DETECTION AND MITIGATION OF WORMHOLE ATTACKS IN MOBILE AD HOC NETWORKS

A DISSERTATION

Submitted in partial fulfillment of the requirements for the award of the degree of

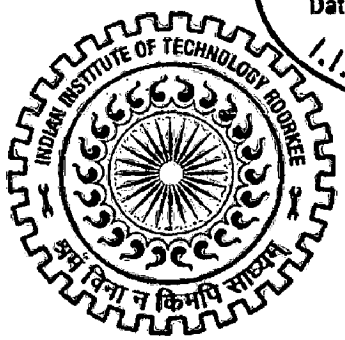
MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

MAHALE RAHUL MACHHINDRA



DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE -247 667 (INDIA)

JUNE, 2010

Candidate Declaration

I hereby declare that the work being presented in the dissertation report titled **"Detection and Mitigation of Wormhole Attacks in Mobile Ad Hoc Networks"** in partial fulfillment of the requirement for the award of the degree of **Master of Technology** in **Computer Science and Engineering**, submitted in the Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, is an authentic record of my own work carried out under the guidance of Dr. A. K. Sarje in the Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee. I have not submitted the matter embodied in this dissertation report for the award of any other degree.

Dated:
Place: IIT, Roorkee

Mahale.
(Mahale Rahul Machhindra)

Certificate

This is to certify that above statements made by the candidate are correct to the best of our knowledge and belief.

Dated: 8/6/2010
Place: IIT, Roorkee

Dr. A. K. Sarje,
Professor,
Department of Electronics and
Computer Engineering
Indian Institute of Technology,
Roorkee.

ACKNOWLEDGEMENT

It is my proud privilege to express my sincere regards to my Dissertation guide Dr. A. K. Sarje, Professor, Department of Electronics and Computer Engineering, Indian Institute of Technology, Roorkee, for their kind cooperation, invaluable guidance and constant inspiration through the various stages of the Dissertation work. I have deep sense of admiration for his innate goodness and inexhaustible enthusiasm. The valuable discussions and suggestions that I had with him have undoubtedly helped in supplementing my thoughts in the right direction for attaining the desired objective.

I am also grateful to all faculty members and staff of Electronics and Computer Engineering Department, Indian Institute of Technology, Roorkee for their kind support.

Special thanks to IIT Roorkee, for providing the necessary facilities to carry out this dissertation work.

I thank Mr. Sandeep Sood and Mr. Tirumalesh for their valuable support, which was helpful in making this dissertation work a success.

Last but not least I would like this opportunity to pay my humble respect and special thanks to my parents for their love, care, and support and my friends Padmaja, Mangesh, Bharat, Sarika, Ragini, Sathish, Sanketh; my sister Kavita and my brother Sachin who directly or indirectly helped me to complete this Dissertation successfully.

Dated: June 2010

Place: IIT Roorkee **(MAHALE RAHUL MACHHINDRA)**

CONTENTS

List of Figures

List of Acronyms

CBR	Constant Bit Rate
JiST	Java in Simulation Time
JVM	Java Virtual Machine
MANET	Mobile Ad hoc Network
MHA	Manet Hop Count Analysis
MPR	Multi Point Relay
OLSR	Optimized Link State Routing
SWAN	Scalable Wireless Ad hoc Network Simulator
TC	Topology Control
WA	Wormhole Avoidance
UDP	User Datagram Protocol

Abstract

The basic characteristic of MANET's is that nodes depend on their neighbouring nodes for routing and forwarding. Because of this nature and its other characteristic like dynamic topology, no central authority etc., manet is vulnerable to many security attacks. The wormhole attack is one of the most severe security attacks in wireless ad hoc networks, in which two or more colluding attacker's tunnel packets from one place to another. From this tunneling they falsely claim to other nodes that they have shorter routes to intercept packets.

In this thesis, we have proposed 2 methods based on Optimized Linked State Routing Protocol. An important effect of wormhole attack is packet dropping. To address this problem we propose a method 1 that correlates the packet sent and receive ratio to find the attacker node and to avoid paths through it. But a wormhole attacker can do more than just packet dropping as described in method 2. We detect such node based on analysis that frequency of using wormhole link is very high compared to other routes. For avoiding such attacker nodes we generate a special type of control packet for suspicious links and detect whether there is a wormhole link based on packet sent and acknowledgement receive timings. Once wormhole nodes are detected, the traffic through wormhole nodes is effectively avoided and throughput of network is maintained.

The proposed technique has been simulated on the java based JiST-Swans simulator using various scenarios.

CHAPTER 1
INTRODUCTION

1.1 Introduction to Ad Hoc Networks

Ad-hoc networks are formed in situations where mobile computing devices require networking applications while a fixed network infrastructure is not available or not preferred to be used. An ad-hoc network can be classified into two main types: mobile ad-hoc network and mobile ad-hoc sensors network.

A mobile ad-hoc sensor or hybrid ad-hoc network consists of a number of sensor spreads in a geographical area. Each sensor is capable of mobile communication and has some level of intelligence to process signals and to transmit data.

A Mobile Ad hoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end-system but also as a router to forward packets. Mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. A MANET is a collection of wireless devices or nodes that communicate by dispatching packets to one another or on behalf of another device/node, without having any central network authority or infrastructure controlling data routing. MANET nodes have limitless connectivity and mobility to other nodes routing, each node acts as a router and network manager to another node. This technology, which is the combination of peer-to-peer techniques, wireless communications, and mobile computing, provides convenient infrastructure-less communications and could be very useful to provide communications for many applications especially when the infrastructure networks is not feasible.

As mobile ad-hoc networks are self-organized networks, communication in ad-hoc networks does not require a central base station. Each node of an ad-hoc network can generate data for any other node in the network. All nodes can function, if needed, as relay stations for data packets to be routed to their final destination. A mobile ad-hoc network may be connected to other fixed networks or the Internet. The multi-hop support in ad-hoc

networks, which makes communication between nodes out of direct radio range of each other possible, is probably the most distinct difference between mobile ad-hoc networks and other wireless communication systems. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. Hence it is essential to use some techniques to protect MANET's from various security attacks.

Similar to other networks, MANET is also vulnerable to many security attacks. MANETs suffer from a variety of security attacks such as: Denial of Service (DoS), flooding attack, impersonation attack, selfish node misbehaving, routing table overflow attack, wormhole attack, blackhole attack, and so forth. In addition to security threats in both wired and wireless networks it has security attacks unique to itself.

A wormhole attack is one of the most sophisticated and severe attacks in MANETs. In the wormhole attacks, a compromised node in the ad hoc networks colludes with other attacker to create a shortcut in the networks. They could claim the source node that they have shorter route to win in the route discovery process and later they can launch the interception attacks.

1.2 Problem Statement

Our aim is to provide an easily implementable method for detecting and avoiding the wormhole attack. It should not add high overhead and also should not require any special hardware.

1.3 Motivation

The open nature of the wireless medium makes it easy for outsiders to listen to network traffic or interfere with it. And also MANET's are open to vulnerabilities as a result of their basic characteristics like: no point of network management, topology changes vigorously, resource restriction, no certificate authority or centralized authority etc.

A wormhole attack is one of the most sophisticated and severe attacks in MANETs. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.

The detection of Wormholes in ad hoc networks is considered to be a challenging task and many research works are going on for detecting and preventing these attacks. A number of recent works have been studied before proposing this new methodology. The proposed solution unlike some of its predecessors does not require any specialized hardware like directional antennas, etc for detecting the attackers.

