A Defense against Wormhole Attacks in Wireless Ad hoc Networks using Cluster Technique

Amol V. Zade
M.E. II Year. Dept. of CSE
Sipna's COET, Amravati, MH, India

Vijaya K. Shandilya
Asso. Prof. Dept. of CSE,
Sipna's COET, Amravati, MH, India

ABSTRACT
In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. A particularly devastating attack is the wormhole attack, where a malicious node records control traffic at one location and tunnels it to another compromised node, possibly far away, which replays it locally. Routing security in ad hoc networks is often equated with strong and feasible node authentication and lightweight cryptography. Unfortunately, the wormhole attack can hardly be defeated by cryptographical measures, as wormhole attackers do not create separate packets. We present a cluster based counter-measure for the wormhole attack that alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET. The Wormhole attack does not require exploiting any nodes in the network and can interfere with the route establishment process. We also discuss previous works which require the role of administrator and their reliance on impractical assumptions.

Keywords: MANET, Wormhole attack, Cluster, Guard Node.

1. INTRODUCTION
Recently many network researchers are studying networks based on new communication techniques, especially wireless communications. Wireless networks allow hosts to roam without the constraints of wired connections. People can deploy a wireless network easily and quickly. End users can move around while staying connected to the network. Wireless networks play an important role in both military and civilian systems. Handheld personal computer connectivity, notebook computer connectivity, vehicle and ship networks, and rapidly deployed emergency networks are all applications of this kind of network. Hosts and routers in a wireless network can move around. Therefore, the network topology can be dynamic and unpredictable. Traditional routing protocols used for wired networks cannot be directly applied to most wireless networks because some common assumptions are not valid in this kind of dynamic network.

1.1 Wireless Networks
Like traditional wired networks, wireless networks are formed by routers and hosts. In a wireless network, the routers are responsible for forwarding packets in the network and hosts may be sources or sinks of data flows. The fundamental difference between wired and wireless networks is the way that the network components communicate. A wired network relies on physical cables to transfer data. In a wireless network, the communication between different network components can be either wired or wireless. Since wireless communication does not have the constraint of physical cables, it allows a certain freedom for the hosts and/or routers in the wireless network to move.

1.2 Mobile Ad hoc Networks:
Mobile Ad hoc Networks (MANET) is an autonomous system, where nodes/stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. Mobile ad-hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes the mobile ad-hoc networks unpredictable from the point of view of scalability and topology.

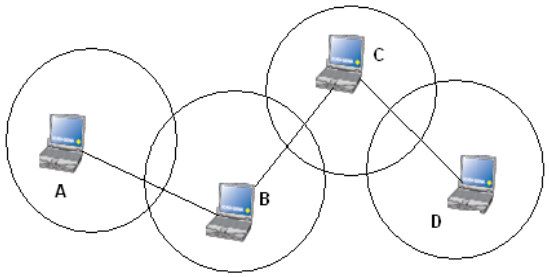

Fig 1: Mobile ad-hoc Network (MANET)

From above figure 1, when a node wants to communicate with another node, the destination node must lies within the radio range of the source node that wants to initiate the communication [1]. These networks are fully self organized, having the capability to work anywhere without any infrastructure. Nodes are autonomous and play the role of router and host at the same time. MANET is self governing, where there is no centralized control and the communication is carried out with blind mutual trust amongst the nodes on each other. The network can be set up anywhere without any geographical restrictions. One of the limitations of the MANET is the limited energy resources of the nodes.

Security in Mobile Ad Hoc Network is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

2. LITERATURE REVIEW:

2.1 Packet Leashes
Hu, Perrig and Johnson [2] developed protocols with packet leashes have been proven to be reliable wormhole attack detectors. Packet leashes place restrictions on a packet's maximum allowed transmission distance in a network. Two types of packet leashes discussed in this article are temporal and geographical leashes. Temporal leashes require tightly synchronized clocks on all nodes. Protocols based on temporal leashes ensure that packets transmitted across the network

have an upper bound on its lifetime, which restricts the maximum distance of travel. Packets on a network remain valid for a certain time interval before they are rejected. However, setting up wormhole attacks under temporal leashes is difficult because packets must be sent through the wormhole within the restricted time period. A geographical leash is the second type of leash discussed. Protocols based on geographical leashes differ slightly from temporal leashes in that each node must know its location and have loosely synchronized clocks.

