure and can arrange them into a network quickly and efficiently. MANETs must have a secure means for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. In order to provide secure communication and transmission, the researchers must understand various types of attacks and their effects on the MANETs. Wormhole attack, Blackhole attack, Sybil attack, Flooding attack, Routing table overflow attack, Denial of Service (DoS), Selfish node misbehaving, Impersonation attack are the kind of attacks that MANETs can suffer from Ad-hoc Networks (MANETs) [1],

The wormhole attack [2] is a severe type of attack in which two malicious nodes can forward packets through a private "tunnel" in the network as shown in Figure 1

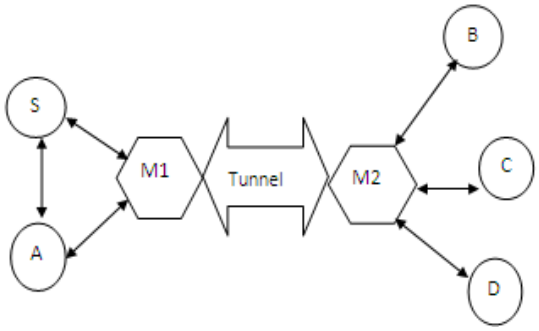

Fig .1. Example of wormhole attack

Here, two malicious nodes i.e M1, M2 which link through a private connection. Every packet that M1 receives from the network is forwarded through "wormhole" to node M2.

2. RELATED WORK
The most commonly cited wormhole prevention mechanism is 'packet leashes' by Hu et al. [3], proposed to add protected 'leash' contain timing and Global Positioning System (GPS) information to each packet on a hop-by-hop basis. Based on the information enclosed in a packet leash, a node receiving the packet would be able to decide whether the packet has traveled a distance larger than actually possible.

Hu et al. [3] proposed two different kind of leashes: physical leashes and chronological leashes. Physical leashes require each node to have access to up-to-date GPS information, and rely on loose (in the order of ms) clock synchronization. When Physical leashes are used, a node transfer a packet appends to it the time the packet is sent ts and its location ps. A receipt of node uses its own position pr and the time it receives a packet tr to decide the distance the packet could have traveled. Keeping in mind maximum possible node velocity v, clock synchronization error Δ, and possible GPS distance error Δ, the distance amongst the sender and the recipient dsr is upper-bounded by::

$$dsr<||ps-pr||+2v(tr-ts+\Delta)+\Delta \quad \text{……..(i)}$$

Physical leashes ought to work fine when GPS coordinates are useful and available. However, modern GPS technology has important boundaries that should not be unnoticed. While the price of GPS devices is going down, it remains considerable.

lastly, GPS systems are not adaptable, as GPS devices do not function well within buildings, under water, in the occurrence of strong magnetic radiation, etc. As contrasting to physical leashes, chronological leashes need much tighter clock synchronization but do not rely on GPS information. When chronological leashes are used, the transfer node specify the time it sends a packet ts in a packet leash, and the in receipt of node uses its individual packet reception time tr for

verification. In a somewhat different version of chronological packet leashes, the transfer node calculates an finishing time te subsequent to which a packet should not be established, and puts that information in the leash. This is to avoid a packet from wandering farther than distance L

$$te=ts+L/C-\Delta, \quad \ldots.(ii)$$

where C is the momentum of light and Δ is the maximum clock.

One probable way to avoid wormholes, as used by Capkun et al. [4], Hu et al. [5], Hong et al. [6] , and Korkmaz et al. [7], is to calculate round-trip travel time of a message; and its acknowledgement, estimation the distance among the nodes based on this pass through time, and establish whether the considered distance is within the greatest possible communication range. The foundation of all these approaches is the following. The Round Trip Travel Time (RTT) δ of a message in a wireless medium can, hypothetically, is linked to the distance d between nodes, assuming that the wireless signal movements with a momentum of light c:

$$d=(\delta c) / 2 \text{and } \delta=2d/c \quad \ldots\ldots\ldots\ldots\ldots \text{ iii)}$$

The neighbor position of nodes is confirmed if d is surrounded by the radio broadcast range R for R > d (d within broadcast range): $R > \delta c/2$ and $\delta < 2R/c$. In soul, the use of RTT eliminate the necessitate for tight clock synchronization required in chronological leashes: a node only uses its clock to determine time. However, this approach, while accounting for message propagation, completely ignores message processing time. When a message is sent by one node and is approved by an additional, the time it takes for a node to progression a message and to reply to it is usually non-negligible, mainly in the context of bounding short distance with signals whose speed is similar to that of light in vacuum.After all, it takes the light less than 0.2 seconds to circle the entire Earth around the equator. Outstanding clock precision and practically nonexistent errors are required to bind distances on the order of hundreds of meters.