1.4 Organization of the Report

Chapter 1 introduces the mobile ad hoc networks and motivation to do the work.
Chapter 2 gives the brief information of Optimized Link State Routing in its modified form which has been simulated for implementing our proposed method. It gives brief information about different routing attacks possible in manet and then discusses wormhole attacks in detail. It also describes that how wormhole attack can be formed on OLSR.
Chapter 3 discusses the existing detection and prevention techniques for wormhole attack and their limitations.
Chapter 4 describes our proposed method.
Chapter 5 contains simulation environment used and discussion of results obtained using proposed methods.
Finally the thesis is concluded by analysing the proposed method and modifications possible.

CHAPTER 2

WORMHOLE ATTACK IN MANETS

2.1 Routing protocols in ad hoc networks

Routing is an important mechanism in any type of network. In wired networks two main classes of routing protocols are used in packet switching networks for computer communication. One is Distance Vector routing protocols and the other is Link-State routing protocols.

A distance-vector routing protocol uses the Bellman-Ford algorithm to calculate paths. Distance means how far and Vector means in which direction. Distance Vector routing protocols pass periodic copies of routing table to neighbour routers and accumulate distance vectors. In distance vector routing protocols, routers discover the best path to destination from each neighbour. The routing updates proceed step by step from router to router.

In link-state routing each node maintains an up-to-date view of the network by periodically broadcasting the link state costs of its neighbouring nodes to all other nodes using flooding strategy. When each node gets periodic update packets, it updates its view of the network by applying a shortest path algorithm to choose the next hop node for each destination.

In case of mobile ad hoc networks resources are limited because mostly the devices are operated on battery and also the bandwidth is limited as compared to wired networks. The limited resources in MANETs have made designing an efficient and reliable routing strategy a very challenging problem. An intelligent routing strategy is required to efficiently use the limited resources while at the same time be adaptable to the changing network conditions such as network size, traffic density, and network partitioning. In parallel with this, the routing protocol may need to provide different levels of QoS to different types of applications and users.

The traditional routing protocols do not scale in MANETs, because periodic or frequent route updates in large MANETs may consume a significant part of the available bandwidth, increase channel contention, and require each node to frequently recharge its power supply. To overcome such problems a number of routing protocols have been proposed for MANET's which are classified in three different groups: proactive, reactive and hybrid.

In reactive routing protocols a route to a destination is created only on demand, means only when source requires the route it initiates route discovery process. Examples of reactive protocols are AODV (Ad hoc On-demand Distance Vector), DSR (Dynamic Source Routing), etc.

In proactive routing protocols the node determines routes to all destinations in the network or some part of the network and periodically exchange control packets with neighbours to update the knowledge. Examples of this class are OLSR, DSDV (Destination-Sequenced Distance Vector), etc.

The Hybrid routing protocols combine the advantages of both reactive and proactive approaches into one. Examples of this class are ZRP (Zone Routing Protocol), TORA (Temporally Ordered Routing Algorithm)

2.2 Optimized Link State Routing Protocol

The Optimized Link State Routing Protocol (OLSR) is documented in the experimental Request for Comment (RFC) 3626 [2]. OLSR is table-driven and pro-active and utilizes an optimization called *Multipoint Relaying* for control traffic flooding. In OLSR, link state information is generated only by nodes elected as MPRs.

2.2.1 Control Messages

The core functionality of OLSR defines two message types. All core functionality of OLSR is based on processing and generation of these messages. The third control packet is generated to find wormhole nodes on suspicious links.

1) HELLO message

To keep up to date information of all direct neighbours of node. Each node broadcasts HELLO message periodically. It serves three purposes link sensing, neighbourhood detection and MPR selection signalling.

2) TC Message

In order to build the topology information base, each node, which has been selected as MPR, broadcasts Topology Control (TC) messages. TC messages are flooded to all nodes in the network and take advantage of MPRs. MPRs enable a better scalability in the distribution of topology information. The information diffused in the network by these TC messages will help each node calculate its routing table.

3) Wormhole Avoidance (WA) Packet

This type of packet is generated by a source whenever it finds a suspicious link and flooded towards other end of the link. When a node receives WA packet it is processed as given in section. The format of packet is given below.

0 31

Packet Type	Packet Size
Sequence Number	
Source Address	
Digital Signature of Source	
Destination Address	
Digital Signature of Destination	

Figure 2.1 Packet format of WA packet

Sequence Number: To identify the WA packet, the source inserts a unique sequence number.

Digital Signature: Source and destination both add their digital signatures in the packet.
The Size of the WA packet always remains so that it cannot be encapsulated in other packet

2.2.2 Multipoint Relaying

The idea of multipoint relays is to minimize the overhead of flooding messages in the network by reducing redundant retransmissions in the same region. Each node in the network selects a set of nodes in its 1-hop neighbourhood which may retransmit its messages. This set of selected neighbour nodes is called the "Multipoint Relay" (MPR) set of that node. The

neighbours of node N which are not in its MPR set receive and process broadcast messages but do not retransmit broadcast messages received from node N. This set is selected such that it covers all strict 2-hop nodes.

2.2.3 Routing Table Calculation

Each node maintains a routing table which allows it to route data, destined for the other nodes in the network. The routing table is based on the information contained in the local link information base and the topology set. Therefore, if any of these sets are changed, the routing table is recalculated to update the route information about each destination in the network.
In the proposed protocol one extra field in the routing table is added which contains a list of all 1-hop neighbours of the node.

2.2.4 Advantages of OLSR

- Being a proactive protocol, routes to all destinations within the network are known and maintained before use. There is no route discovery delay associated with finding a new route.

- The routing overhead generated, while generally greater than that of a reactive protocol, does not increase with the number of routes being used.

2.2.5 Limitations of OLSR

- The original definition of OLSR does not include any provisions for sensing of link quality; it simply assumes that a link is up if a number of hello packets have been received recently.

- Being a proactive protocol, OLSR uses power and network resources in order to propagate data about possibly unused routes.

2.3 Attacks against routing protocol in ad hoc networks

Routing is an important mechanism in any type of network. Improper and insecure routing not only degrades performance but also creates many security threats. The main target of attacker here is routing message. Attacks against routing message can be launched in many forms and may have different characteristics such as Passive or active attacks, External or internal attacks. Attacks can be launched by mobile or wired attackers and by Single or multiple attackers. Such attacks can be classified as follows [3, 23]-

A. Modification

Here attacker makes changes to routing message the and thus endanger the integrity of the packets in the networks. It includes two types of attacks

1) Packet misrouting attacks: Here malicious nodes reroute traffic from their original path to make them reach wrong destinations.

2) Impersonation attacks (spoofing attacks): Here a malicious node gets the identity of another node in the network. By impersonating another node, an attacker is able to receive routing messages that are directed to the node it faked.

B. Interception

In interception attacks the attacker gets unauthorized access to the routing messages which are actually not sent to them. These attacks endanger the integrity of the message as it could be modified or analyzed. Following are the examples of the interception attacks-

1) Blackhole Attack: In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.

2) Wormhole Attack: In the wormhole attack, a compromised node in the ad hoc network colludes with external attacker to create a shortcut in the network. It could claim that it has a shorter route to the destination and wins in the route discovery process. Later it can launch the other interception attacks.

3) Routing Packet Analysis Attack: Routing packet analysis is a passive attack. One way to launch this attack is by exploiting the promiscuous mode employed in ad hoc networks. In

the promiscuous mode, if node A is the neighbour of both nodes B and C at a particular time, node A can always hear the transmissions between node B and node C. By exploiting this nature, node A is able to analyze the overheard packets transmitted between node B and node C. Also in multi hop routing, packets need to be forwarded through several intermediate nodes before reaching the actual destination. Malicious nodes might exploit this opportunity by locating themselves in any location along the route to participate in the message forwarding process and later launch the routing packet analysis attacks.

