# Wormhole Attack Prevention By Next Hop Analysis

Gouthamamani Venkatesan

**Abstract**— A Mobile Ad-hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. It uses open medium, dynamic topology and distributed co-operation. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. Routing is the primary function of each node. Mobile Ad-hoc Networks are highly vulnerable to many security attacks like black holes, denial of service, etc and the issue addressed here is one such attack called the "*Wormhole attack*". In this attack, a tunnel is created between two malicious nodes and packets are tunneled between them in such a way that tunneled packet arrives sooner than other packets transmitted over a normal multi-hop route and thus the route via the malicious nodes is selected. The wormhole puts the attacker in a very powerful position relative to other nodes in the network and the attacker could exploit this position. Existing solutions for this attack like packet leashes, directional antennas, etc either increase the overhead in processing or do not completely eliminate the tunnel. In this paper, the solution proposed is by analyzing the next hop of nodes and identifying the tunnel and thus removing the associated nodes from the network. The protocol under consideration is Ad-hoc On Demand Routing Protocol (AODV). The solution has been tested for throughput by using the simulation environment "GLOMOSIM" and the simulation results confirm the increase in throughput by implementing this solution.

**Index Terms**— Mobile Ad-hoc Networks (MANET), Wormhole Attack, Ad-hoc On Demand Vector (AODV) Protocol, Next Hop Analysis

## 1 Introduction

A mobile ad hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. This type of networks is suited for use in situations where a fixed infrastructure is not available, not trusted, too expensive or unreliable. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. Routing is one of the primary functions each node has to perform in order to anytime; anywhere networking enable connections between nodes that are not directly within each others send range. The development of efficient routing protocols is a non-trivial and challenging task because of the specific characteristics of a MANET environment.

## 2 Characteristics Of Manets

### 2.1 Dynamic Topologies

Nodes are free to move arbitrarily; thus, the network topology may change randomly and rapidly at unpredictable times.

### 2.2 Bandwidth-constrained

Wireless links have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communication is often much less than a radio's maximum transmission rate, due to fading, noise, interference conditions, etc.

### 2.3 Energy-constrained

Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

### 2.4 Limited Physical Security

Mobile wireless networks are generally more prone to physical security threats than wired networks. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered.

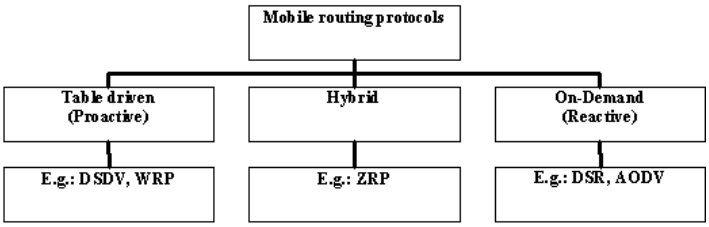
## 3 Goals Of Routing Protocols

The Routing Protocols should minimize routing (bandwidth) overhead and memory/computation power at the hosts. There should be little or no periodic advertisements - but broken links or new routes should be detected as soon as possible. Changes to the network topology should be detected and new routes created as soon as possible. It should be self-starting. MANETs should be set up with as little administrative overhead as possible and should be loop-free, avoiding problems such as count-to-infinity problem and scale to a fairly large network. The Routing Protocols should be independent of the underlying link layer or physical layer. It should not assume that all links are symmetric. That is, not all links are bi-directional.

The protocol should give up gracefully when the destination node is not reachable. It should not repeatedly try to send to that destination and take up unnecessary bandwidth. That is, there should not be any problems if part of the network is partitioned off temporarily. It should provide loop-free routes. This holds not only after the routing algorithm has converged, but also while it is converging. If possible, should provide multipaths to a destination to avoid congestion and compatible with existing wired routing protocols or when there is a central access point. And finally simplicity of the algorithm is preferred. It should be easy to understand and implement.

## 4 Classification Of Routing Protocols

The existing ad hoc routing protocols can be broadly classified into the following two categories:




### 4.1 Table Driven Protocols

Table Driven Routing Protocols, also known as Proactive Protocols, work out routes in the background independent of traffic demands. Each node uses routing information to store the location information of other nodes in the network and this information is then used to move data among different nodes in the network. This type of protocol is slow to converge and may be prone to routing loops. These protocols keep a constant overview of the network and this can be a disadvantage as they may react to change in the network topology even if no traffic is affected by the topology modification which could create unnecessary overhead. Even in a network with little data traffic, Table Driven Protocols will use limited resources such as power and link bandwidth therefore they might not be considered an effective routing solution for Ad-hoc Networks. Destination Sequenced Distance Vector (DSDV) is an example of a Table Driven Protocol.