2.2 Graph Theoretic Approach

Lazos *et al*. [3] proposed a graph theoretic model to characterize the wormhole attack and ascertain the necessary and sufficient conditions for any candidate solution to prevent wormholes. They used a *Local Broadcast Key* (LBK) based method to set up a secure *adhoc* network against wormhole attacks. In other words, there are two kinds of nodes in their network: guards and regular nodes. Guards access the location information through GPS or some other localization method like SeRLoc [4] and continuously broadcast location data. Regular nodes must calculate their location relative to the guards beacons, thus they can distinguish abnormal transmission due to beacon retransmission by the wormhole attackers.

2.3 Localization Scheme

Wireless security protocols based on localization have the potential to detect wormhole attacks. Localization systems are based on verifying the relative locations of nodes in a wireless network. Knowing the relative location may help conclude whether or not packets are sent by either a node or wormhole. Several localization schemes discussed in this section: Rather than focusing on individual nodes of a network, this protocol emphasizes the regions of verification. The verified node determines whether or not the unverified node is in the region of verification depending on the time it takes to receive an ultrasonic signal.

2.4 Directional antennas

Awerbuch [5] proposed a technique known as directional antennas can be used to prevent the wormhole attack. To thwart the wormhole, each node shares a secret key with every other node and maintains an updated list of its neighbors. To discover its neighbors, a node, called the announcer, uses its directional antenna to broadcast a HELLO message in every direction. Before the announcer adds the responder to its neighbor list, it verifies the message authentication using the shared key, and that it heard the message in the opposite directional antenna to that reported by the neighbor. This approach is suitable for secure dynamic neighbor detection. However, it only partially mitigates the wormhole problem. Specifically, it only prevents the kind of wormhole attacks in which malicious nodes try to deceive two nodes into believing that they are neighbors. Radio Frequency (RF) watermarking is another possible approach to providing the security

3. SECURITY ISSUES IN MANET:

Recently in the past few years security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. With the comparison of wired network Mobile ad hoc network is different. The routing protocols designed majorly for internet is different from the mobile ad hoc networks (MANET) [7].

A. Attacks in MANET

Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks. Major vulnerabilities which have been so far researched are mostly these types which include selfishness, dynamic nature, and severe resource restriction and also open network medium. Fabrication attacks involve Black hole attack, Grayhole attack, and Wormhole attack.

4. WORKING OF WORMHOLE ATTACK

A *wormhole* is an attack on the routing protocol of a Mobile Ad-hoc Network (MANET). Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. In a *wormhole attack*, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. In general, wormhole attacks consists two malicious nodes tunneling traffic from one end of the network to the other For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multihop route, for example through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker.

A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network [10]. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go through them.

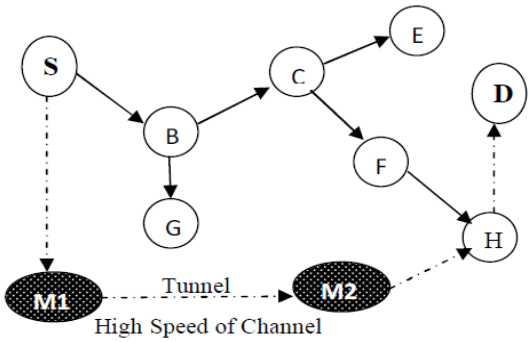

Fig 2: Wormhole Attack

5. CLUSTER BASED DETECTION TECHNIQUE OF WORMHOLE ATTACK IN MANET

The objective is to find out the malicious node that performs the wormhole attack in network. I have assumed that the MANET consists of clusters of nodes. The assumptions regarding the organization of the MANET are listed in section 5.1

5.1 Cluster Information

The AODV routing protocol is used as the underlying network topology. A two layer approach is used for detecting whether a node is participating in a wormhole attack. The layered approach is introduced to reduce the load of

processing on each cluster heads. From security point of view, this will also reduce the risk of a cluster head being compromised.