C. Fabrication

Instead of modifying other packets the malicious node could fabricate its own packets to disrupt network operation. The types of such attacks are as follows,

1) Sleep deprivation attacks: Here targeted node is flooded by unnecessary routing packets so that node is unable to participate in the routing mechanisms and may become unreachable by the other nodes in the networks.

2) Route salvaging attacks: are launched by the greedy internal nodes in the networks. In manet there is no guarantee that packet will reach the destination may be because of some network failure or some other attack. In such case misbehaving node may duplicate and retransmit the packets and sending any error message to source.

D. Interruption

Interruption attacks are launched to deny routing messages from reaching the destination nodes.

1) Packet dropping attacks: Here malicious node is the intermediate node and it can drop all or some packets.

2) Flooding attacks: Here targeted node is flooded by unnecessary packets so that it can response to other packets.

3) Lack of cooperation attacks: here some internal node does not cooperate or participate in network operation to save its resources.

2.4 Wormhole Attack

A wormhole attack is one of the most sophisticated and severe attacks in MANETs. It is a colluding type of attack and formed between two or more attackers. Attackers are the nodes that form the wormhole tunnel between them and falsely claim to other nodes that they are neighbours to each other even if actually they are far apart from each other. They claim this to show that they have shorter route to destination to win in the route discovery process. Once this is done first attacker records a packet at one location in the network, tunnels the packet through Wormhole link to another attacker at other location, and replays it there or forms some other attack.

This attack is more challenging because the attack can be performed even if the network communication provides confidentiality and authenticity, and even if the attacker has no cryptographic keys.

Furthermore, the attacker is invisible at higher layers, unlike a malicious node in a routing protocol, which can often easily be named, the presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route.

In Manet's most of the routing protocols, each node depends on information provided by its neighbour for finding the route and forwarding the packet. In this attack attacker nodes provide false information to others and prevent 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.

Once the attacker succeeds in creating wormhole attack next he can launch some other attack denial-of-service (DoS) attack (no other route to the destination can be discovered as long as the attacker maintains the wormhole) or dropping all the data packets.

The neighbour discovery mechanisms of proactive routing protocols such as dynamic destination-sequenced distance-vector (DSDV), optimized link-state routing (OLSR), and topology broadcast based on reverse path forwarding (TBRPF) rely heavily on the reception of broadcast packets as a means for neighbour detection, and are also extremely vulnerable to this attack. For example, OLSR and TBRPF use HELLO packets for neighbour detection, so

if an attacker tunnels through a wormhole to a colluding attacker near node all HELLO packets transmitted by node, and likewise tunnels back to the first attacker all HELLO packets transmitted by, then and will believe that they are neighbours, which would cause the routing protocol to fail to find routes when they are not actually neighbours.

Once the wormhole attackers have control of a link, they can do a number of things to actively disrupt the network. Attackers can drop the packets even if their link is supposed to be forwarding. They can drop all packets, a random portion of packets, or specifically targeted packets. Attackers can also forward packets out of order or can just monitor over some important data.

2.5 Types of Wormhole Attack

The Wormhole attack can be classified based on Wormhole tunnel in two types:
1) In-Band Wormhole attack 2) Out Band Wormhole attack

1) In Band Wormhole attack
Here one attacker encapsulates the actual data packet into its own packet destined to other attacker and then transmits it using existing wireless network.
An in-band wormhole can be a preferred choice of attackers and can be potentially more harmful as it does not require any additional hardware infrastructure and consumes existing communication medium capacity for routing the tunnelled traffic.

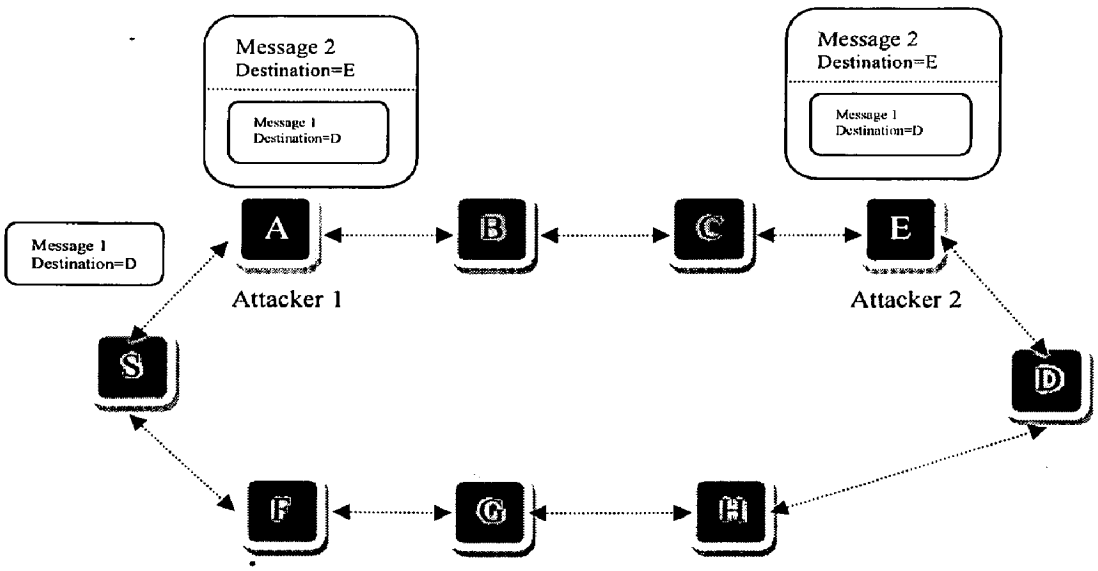


Figure 2.2 Example of In Band Wormhole Attack

For example, in figure 2.1 attackers A and E claim that they are neighbours. When S sends data packet to D, A encapsulates it in its own packet and transfers it to other attacker E. Attacker E can then drop the packet or use it for some other attack. Transmission between A and E is independent of route between S and D.

2) Out Band Wormhole attack

Here one attacker is actually connected to the other through a wired link and packets which are to be attacked are directly sent over this link. The attackers do not depend on other nodes for their communication.

If the attacker performs this tunnelling 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.

For example in Figure 2.3, the two attackers A and E have a wired link between them. By claiming that they are neighbours they claim that they have shorter route for transmission between nodes S and D. So S can choose the route going through A and E causing the Wormhole attack to establish.

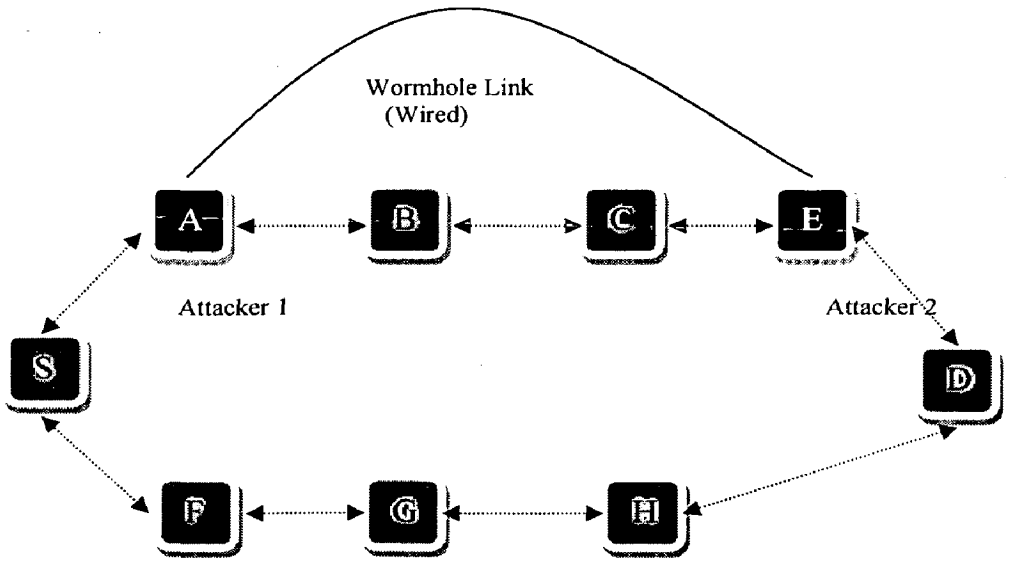


Figure 2.3 Example of Out Band Wormhole Attack

2.6 How Wormhole Attack is formed in OLSR?

In a MANET, nodes which are not within direct communication range of one another must communicate via intermediate nodes, with the packets hopping from neighbour to neighbour until they reach their destination. The route they travel is defined by the routing protocol in use, which determines the network topology.