Destination Sequenced Distance Vector (DSDV) is a Proactive routing protocol that solves the major problem associated with the Distance Vector routing of wired networks i.e., Count-to-infinity, by using Destination sequence numbers. Destination sequence number is the sequence number as originally stamped by the destination. The DSDV protocol requires each mobile station to advertise, to each of its current neighbors, its own routing table (for instance, by broadcasting its entries). The entries in this list may change fairly dynamically over time, so the advertisement must be made often enough to ensure that every mobile computer can almost always locate every other mobile computer. In addition, each mobile computer agrees to relay data packets to other computers upon request. At all instants, the DSDV protocol guarantees loop-free paths to each destination

### 4.2 On Demand Routing Protocols

On Demand Routing Protocols, also known as Reactive Protocols, establish routes between nodes only when they are required to route data packets. There is no updating of every possible route in the network instead it focuses on routes that are being used or being set up. When a route is required by a source node to a destination for which it does not have route information, it starts a route discovery process which goes from one node to the other until it arrives at the destination or a node in-between has a route to the destination. On Demand protocols are generally considered efficient when the route discovery is less frequent than the data transfer because the network traffic caused by the route discovery step is low compared to the total communication bandwidth. This makes On Demand Protocols more suited to large networks with light traffic and low mobility. Examples of On Demand Protocols are Dynamic Source Routing (DSR) and Adhoc On Demand Distance Vector (AODV).

Dynamic Source Routing (DSR) computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass; the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. DSR uses no periodic routing advertisement messages, thereby reducing network bandwidth overhead, particularly during periods when little or no significant host movement is taking place. DSR has a unique advantage by virtue of source routing.

### 4.3 Hybrid Routing Protocols

Hybrid Routing Protocols combine Table Based Routing Protocols with On Demand Routing Protocols. They use distance-vectors for more precise metrics to establish the best paths to destination networks, and report routing information only when there is a change in the topology of the network. Each node in the network has its own routing zone, the size of which is defined by a zone radius, which is defined by a metric such as the number of hops. Each node keeps a record of routing information for its own zone. Zone Routing Protocol (ZRP) is an example of a Hybrid routing protocol.

Zone-based routing attempts to divide the network into "zones". A node considers other nodes belonging to the same zone (intrazone) if those nodes are within a routing zone radius from it. For example, if the routing zone radius is 2, then all nodes within 2 hops from the node are considered within that node's zone. The number of zones is equal to the number of nodes, each zone with a node at its center. The zones overlap. Each node uses table-driven routing protocols for determining how to route packets within its zone (Intrazone). That is, the node will know right away where to send the packets. Each nodes uses on-demand routing protocols for determining how to route packets outside its zone (Interzone). That is, the node has to query how to send the packets before it can actually send the packets.

Unfortunately, these protocols suffer from a number of shortcomings:

1. Scalability problems with growing network size
2. Their performance is only optimal under certain network conditions (mobility, network load, network topology…)

## 5 Trade-Offs Between Routing Protocols

There exists many trade-offs between the routing protocols.

### 5.1 Latency of Route Discovery

Proactive protocols may have lower latency since routes are maintained at all times whereas Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y.

### 5.2 Overhead of Route Discovery/Maintenance

Reactive protocols may have lower overhead since routes are determined only if needed whereas Proactive protocols can (but not necessarily) result in higher overhead due to continuous route updating.

## 6 Security In Manets

Ad-hoc networks are highly vulnerable to security attacks and dealing with this is one of the main challenges of developers of these networks today. The main reasons for this difficulty are; "Shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among nodes, limited availability of resources, and physical vulnerability." For secure routing in MANET, the following are the requirements: Confidentiality, Authenticity, Integrity, Availability, Accountability / Non-Repudiation, Access Control, Privacy.

Availability refers to the fact that the network must remain operational at all times despite denial of service attacks. Confidentiality ensures that certain information is never disclosed to certain users. Authentication is the ability of a node to identify the node with which it is communicating. Integrity guarantees that a message is never corrupted when transferred. Non-repudiation states that the sender of the message cannot deny having sent it.