The entire network is divided in clusters as in figure 3. The clusters may be overlapped or disjoint. Each cluster has its own cluster head and a number of nodes designated as member nodes. Member nodes pass on the information only to the cluster head. The cluster-head is responsible for passing on the aggregate information to all its members.

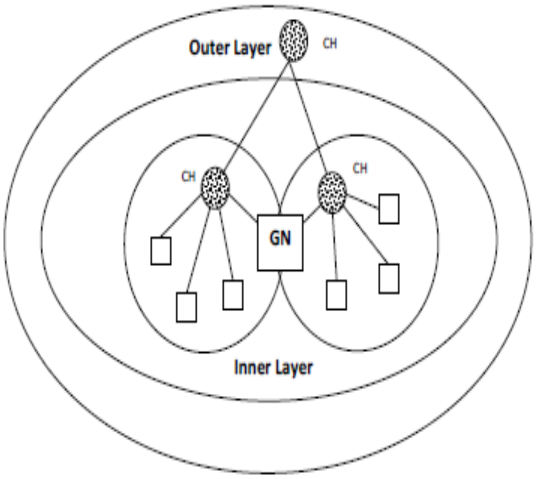

Fig 3: The Layered architecture

We present the algorithm to detect wormhole attacks. When a node in the i^{th} cluster of layer 1 suspect wormhole attack within the cluster, it informs the cluster head of i^{th} cluster at layer 1, which is denoted as CH (1,i). CH (1, i) informs cluster head at layer 2 ($CH_{2)}$, about the malicious node. CH_2 broadcast this information to all cluster heads at layer 1. The cluster heads at layer 1 inform their respective cluster members.

5.2 Procedure Wormhole Detection

Begin

Step A: Initiate the network with two clusters and each cluster has some nodes.
Step B: The node within a cluster having minimum node ID becomes Cluster Head. The node ID for each node is provided when the node enter into the cluster.
Step C: Each node stores the information of its immediate neighbors in its neighbor table.
Step D: The node nearest to both the cluster heads at layer 1 is chosen as the guard node.
Step E: Source node S sends a HELLO packet to the intermediate node with destination node ID and cluster ID

Step I: S starts timer, initializes T_1
Step II: S increments the PKTCNT(S, D)
Step III: When S get acknowledgement from destination node stop timer, T_2
Step IV: The expected round trip time is computed as
$T_e = T_2 - T_1$
Step V: Source node S sends a packet to destination node
Step VI: S starts timer TP_1
Step VII: When S get acknowledgement from destination node stop timer, TP_2
Step VIII: The round trip time is calculated as
$T_r = TP_2 - TP_1$
Step IX: If $T_r << T_e$ then inform guard node.
Step F: The guard nodes checks number of packet send by source node PKTSNT (S, D) and number of packet receive by destination node PKTRCD(S, D).
Step G: Δp = PKTSNT (S, D) - PKTRCD (S, D).
Step H: If $\Delta p > P_{th}$ then inform the source node to stop packet transfer.
Step I: The source node stop packet transfer and inform cluster head.
End.