.A wormhole attack can heavily affect the topology construction in many ad hoc routing protocols, especially proactive routing protocols such as OLSR, which periodically exchange control packets for neighbour discovery and topology construction.

OLSR uses two kinds of the control messages: Hello and Topology Control (TC). Hello messages are used for finding the information about the link status and the host's neighbours. TC messages are used for broadcasting information about own advertised neighbours which includes at least the MPR Selector list. HELLO message are exchanged periodically between direct neighbours only and contain the list of direct neighbours of the node.

In figure 2.4 A and E are two attackers. A and E directly tunnel their HELLO packets to each other. Attacker A includes the E as its direct neighbour in its HELLO message which is sent to all other neighbours of A. The other neighbours of A will assume that E is also a direct neighbour to A. Similarly E also broadcasts false information to its other neighbours.

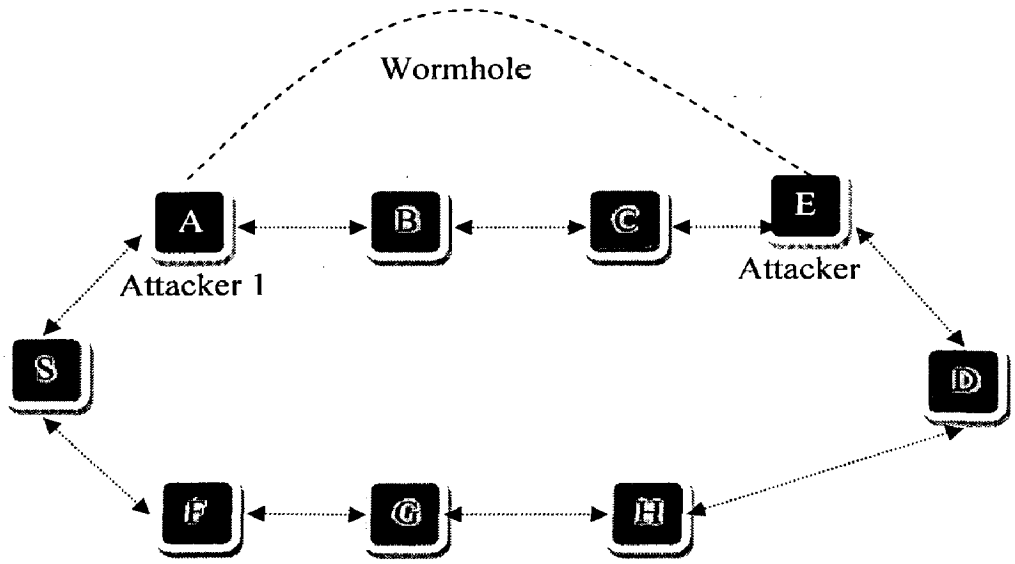


Figure 2.4 Formation of Wormhole Tunnel

Once this spoofed-symmetric link is established, S and E are very likely to choose each others as multi-point relays (MPRs) which then lead to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel.

Although there are other routes from S to D, because of the wormhole, other routes are certainly more than two hops long. So the route through wormhole tunnel has higher priority over other routes. Moreover, in OLSR, only MPR nodes can forward TC messages, so selecting MPRs that forward false topology information will result in the spread of incorrect topology information throughout the network. This leads to routing disruption and ultimately results in significant performance degradation of the ad hoc network as a whole.

CHAPTER 3

EXISTING TECHNIQUES FOR WORMHOLE ATTACK PREVENTION

3.1 Existing Techniques for Wormhole Attack Prevention

3.1.1 Packet Leash

Packet Leash is a mechanism to detect and defend against wormhole attacks [4, 5]. The mechanism proposes two types of leashes for this purpose: Geographic and Temporal. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance.

In Geographic Leashes, each node knows its precise position and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance anytime information to deduce whether the received packet passed through a wormhole or not.

To construct a geographical leash, in general, each node must know its own location, and all nodes must have loosely synchronized clocks. When sending a packet, the sending node includes in the packet its own location, ps, and the time at which it sent the packet, ts; when receiving a packet, the receiving node compares these values to its own location, pr, and the time at which it received the packet, tr. If the clocks of the sender and receiver are synchronized to within $\pm\Delta$, and 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. Specifically, based on the timestamp ts in the packet, the local receive time tr, the maximum relative error in location information δ, and the locations of the receiver pr and the sender ps, then dsr can be bounded by $dsr <= ||ps - pr|| + 2v \cdot (tr - ts + \Delta) + \delta$.

In Temporal Leashes, all nodes are required to maintain a tightly synchronized clock but do not rely on GPS information. When temporal leashes are used, the sending node append the time of transmission to each sent packet *ts* in a packet leash, and the receiving node uses its

own packet reception time *tr* for verification. The sending node calculates an expiration time *te* after which a packet should not be accepted, and puts that information in the leash.
The receiver is able to detect if the packet travelled too far, based on the claimed transmission time and the speed of light

3.1.2 Directional Antennas

Hu and vans propose a solution to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas in [6]. In this technique nodes use specific 'sectors' of their antennas to communicate with each other. For each node some nodes from different sectors are chosen as verifier nodes. Verifier nodes have to examine the direction of received signals from its neighbour. Hence, the neighbour relation is set only if the directions of all verifier nodes match. This is a Good solution for networks relying on directional antennas, but not directly applicable to other type of networks.

3.1.3 Network Visualization

Wang and Bhargava [7] introduce an approach in which network visualization is used for discovery of wormhole attacks in stationary sensor networks. In their approach, each sensor estimates the distance to its neighbours using the received signal strength. All sensors send this distance information to the central controller, which calculates the network's physical topology based on individual sensor distance measurements. With no wormholes present, the network topology should be more or less flat, while a wormhole would be seen as a 'string' pulling different ends of the network together.

3.1.4 Graph Theoretic Approach

Lazos et al [8] proposed a 'graph-theoretical' approach to wormhole attack prevention based on the use of Location-
Aware 'Guard' Nodes (LAGNs). Lazos uses 'local broadcast keys' - keys valid only between one-hop neighbours - to defy wormhole attackers: a message encrypted with a local key at one end of the network cannot be decrypted at another end. Lazos proposes to use hashed messages from LAGNs to detect wormholes during the key establishment. A node can detect certain inconsistencies in messages from different LAGNs if a wormhole is present. Without

a wormhole, a node should not be able to hear two LAGNs that are far from each other, and should not be able to hear the same message from one guard twice.

In [19] Maheshwari et al proposes a novel algorithm for detecting wormhole attacks in wireless multi-hop networks. The algorithm uses only connectivity information to look for forbidden substructures in the connectivity graph.

3.1.5 Neighbourhood Based Approach

Khalil et al [9] propose a protocol for wormhole attack discovery in static networks they call LiteWorp. In LiteWorp, once deployed, nodes obtain full two-hop routing information from their neighbours. While in a standard ad hoc routing protocol nodes usually keep track of their neighbours are, in LiteWorp they also know who the neighbours' neighbours are, - they can take advantage of two-hop, rather than one-hop, neighbour information. This information can be exploited to detect wormhole attacks. Also, nodes observe their neighbours' behaviour to determine whether data packets are being properly forwarder by the neighbour.