An ad-hoc network has extra security requirements caused by its lack of proper infrastructure and the dynamic relationship between the nodes in the network. Because of the lack of infrastructure, accountability is very difficult to determine as there is no central authority which can be referenced when it comes to making trust decisions about other parties in the network. The dynamic relationship between the nodes leaves very little opportunity for the nodes to form trust relationships with each other. In an ad-hoc network, nodes must act as both terminals and routers for other nodes. Because there are no dedicated nodes, a secure routing protocol is needed. Multi hop routing protocols are usually employed. These can lead to problems due to non-cooperating nodes and denial of service attacks.

## 7 Security Attacks In Manets

Mobile ad hoc networks are the future of wireless networks. Because they're practical, versatile, simple, easy to use and inexpensive. The promise of mobile ad hoc networks to solve challenging real-world problems continues to attract attention from industrial and academic research projects. Applications are emerging and widespread adoption is on the horizon. Most previous ad hoc network research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require secure communication and routing. Applications that may require secure communications include emergency response operations, military or police networks, and safety-critical business operations such as oil drilling platforms or mining operations. For example, in emergency response operations such as after a natural disaster like a flood, tornado, hurricane, or earthquake, ad hoc networks could be used for real-time safety feedback; regular communication networks may be damaged, so emergency rescue teams might rely upon ad hoc networks for communication

### 7.1 Modification

Modify the protocol fields of control messages, compromise the integrity of routing computation and cause network traffic to be dropped, redirected to a different destination or take a longer route.

### 7.2 Wormhole Attack

Colluding attackers uses “tunnels” between them to forward packets, it places the attacker in a very powerful position. The attackers take control of the route by claiming a shorter path.

### 7.3 Denial of Service Attack

Adversary floods irrelevant data consume network bandwidth and consume resource of a particular node.

### 7.4 Rushing Attack

Directed against on-demand routing protocols. The attacker hurries route request packet to the next node to increase the probability of being included in a route.

## 8 Wormhole Attack

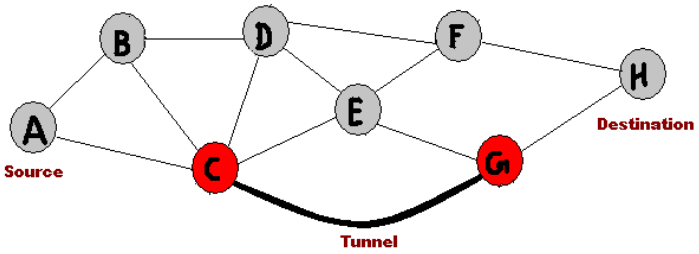
We are going to handle the detection of wormhole attack and provide a solution for it. In wormhole attack, a tunnel is created between two nodes that can be used to secretly transmit packets. In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network and then replays them into the network from that point. 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 sooner than other packets transmitted over 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. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole.

If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network and the attacker could exploit this position in a variety of ways; the attacker can also still perform the attack even if the network communication provides confidentiality and authenticity and even if the attacker does not have any cryptographic keys.

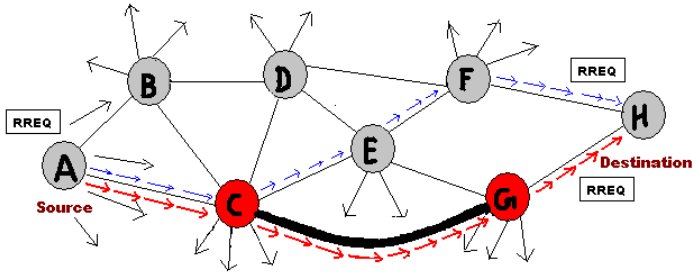
The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. For example, when used against an on-demand routing protocol such as DSR or AODV, a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbors hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST and then

discard without processing all other received ROUTE REQUEST packets originating from this same Route Discovery.

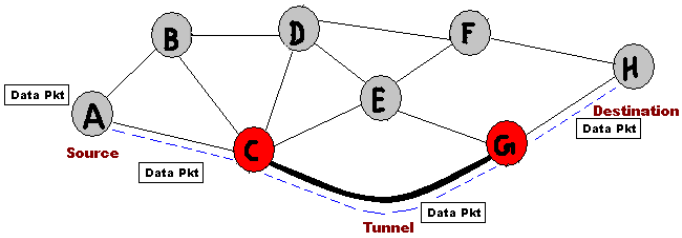
This attack thus prevents any routes other than through the wormhole from being discovered and if the attacker is near the initiator of the Route Discovery, this attack can even prevent routes more than two hops long from being discovered. Possible ways for the attacker to then exploit the wormhole include discarding rather than forwarding all data packets, creating a permanent Denial-of-Service attack (no other route to the destination can be discovered as long as the attacker maintains the wormhole for ROUTE REQUEST packets), or selectively discard or modify certain data packets.