In (Roy, Chaki & Chaki)[8], the authors have proposed a cluster-based scheme to avoid wormhole attack in MANETs that uses AODV as a routing protocol. The network is separated into dissimilar clusters. Each cluster has cluster head which is elected energetically in the inner layer and keeps routing information of all associated nodes. There is a cluster head in the outer layer conscientious for passing on information to all associate nodes in each cluster. The guard node positioned on the connection of clusters is accountable for monitoring the malicious activity of member nodes. In a case when a guard node detects any malicious movement of a node, it hearsay it to the cluster head, which replies the information to the cluster head in the outer layer which in turn inform all other nodes in the network about the malicious movement.

3. PROPOSED ALGORITHM

There are more number of malicious nodes are present in the clusters than the non malicious nodes in the Mobile Ad-hoc Networks, if these malicious nodes give wrong information to the cluster head about the nonmalicious nodes, then this nonmalicious nodes will be declared as malicious nodes.

Suppose if node 4 (malicious node) give wrong information to the CH1 about node 5 (nonmalicious node) then node 5 will declare as a malicious node. So the objective of this algorithm is to prevent the nonmalicious nodes cannot be declared as malicious nodes.

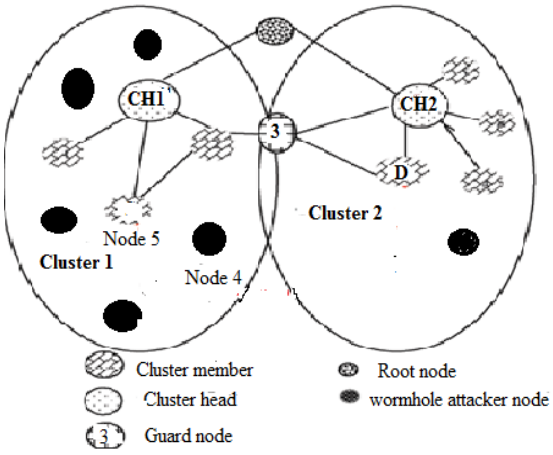

Fig.2. Overview of wormhole [8]

In this Wormhole Detection Algorithm in MANETs Using Enhanced Cluster-Based Technique, there is the solution for the problem that is caused when the malicious nodes give wrong information to the cluster head about the nonmalicious nodes, that nonmalicious nodes are malicious nodes (which are actually not malicious nodes). This problem is addressed by this algorithm. This technique will prevent nonmalicious nodes to be declared as malicious nodes and also, detects and removes wormhole attack in MANETs.

In this proposed algorithm, only one restriction that is Packets travelled from one cluster to the other cluster through the guard node (3). Guard node monitors the malicious activity within the network. Guard node is elected which is closer to the both Cluster Head.

When malicious nodes inform to the cluster head about the nonmalicious nodes as malicious nodes, then this problem is addressed by this algorithm. The CH (Cluster Head) will check the Packet Delivery Ratio of nodes. If the Packet Delivery Ratio of nodes is greater than zero, then nodes are not malicious nodes otherwise these nodes are declared as malicious nodes.

Packet Delivery Ratio is checked by the CH for the node, whether that node is forwarding the packets or dropping the packets.

Suppose in Fig: 2, if node 4 (malicious node) give wrong information to the CH1 about node 5 (nonmalicious node) then the cluster head CH1 will check the Packet Delivery Ratio of the node 5. If the node 5 Packet Delivery Ratio is greater than the zero, then node 5 will not declare as a malicious node.

If malicious nodes forward the packets to nonexisting nodes in the network, then packets will be dropped or not reached to the destination node. So to address this problem, packets will travelled through guard node (node 3) and guard node verifies the existence of the node with the associated cluster head that maintains the routine table of cluster. If the node is not in the corresponding cluster head routine table then malicious nodes are identified.

Referring from above Fig: 2, if malicious node (node4) forward the packets to node 20 (which is a non existing node), then the guard node (node 3) will check the CH2 routine table entries whether the node 20 is exist or not. Guard Node verifies that this node 20 is nonexistence node so the packets

will not be sent and monitor the behavior of the node 4 (which has sent the packet to the nonexistence node).

4. SIMULATION SCENARIO

In this simulation, there are two clusters. Each cluster has its own cluster head. When nodes join the network and these nodes which are in the communication range of the cluster head are assigns to that cluster. The node which is in the communication range of both cluster head is known as guard node (node 3).

Simulation without attack shown in Fig.3, there are 30 nodes in the network. Node 1 and Node 2 are the cluster head of the clusters. Node 5, node 6, node 4, node 5, node 7, node 8, node 9 node 11, node 12 are in the cluster 1 and node 13, node 14, node 15, node 16, node 17, node 18, node 19, node 20, node 21 are in the cluster 2. Node 3 is the guard node. Packets travelled from one cluster to another cluster through guard node, i.e. node 3.