3.1.6 Based on Statistical Analysis

Song et al [14] proposes a wormhole discovery mechanism based on statistical analysis of multipath routing. Song observes that a link created by a wormhole is will be selected and requested with very high frequency as it only uses routing data already available to a node. These factors allow for easy integration of this method into intrusion detection systems only to routing protocols that are both on-demand and multipath.

3.1.7 Packet Timing Analysis

In [11] Mason, Gorlatoval et al studies a statistical property of the OLSR network management traffic in the MANET and proposes an intrusion detection system that detects intruder by monitoring HELLO message intervals.

For the valid station, the HELLO Message Timing Intervals appear as a random sequence in some range. Its frequency profile does not fit the OLSR protocol specifications. HELLO messages are not sent at a set frequency; the interval between packets is repeatedly much larger than it should be for a valid station.

One possible way to prevent wormholes, as used by Roy, Chaki et al in [10] is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determines whether the calculated distance is within the maximum possible communication range: Approaches based on RTT that one node sends a packet to another; the answer should arrive very shortly, ideally within the amount of time a wireless signal would travel between the nodes. If there is a wormhole attacker involved, packets end up travelling farther, and thus cannot be returned within a short time.

3.1.8 Based on Probability Distributions

In [12] Khabbazian, Vijay Bhargava et al analysed the effects of wormhole attacks based on probability distributions and proposed a robust and secure on demand distance vector routing protocol to counter the wormhole attack launched in the hidden or participation mode. The proposed protocol uses digital signatures, destination acknowledgments and fault reports in order to remove the faulty links. The proposed protocol uses similar cryptographic primitives as ARAN, thus it can employ most of its optimization techniques. It is shown that two malicious nodes can disrupt 32% of all communications across the network when they initiate a wormhole attack.

3.1.9 Based on HOP Count Analysis

Jen et al [13] propose a new protocol MHA based on Hop Count Analysis. 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. In MHA examine the hop-count values of all routes. Then a safe set of routes for data transmission is chosen.

3.1.10 Secure Multipath Routing

Tirumalesh et al [15] proposed a multipath DSR protocol and a secure extension for it to avoid wormhole attacks. The multipath DSR adds only legitimate neighbours into its neighbour list. The extension is based on fixed size of RREPLY messages.

3.2 Limitations of Existing Techniques

- Most of the methods require specialized hardware to achieve accurate time synchronization or time measuring, or to transmit maximum power in a particular direction, or to locate the location of the node. Also the level of time synchronization required for Temporal leashes is impractical to achieve.

- Geographical leashes provide a Robust and straightforward solution but also inherit general limitations of GPS technology. GPS is a nuisance for personal laptops and also it adds extra cost of GPS devices. GPS systems are not versatile, as GPS devices do not function well inside buildings, under water, in the presence of strong magnetic fields.

- Most of the methods which do not require specialised hardware cannot detect a wormhole attack of all types like Exposed Wormhole attack. Also most methods detect the wormhole attack which causes Packet dropping. But Wormhole attack can do much more than that.

- Solutions given in [6] are good for networks relying on directional antennas, but not directly applicable to other networks.

- For some methods as in [4, 5] the nodes should know its location. It is Good solution for sensor networks but not readily applicable to mobile networks.

- Techniques based on Packet Timing Analysis as in which uses RTT, are incompatible with 802.11 MAC protocol. So these approaches do not seem practical.

- Neighbourhood based methods used in works well with only static stationary networks because for mobile networks neighbourhood of nodes keep on changing after some time.

- Statistical Analysis techniques given in require the information like link frequency etc which is available through multiple paths only. It works only with multi-path, on-demand protocol. Likewise most proposed approaches are specific to some type of routing protocol.

CHAPTER 4
PROPOSED WORK

In this chapter proposed methods with two different cases of wormhole attack are discussed. In first case wormhole attacker drops all the packets it receives for forwarding. In second case packets are not dropped but all are forwarded.

Following assumptions are considered in the design of these methods.

1. All the nodes are available with unique digital signature and other node can't get this signature.
2. The attacker cannot change the contents of the packet.
3. All the nodes know the maximum transfer unit (MTU) of the network.
4. Attacker nodes cannot fragment and reassemble packets without losing the digital signature.
5. All the links are bi-directional.

4.1 Method 1: Using Packet Delivery Ratio of Node

One method for detecting and avoiding wormhole attack nodes is to monitor the behaviour of neighbours and rate them based on the packet it receives and packet it delivers. Assuming that a wormhole drops all the packets it receives as in blackhole, a wormhole in such a system should has the least ratio of packets sent to packets received and hence can be easily eliminated.

In this model each node maintains two counters for each of its direct neighbours one packet sent counter and second packet received counter. Whenever a node receives a data packet from its neighbour it increments its packet receive counter by 1, similarly when it forwards some packet to that node it increments its packet sent counter by 1. This information is stored periodically for different intervals.

Both these counters are inserted in HELLO message with the neighbour's information. Other nodes particularly MPR's get the counters from all nodes and find the ratio between packet

sent and packets received. As the wormhole node drops the number of packets, the difference between these counters is very high for wormhole nodes.

If a node finds the ratio for a node very high, it declares the node as malicious node and also broadcasts this information in TC message to other nodes. All nodes avoid sending the traffic using this malicious node.

The above method avoids all type of wormhole present in the network. The limitation of above method is that it only detects the wormholes which cause packet drops. But wormholes can do much more than that. They can drop all packets, a random portion of packets, or specifically targeted packets. Attackers can also forward packets out of order or can just monitor over some important data.