The wormhole tunnel exists between the two malicious nodes C and G. When node A wants to send data to node H, it will broadcast a RREQ packet to all its neighbors. The malicious node C on receiving this RREQ will immediately forward to the malicious node G through the tunnel. The node G forwards the RREQ packet to the destination H and to node F. the node F will now discard the RREQ packet arriving from the normal multihop route. This prevents nodes from discovering legitimate paths that are more than two hops away.




The two colluding malicious nodes thus give a false illusion that the route through them is the shortest, even though they may be many hops away. Thus the route through the malicious nodes is selected and the data packets are forwarded through this.




Many solutions were proposed to solve this worm hole attack. A packet leash as a general mechanism for detecting and thus defending against wormhole attacks. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. We distinguish between geographical leashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed of light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet traveled further than the leash allows.

Packet leashes provide a way for a sender and a receiver to ensure that a wormhole attacker is not causing the signal to propagate farther than the specified radius. When geographic leashes are used, nodes also detect tunneling across obstacles otherwise impenetrable by radio, such as mountains. As with other cryptographic primitives, a malicious receiver can refuse to check the leash, just like a malicious receiver can refuse to check the authentication on a packet. This may allow an attacker to tunnel a packet to another attacker without detection. A malicious sender can claim a false time stamp or location, causing a legitimate receiver to have mistaken beliefs about whether or not the packet was tunneled. When geographic leashes are used in conjunction with digital signatures, nodes may be able to detect a malicious node and spread that information to other nodes

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. Each node that hears the HELLO message sends its identity and an encrypted message, containing the identity of the announcer and a random challenge nonce, back to the announcer. 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.

Another approach is sending acknowledgment to packets to discover wormholes in the path. This approach introduces overhead of control messages and does not isolate the malicious nodes. Radio Frequency (RF) watermarking is another possible approach to providing the security. If the radio hardware is kept secret, such as through tamper-resistant modules, some level of security can be provided against compromised nodes; however, if the radio band in which communications are taking place is known, then an attacker can attempt to tunnel the entire signal from one location to another. It may be possible to modify existing intrusion detection approaches to detect a wormhole attacker; since the packets sent by the wormhole are identical to the packets sent by legitimate nodes, such detection would more easily be achieved jointly with hardware able to specify some sort of directionality information for received packets.

## 9 AODV

Adhoc On-Demand Distance vector (AODV) algorithm provides dynamic, self starting and multi hop routing between

the nodes. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner.

Types of messages are Route Requests (RREQs), Route Replies (RREPs) and Route Errors (REERs). Whenever a route is required for a particular destination a route request (RREQ) packet is broadcast This broadcast message propagates through the network until it reaches an intermediate node that has recent route information about the destination or until it reaches the destination node. Whenever an intermediate node forwards the route request packet, it records in its own tables which node the route request came from. This route information is used to form the reply path for the route reply (RREP) packet as AODV uses only symmetric links. As RREP packet traverses back to the source, the nodes along the reverse path enter their routing information in their tables. Nodes monitor the link status of next hops in active routes. Whenever a link failure occurs, the source is notified with a route error (RERR) message and a route discovery may be requested again if needed. The RERR message indicates those destinations which are now unreachable due to the loss of the link.

A node disseminates a RREQ when it determines that it needs a route to a destination and does not have one available. This can happen if the destination is previously unknown to the node or if a previously valid route to the destination expires or is marked as invalid. The Destination Sequence Number field in the RREQ message is the last known destination sequence number for this destination and is copied from the Destination Sequence Number field in the routing table. If no sequence number is known, the unknown sequence number flag MUST be set. The Originator Sequence Number in the RREQ message is the node's own sequence number, which is incremented prior to insertion in a RREQ. The RREQ ID field is incremented by one from the last RREQ ID used by the current node. Each node maintains only one RREQ ID. The Hop Count field is set to zero.