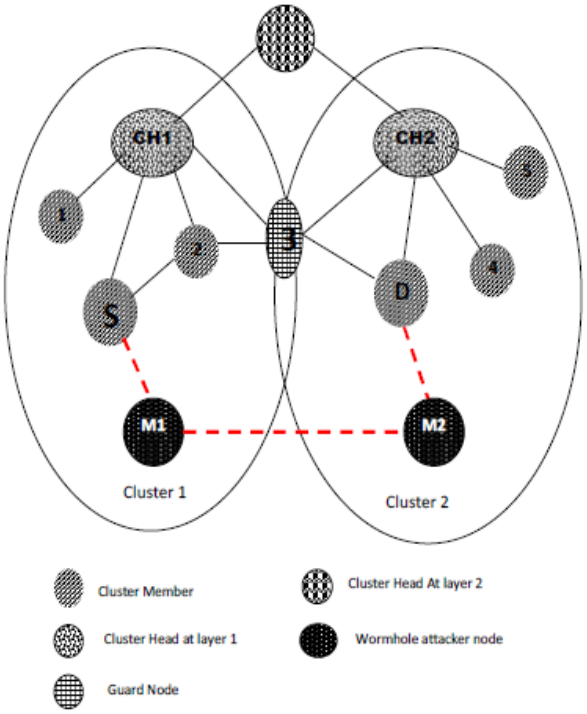

Fig 4: Cluster Based Detection Technique

Node S sends a HELLO packet for destination node D. S has a path to D via (2, 3). M1, being in the proximity of S, overhears the HELLO message and forwards the same to node M2 in the other end of the network. Node D hears this HELLO message from S and therefore considers S to be its immediate neighbor and follow the route to send message to S via M1 and M2. The node 3 which is at the overlapping position of two cluster acts as GUARD node who can here every packet send by node S for the destination node D and monitor the packets route from source to destination. The guard node is also called monitoring node. When S observes some malicious behavior when it sends packet to D it informs the guard node. The guard node then checks the number of packets send for the node D and those actually received by D from S. Then it calculates *Δp = PKTSNT(S, D) - PKTRCD (S, D)*. If the value of Δp surmounts the threshold value that is predefined by the monitoring node then monitoring node finds out the wormhole attack.

6. SIMULATION ENVIRONMENT

Here we give more focus on the varying number of mobile nodes for the evaluation of performance of Ad-hoc routing protocol AODV under the Wormhole attack. The simulations have been performed using network simulator NS-2. The network simulator ns-2 is discrete event simulation software for network simulations which means it simulates events such

as sending, receiving, forwarding packets. The ns-allinone-2.32 supports simulation for routing protocols.

6.1 Simulation Model:

We consider the network of nodes placing within a 1000m × 1000m area, the performance of AODV is evaluated by considering following parameters.

Table-1. Parameter Values for AODV under Wormhole

Simulation Parameters	
Simulator	Ns-2.32
Protocol	AODV
Simulation Duration	500 Seconds
Simulation Area	1000m × 1000m
Number of Nodes	10,20,30,40,50
Channel Type	Channel/ Wireless Channel
Network Interface type	Phy/ wireless phy
MAC type	Mac/ 802.11
Link Layer type	LL
Number of Wormhole Link	0,1

6.2 Performance Metrics:

For analyzing AODV protocol under wormhole attack, we focused on two performance parameters which are Packet Delivery Ratio (PDR) and throughput.

6.2.1 Packet Delivery Ratio (PDR):

The fraction of all the received data packets successfully at the destinations over the number of data packets sent by the sources is known as Packet delivery fraction. The greater value of packet delivery ratio means better performance of the protocol.

$$PDR = \frac{Number\ of\ Packets\ Received}{Number\ of\ Packets\ Send}$$

6.2.2 Throughput:

Throughput is the average number of messages successfully delivered per unit time i.e. average number of bits delivered per second.

7. RESULTS AND ANALYSIS:

7.1 Packet Delivery Ratio:

- Simulation:

Table-2: Simulation Result for PDR

Sr. No.	No. of Nodes	Packet Sent	Packet Received	PDR
1	10	4388	1578	0.3596
2	20	4388	966	0.2201
3	30	4388	1261	0.2874
4	40	4388	958	0.2183
5	50	4388	946	0.2156

- Analysis:

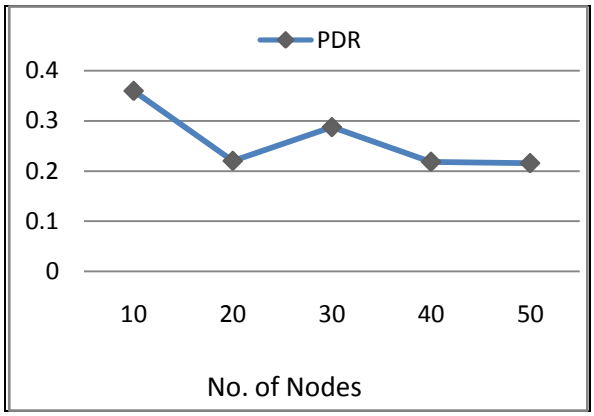

Fig 5: Graphical representation of PDR

The above graphical figure shows us that the value of PDR is decreasing from nodes 10 to nodes 20, and then it is increases for node 30 and decreases for node 40 slightly and finally remains constant for nodes 50.

7.2 Throughput:

- Simulation:

Table-3: Simulation Result for Throughput.

Sr. No.	No. of Nodes	Throughput
1	10	16.66
2	20	30.48
3	30	20.18
4	40	39.73
5	50	39.23

- Analysis:

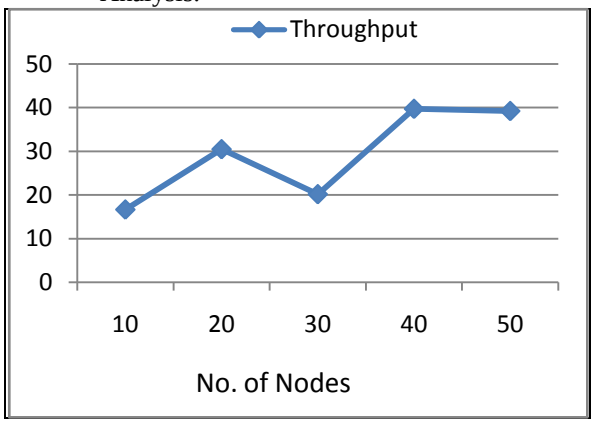

Fig 6: Graphical representation for Throughput.

From the above simulation results for throughput we can say that throughput increases for nodes 20 and again decreasing for 30 nodes and for nodes 40 it increases largely and finally for 50 nodes it remains slightly constant.

8. CONCLUSION

In this work, a new cluster based wormhole detection method has been proposed. In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security threats including the wormhole attack. One of the most interesting parameters to consider when supporting real time communication is the Packet Delivery Ratio (PDR), Throughput. In the future, further study also needs to be done with delay jitter metric.

The proposed solution unlike some of its predecessors does not require any specialized hardware like directional antennas, etc for detecting the attackers. Currently more studies are being done to analyze the performance of the proposed

algorithm in presence of multiple attacker nodes. We have proposed a solution for the wormhole attack problem in MANET, the dynamic information of the packets could still be modified.

9. REFERENCES

[1] Kuldeep Sharma, Dr.G.Mahadevan, "Advance Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", International Journal On Recent Trends in Engineering & Technology, Vol. 05, No. 01, Mar 2011

[2] Hu, Yih-Chun, Adrian Perrig and David B. Johnson. "Wormhole attacks in wireless networks", IEEE journal on selected areas in communications, vol. 24, no. 2, february 2006, 0733-8716

[3] Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W. "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In *IEEE WCNC 2005*, Seattle, WA, USA, 2005; pp. 1193–1199.

[4] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki," 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, April 2009.

[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah," MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[6] Hu, Lingxuan and David Evans. "Using Directional Antennas to Prevent Wormhole Attacks", In Network and Distributed System Security Symposium (NDSS 2004), San Diego, California, USA. February 2004.

[7] Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru "Mitigating Byzantine Attacks in Ad Hoc Wireless Networks", March 2004

[8] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006.

[9] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[10] Shang-Ming Jen, Chi-Sung Laih and Wen-Chung Kuo , A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET, *Sensors* 2009, *9*, 5022-5039.