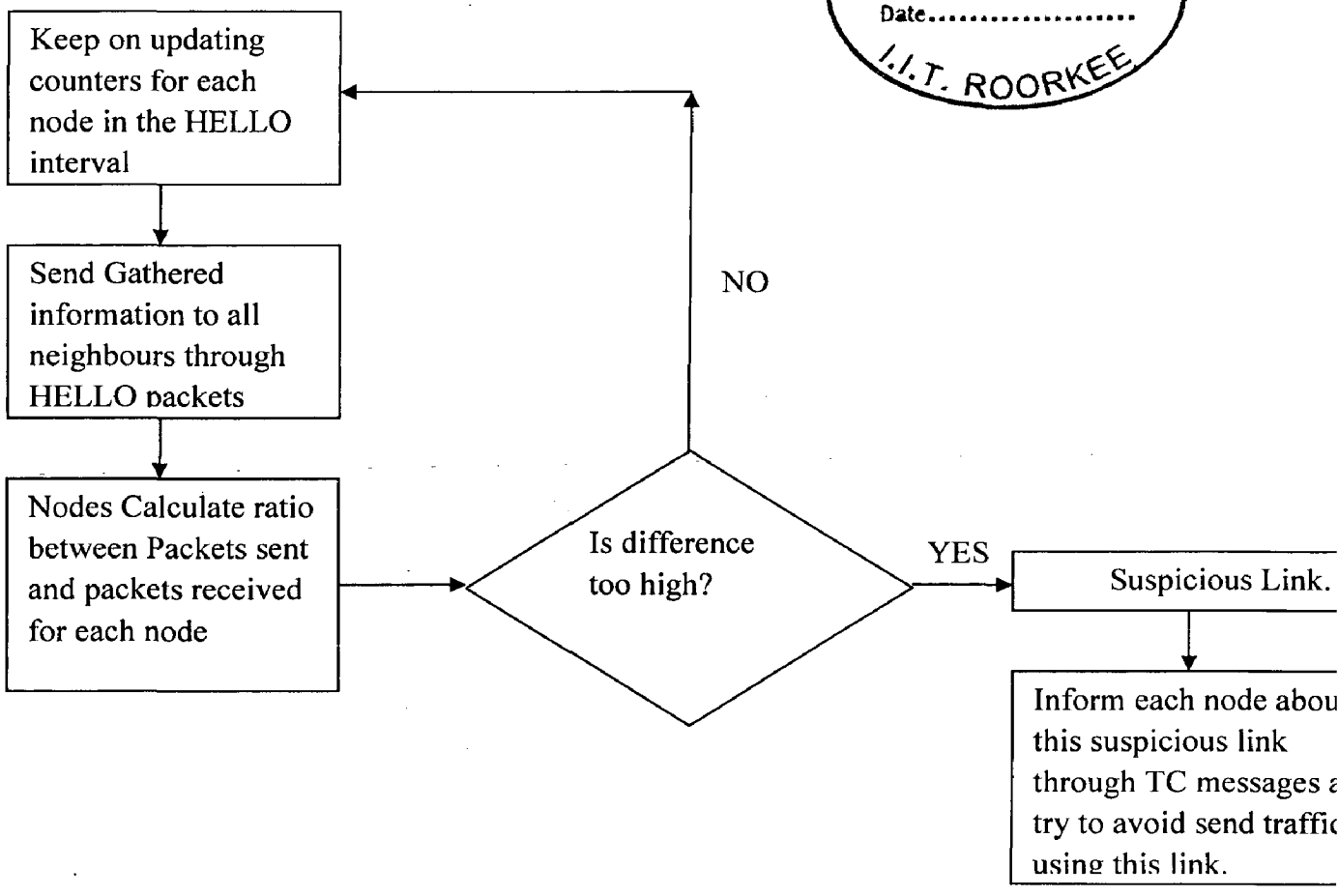


Figure 4.1 Flow Chart for detecting and avoiding Wormhole in method 1

4.2 Method 2

4.2.1 Detection of Wormhole

Here for detecting wormhole attackers same procedure as above is used. Wormhole attackers always predict that they have shorter route to destination as compared to other routes. So they always win in the route discovery process. Wormhole link is used most of the times. If suppose wormhole attacker is not dropping the packets, but instead it is forwarding all the traffic then the packet delivery ratio for these nodes is very high compared to other nodes in the network. If packet delivery ratio for the nodes on a specific link is very high it is declared as a suspicious link.

4.2.2 Mitigation of Wormhole Nodes

For suspicious links a special type of control packets (WA packets) is generated as follows.

1) The node which found that link is suspicious generates WA packet for the node which is at 2-hop distance on the suspicious link and sends it through 1-hop neighbour on the same link. It adds its digital signature inside the packet.

2) The sender node waits for the time equal to 4T. 4T represents the time required by the packet to travel the distance up to 2 HOP neighbour of the node and come back from there. T is described as below.

The Round Trip Travel Time (RTT) δ of a message in a wireless medium is related to the distance d between nodes, assuming that the wireless signal travels with a speed of light v [11].

$$d = \frac{(\delta v)}{2} \qquad \text{..... (1)}$$

If node is not in the transmission range then,

$$\delta < \frac{2R}{v} \quad \text{Where, R=Transmission range.} \qquad \text{..... (2)}$$

From the above equations of RTT, the equation for 1-way propagation delay can be obtained.

$$T = \frac{R}{v} + C \qquad \text{..... (3)}$$

Where, C=Constant Value
C= R/2*V

3) The destination of WA packet immediately generates the acknowledgement for the WA packet and includes its own digital signature in the acknowledgement.

4) If the initiator node is getting acknowledgement from destination within this time it means the neighbour information provided is true and the 2-HOP neighbour is really within the distance of 2-HOPs.

5) If acknowledgement is received within time period, then the same procedure is repeated for each node on the link. Each node checks if the 2-hop neighbour on the link is whether really at a distance of 2 HOPs.

6) If no acknowledgement is received within this time period then it declares the neighbour node through which it has sent packet as wormhole node.

7) It informs to other nodes through next TC messages about wormhole node present. All nodes try to avoid the use of links that goes through wormhole nodes.

By following above algorithm the node ensures that WA packet is not going through wormhole link. It tries to avoid both Out-band and In-band Wormhole attack.

Size of the WA packet and its acknowledgement is fixed. Whenever a node finds the packet size more than allowed size it reports it to source of the packet and discards the respective packet. The fixed size of WA packet avoids the packet to go through wormhole link because attacker node is not able to encapsulate it inside other WA packet.

CHAPTER 5
SIMULATION RESULTS

5.1 Simulator Details

JiST Architecture

The JiST system architecture consists of four distinct components: a compiler, a bytecode rewriter, a simulation kernel and a virtual machine. One writes JiST simulation programs in plain, unmodified Java and compiles them to bytecode using a regular Java language compiler. These compiled classes are then modified, via a bytecode-level rewriter, to run over a simulation kernel and to support the *simulation time* semantics described shortly. The simulation program, the rewriter and the JiST kernel are all written in pure Java. Thus, this entire process occurs within a standard, unmodified Java virtual machine (JVM).

The benefits of this approach to simulator construction over traditional systems and languages approaches are numerous. Embedding the simulation semantics within the Java language allows us to reuse a large body of work including the Java language itself, its standard libraries and existing compilers. JiST benefits from the automatic garbage collection, type-safety, reflection and many other properties of the Java language. This approach also lowers the learning curve for users and facilitates the reuse of code for building simulations. The use of a standard virtual machine provides an efficient, highly-optimized and portable execution platform and allows for important cross layer optimization between the simulation kernel and running simulation. Furthermore, since the kernel and the simulation are both running within the same process space we reduce serialization and context switching overheads. In summary, a key benefit of the JiST approach is that it allows for the efficient execution of simulation programs within the context of a modern and popular language. JiST combines simulation semantics, found in custom simulation languages and simulation libraries, with modern language capabilities. This design results in a system that is convenient to use, robust and efficient [24, 25].

SWANS Details

SWANS is a scalable wireless network simulator built atop the JiST platform. It was created primarily because existing network simulation tools are not sufficient for current research needs, and its performance serves a validation of the virtual machine-based approach to simulator construction. SWANS are organized as independent software components that can be composed to form complete wireless network or sensor network configurations. Its capabilities are similar to ns2 and GlomoSim, but are able to simulate much larger networks. SWANS leverages the JiST design to achieve high simulation throughput, save memory, and run standard Java network applications over simulated networks. In addition, SWANS implements a data structure, called hierarchical binning, for efficient computation of signal propagation.

Every SWANS component is encapsulated as a JiST entity: it stores it own local state and interacts with other components via exposed event-based interfaces. SWANS contains components for constructing a node stack as required by our proposed protocol, as well components for a variety of mobility models and field configurations. It allows components to be readily interchanged with suitable alternate implementations of the common interfaces and for each simulated node to be independently configured. Finally, it also confines the simulation communication pattern. For example, Application or Routing components of different nodes cannot communicate directly. They can only pass messages along their own, node stacks. Consequently, the elements of the simulated node stack above the Radio layer become trivially parallelizable, and may be distributed with low synchronization cost. In contrast, different Radios do contend (in simulation time) over the shared field entity and raise the synchronization cost of a concurrent simulation execution. To reduce this contention in a distributed simulation, the simulated field may be partitioned into non-overlapping, cooperating Field entities along a grid [26].

5.2 Simulation Environment

In order to simulate proposed methods first the attacker nodes and wormhole link is created in the network of 100 nodes. First two attackers are placed, one near source and one near

destination and moved away as the simulation progress. Both types of wormhole attacks out-band as well as in-band are created.