If a node receives a route request for a destination, and either has a fresh enough route to satisfy the request or is itself the destination, the node generates a RREP message. This node copies the Destination IP Address and the Originator Sequence Number in RREQ message into the corresponding fields in the RREP message. Processing is slightly different, depending on whether the node is itself the requested destination, or instead if it is an intermediate node with a fresh enough route to the destination.

A Route Error (RERR) message may be either, unicast, or iteratively unicast to all neighbors A node should not generate more than RERR_RATELIMIT RERR messages per second.

A node initiates processing for a RERR message in three situations:

1. If it detects a link break for the next hop of an active route in its routing table while transmitting data, or

2. If it gets a data packet destined to a node for which it does not have an active route and is not repairing (if using local repair), or

3. If it receives a RERR from a neighbor for one or more active routes.

Currently, AODV does not specify any special security measures. Route protocols, however, are prime targets for impersonation attacks. If there is danger of such attacks, AODV control messages must be protected by use of authentication techniques. In particular, RREP messages should be authenticated to avoid creation of spurious routes to a desired destination. Otherwise, an attacker could masquerade as the desired destination, and maliciously deny service to the destination and/or maliciously inspect and consume traffic intended for delivery to the destination. RERR messages, while less dangerous, should be authenticated in order to prevent malicious nodes from disrupting valid routes between nodes that are communication partners.

## 10. Proposed Solution

We intend to solve the attack by reducing the probability of the wormhole tunnel being used. This can be done by collecting the RREQs for a particular time period and storing it in a request table. From the table of requests one request is selected and taken up for processing. One of the main reasons for this wormhole attack is that the request packets are quickly forwarded through the tunnel, so finding the node from which the packets arrive sooner most of the time can identify the malicious node. The tunnel is thus identified by finding the next hop of the malicious node from which it gets the packet most of the time. After the tunnel is identified, both the malicious nodes forming the tunnel are removed from the network.

The solution can be divided into three modules as follows:

1. Collecting the Route Requests (RREQs) for a specific time period and randomly choosing one of them for the processing.

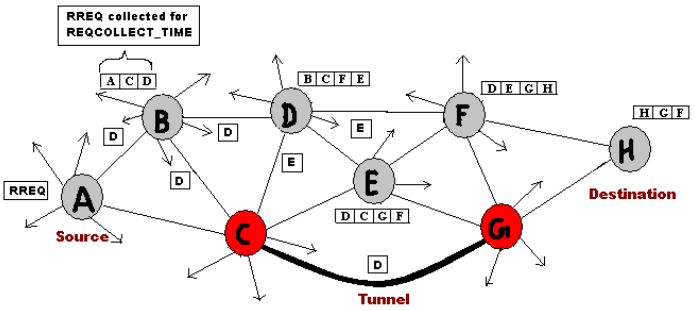
2. Identifying the malicious node.

3. Identifying the wormhole tunnel.

Each of the above modules is explained with an example as follows.

### 10.1 Collecting Route Request Packets

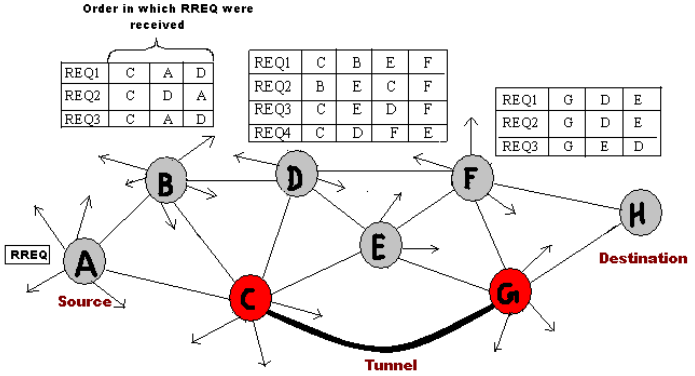
When node A wants to transmit data to node H, it broadcasts the RREQ to all its neighbors (B, C,). The neighbors collect the RREQs forwarded to it by all the other nodes for a specific time period (REQCOLLECT_TIME) and store it in a table (ReqTable). Once the time period expires, it selects a RREQ randomly and forwards it for further processing. For example, the node B collects the requests from nodes A, C, D for the REQCOLLECT_TIME and selects the RREQ from node D for processing.