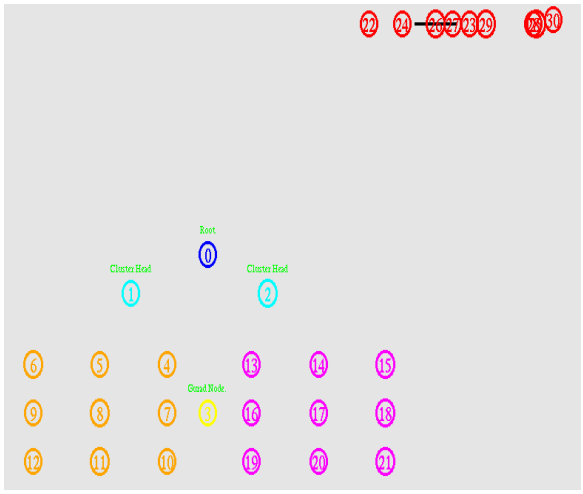

Fig.3. Simulation without attack

In Fig.4 malicious nodes are present in the network. The malicious nodes are 22, 23, 23 etc. In this network due to malicious nodes, the packets are dropped not delivered to the destination. So this attack has to be detected and removed.

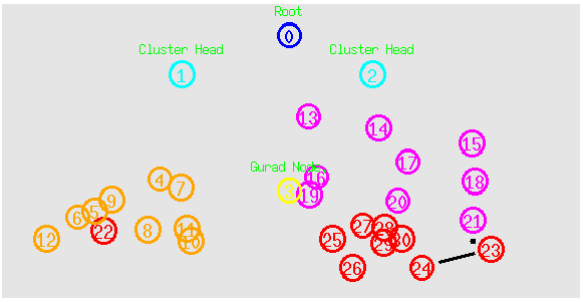

Fig. 4. Simulation Scenario when malicious nodes in the network

5. RESULTS

Results are obtained after performing the simulation when malicious nodes give wrong information to the cluster head about the presence of other malicious nodes and also when malicious nodes forward packets to the non-existing nodes. Results are as follows:

Table 1. Results when malicious nodes give wrong information

Time(sec.)		Source Node	Destination Node	Packet Delivery Ratio	Remarks
Start Time	Stop Time				
0.2	8.5	13	4	92.049	Malicious nodes are not present
5.0	12.5	5	16	84.9	Malicious nodes are not present
12.0	19.5	12	6	100	Malicious nodes are not present
20.0	25.0	5	21	0	Malicious nodes are present in the network
25.0	29.0	4	21	0	Malicious nodes are present in the network.

Table. 2. Results after removal of malicious nodes in communication

Time(sec.)		Source Node	Destination Node	PDR	Remarks
Start Time	Stop Time				
0.2	8.5	13	4	92.18	Communication is done through non malicious nodes
5.0	12.5	5	16	84.9	Communication is done through non malicious nodes
12.0	19.5	12	6	100	Communication is done through non malicious nodes
20.0	25.0	5	21	100	Malicious nodes are removed
25.0	32.0	4	21	89.90	Malicious nodes are removed

6. CONCLUSION

In this "Wormhole Detection & Removal Algorithm in Mobile Ad-hoc Networks Using Enhanced Cluster Based Technique" malicious nodes are detected and removed by Packet Delivery Ratio of the nodes. The simulation results show that if Packet Delivery Ratio of the nodes is zero then this algorithm is declaring nodes as malicious nodes and nodes that are having its Packet Delivery Ratio greater than zero are declared as nonmalicious nodes.

7. REFERENCES

[1] C.Siva Ram Murthy and B. S. Manoj. :Ad hoc wireless networks: Architecture and Protocols", Prentice Hall Publishers, May 2004, ISBN 013147023X.

[2] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad. :Security in wireless Ad-hoc networks, the handbook of Ad hoc wireless network. Chapter 30: CRC PRESS Publisher, 2003.

[3] Y.-C. Hu, A. Perrig, D. B. Johnson.: Packet leashes: a defense against wormhole attacks in wireless networks; INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, pp. 1976-1986, 2003.

[4] S.Capkun, L. Buttyan, J.-P. Hubaux.: SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks; Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks; 2003.

[5] Y-C Hu, A. Perrig, D. Johnson.: Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols ; Proc. of WISE 2003, September 19, San Diego, California, USA, 2003.

[6] Korkmaz T.: Verifying Physical Presence of Neighbours against Replay-based Attacks in Wireless Ad Hoc Networks; Proc. International Conference on Information Technology: Coding and Computing 2005, ITCC 2005, pp. 704-709, 2005.

[7] M.Parsons and P.Ebinger.Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks.

[8] Roy, D.B., Chaki, R & Chaki, N.: A New Cluster-Based Wormhole Intrusion detection Algorithm for Mobile Ad Hoc Networks, International Journal of Network Security and its Applications (IJNSA), (2009).