In In-band Wormhole attack one attacker inserts the address of other attacker node in its TC message as its 1-HOP neighbours. After the successful creation of wormhole, successive data packets are dropped which decreases the network throughput. For out-band wormhole attack attackers we introduce only propagation delay on the packet, no MAC layer delays.
The Table 5.1 gives the various simulation parameters used in our simulation environment.

Table 5.1 Simulation Parameters

Routing Protocol	OLSR
No. of Malicious Nodes	Varying (2-8)
No. of Nodes	100
Simulation Area	1100x1100 sq.mtrs
Transmission Range	130m
Band Width	2 mbps
Connection Type	CBR
Packet Size	512 Bytes
Node Speed	2-8 m/sec
Mobility Model	Random Waypoint
PathLoss Model	Two-Ray
Spatial Model	Hierarchical Grid
Placement	Random
Fading Model	Zero Fading Model
Transmit Power	15dB
Interference Model	RadioNoiseAdditive

5.3 Analysis of Results

Figure 5.1 shows the effect of both in-band and out-band wormhole attack on a single nodes transmission on a normal OLSR protocol. The effects are due to single wormhole link only. First the wormhole attackers are placed such as one attacker at 1 hop distance from source

and other at 1-hop distance from destination. Here as the attacker is very close it intercepts nearly all the packets and hence the throughput is very low. For next successive results the distance between attacker and source is increased by 1-hop. As the attacker goes away from source, it affects less.

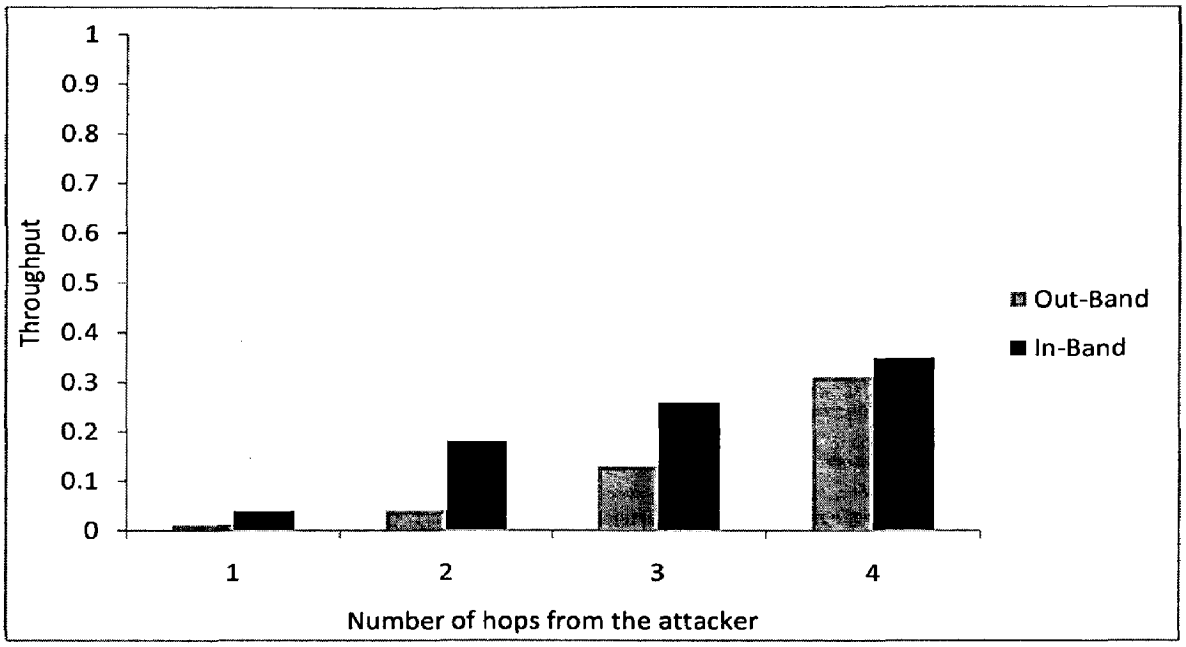


Figure 5.1 Effects of Wormhole Attack

Figure 5.2 below gives the results after simulating the method 1 in the normal OLSR over in-band wormhole attack. Here each node calculates ratio between packets sent and packets received for other node.

And the node for which this ratio is too high, which means node is dropping the packets. We avoid the paths containing such nodes. The method is simulated first by taking 2 attacker nodes then increasing the number of attackers for next turn. The method gives very good improvement over normal OLSR. It cannot achieve the 100% throughput because it takes some time to identify the attacker nodes and till that time attacker drops some number of packets.

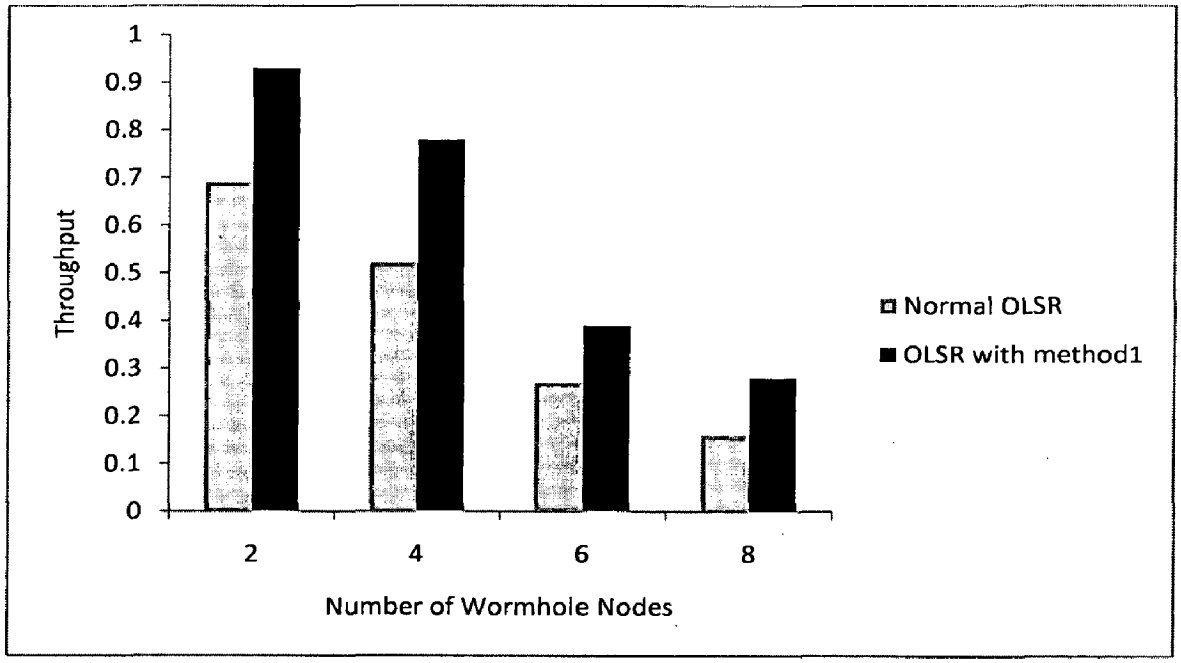


Figure 5.2 Results for Method 1

Figure 5.3 represents the results for method 2 for in-band wormhole attack, where for the link which has very high ratio which represents wormhole link is declared as suspicious link. And WA packet generation algorithm is run for that link.