### 10.2 Identifying the malicious node

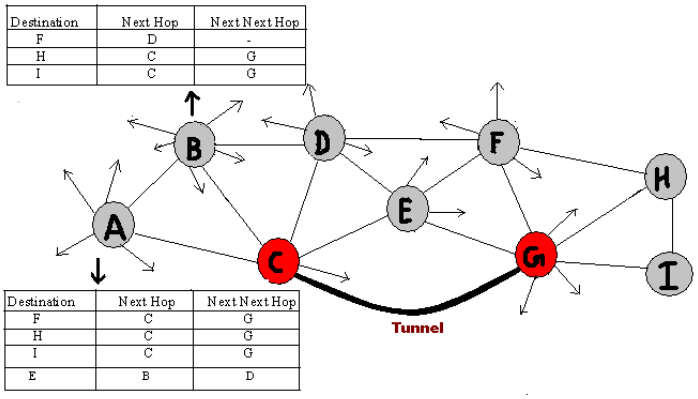
The identification of malicious node is done by analyzing the

ReqTable. The node from which the RREQ was received first most of the time is termed as the malicious node as the packets forwarded by the malicious nodes arrive sooner than the normal multihop route as the tunnel exists between the nodes which are many hops away. For example, the node B receives the RREQ from node C first for three times, so node C is considered to be malicious.

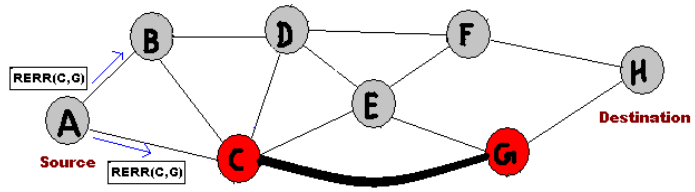



### 10.3 Identifying the Wormhole tunnel

After the malicious node is identified, the next hop of the malicious node for each of the route selected is stored in a table. If the next hop of the malicious node is consistent for 3 or 4 times, then a tunnel is said to be existing between the malicious node and that next hop. For example, the node A finds node G to be next hop of node C (malicious) for 3 times and so node G is also said to be malicious and thus tunnel exists between them.




Once the tunnel is identified, the neighboring nodes are intimated about the malicious nodes via Route Error message.




On receiving the RERR packets, the nodes will remove the entry of the corresponding malicious nodes from their tables.

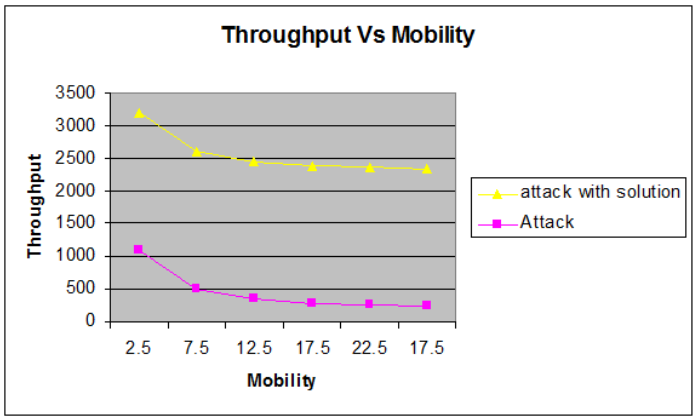
## 11. Results

The proposed solution is analyzed by comparing the throughput for the Wormhole attack and the Wormhole attack with the solution.

The results of the analysis are:

| Mobility | Throughput for the Wormhole Attack | Throughput for the proposed solution |
|---|---|---|
| 2.5 | 1092 | 2102 |
| 7.5 | 498 | 2102 |
| 12.5 | 341 | 2101 |
| 17.5 | 279 | 2101 |
| 22.5 | 252 | 2101 |
| 27.5 | 231 | 2101 |

The following graph for the above data proves that the proposed solution increases the throughput to a great extent when compared to the attack.




## 12 Conclusion And Future Work

### 12.1 CONCLUSION

1) Increase in the throughput when compared to the original attack.

2) Slight increase in the delay due to the additional processing.

3) Slight increase in the overhead due to the additional processing.

### 12.2 FUTURE WORK

In the future, we can try to increase the throughput drastically when compared to the original attack and we should see to that there is no delay due to the processing and also there is negligible overhead.

## References

• Yih-Chun Hu, Adrian Perrig, David B. Johnson,"Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", September 2002

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

• L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang , Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach, University of Washington,2003

• Charles E. Perkins, Ad hoc On-Demand Distance Vector (AODV) Routing draft, IETF