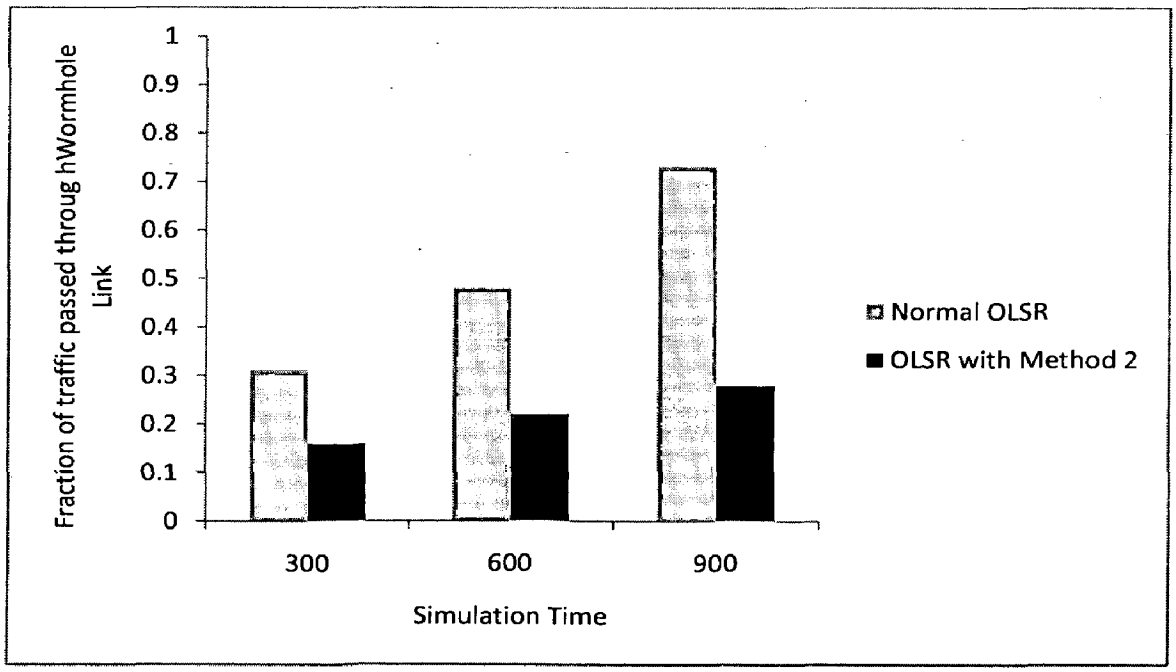


Figure 5.3 Results for Method 2

For taking the results of both methods the throughput of basic OLSR is considered as 100%. Then the wormhole attack is implemented which causes the decrease in the throughput. Only two attackers can disrupt more than 30% traffic. For method 1 throughput further goes down as number of attackers are increased. The maximum decrease in throughput caused by 8 attacker nodes is more than 80%.

For method 2 results are obtained for two attackers and traffic passed through wormhole link is monitored. The results for different simulation times are obtained. In case of normal OLSR as the simulation time is increased the traffic passed through wormhole link also increases proportionally. Method 2 is implemented as described above, which finds the wormhole nodes and prevents passing traffic through it. For the initial time improvement is not much as the method takes the time to detect the suspicious nodes. As time passes for normal OLSR the traffic passed through wormhole links is also increases. For the simulation run with time 300 seconds, almost 30% traffic is passed through wormhole link and it goes more than 70% as time is increased. But for proposed method once it detects wormhole nodes it avoids that paths so traffic passed through wormhole links remains same although simulation time increases.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

In this dissertation work the wormhole attacks in mobile ad hoc networks has been studied. The effects of wormhole attack on OLSR has been analysed and a method is proposed to mitigate its effects. The proposed methods are easily implementable and do not require any special hardware.

In-band wormhole attacks are less powerful as compared to out-band wormhole attacks but they can be easily launched as they make the use of available network resources. Also Only 2 attacker nodes can disrupt more than 30% traffic in the network.

Proposed method 1 gives very good results but it is useful only when the wormhole attackers are dropping the packets. Method 2 works for all cases of wormhole attack. Also both methods are useful in both in-band and out-band wormhole attack. The fixed WA packet size in method 2 avoids the in-band wormhole attack with very less overhead.

The effectiveness of methods has been illustrated. The wormhole nodes are effective initially until the method detects them. Once wormhole nodes are detected, the traffic through wormhole nodes is effectively avoided and throughput of network is maintained.

Though proposed methods works significantly well, yet there is scope for better performance. The technique used here takes significant amount of time before detecting wormhole attackers. Within that time number of packets can be dropped or monitored. Some other detection technique can be used to improve performance. In method 2, the case of bottleneck link is not considered. Bottleneck link is not a wormhole link but is the only link that connects two parts. Such links can be identified from topology set information and are not declared as wormhole links. Also methods proposed here are specific to optimized link state routing. The same mechanism can be modified to work on different routing protocols.

[1] S. Corson, J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," IETF RFC 2501, [Online at http://www.ietf.org/rfc/rfc2501.txt] [Last Accessed on Apr 2010], January 1999.

[2] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)" IETF RFC 3626, [Online at http://www.ietf.org/rfc/rfc3626.txt] [Last Accessed on May 2010], 2003.

[3] Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, volume (2) issue (3) 18, pp. 18-29, year 1999.

[4] 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 Communications. IEEE Societies, Vol. 3, pp. 1976-1986, 3 April 2003.

[5] Y.C.Hu,A. Perrig, and D.B.Johnson, " Wormhole Attacks in Wireless Networks", IEEE JSAC Volume: 24, pp.370-80, 2006.

[6] L.Hu, D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks ", Proceedings of the 11th Network and Distributed System Security Symposium, pp.131, 2004.

[7] S.Kurkowiski, T. Camp, N. Mushell, and M. Colagrosso, "A Visualization and Analysis Tool for NS-2 Wireless Simulations: iNSpect", Proceedings of the 13th IEEE International Symposium on Modelling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), pp.503-506, 2005.

[8] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," In Proc. of IEEE Wireless Communications and Networking Conference, Volume 2, pp 1193-1199, 2005.

[9] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: A lightweight countermeasure for the wormhole attack in multihop," In Proc. of the International Conference on Dependable Systems and Networks (DSN'05), Pages: 612 - 621, 2005.

[10] 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 2, pp. 44-52, April 2009.

[11] Maria A. Gorlatoval, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis" , pp.1-7, MILCOM 2006, October 2006.

[12] Majid Khabbazian, Hugues Mercier and Vijay K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks", IEEE Transactions on Wireless Communications, Volume: 8, Issue 2, Pages: 736-745, 2009.

[13] Shang-Ming Jen, Chi-Sung Laih and Wen-Chung Kuo, "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", *Sensors* 2009, Volume *9, Issue* 6, pp. 5022-5039, 2009.

[14] Lijun Qian, Ning Song and Xiangfang Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path", Parallel and Distributed Processing Symposium, 2005, Proceedings of, 19th IEEE International IPDPS'05, Volume 30, Issue 1, Pages: 308 - 330, 2007.

[15] Tirumalesh C., Kumkum Garg, "Secure Multipath Routing Protocol for detecting and avoiding wormhole attacks", International Conference on Computer and Network Technology -ICCNT 2009, Volume 23, 2009.

[16] Khin Sandar Win, Department of Engineering Physics, Mandalay Technological University, Pathein Gyi, Mandalay, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology, Issue 48, Page 422, 2008.

[17] Farid Nait-Abdesselam, Brahim Bensaou, and Tarik Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", IEEE Communications Magazine, Vol. 46, Issue 4, 2008.

[18] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", WIRELESS/MOBILE NETWORK SECURITY, Springer 2006.

[19] Ritesh Maheshwari, Jie Gao and Samir R Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information", in INFOCOM. IEEE, 2007, pp. 107-115.

[20] Sanzgiri, K.; Dahill, B.; Levine, B.N.; Shields, C.; Belding-Royer, E.M.A. "A Secure Routing Protocol for Ad Hoc Networks." In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), Pages: 78 – 89, Paris, France, November 2002.

[21] P. Nikander, J. Kempf, E. Nordmark, "RFC3756 - IPv6 Neighbor Discovery (ND) Trust Models and Threats", IETF RFC 3756, Online at http://www.ietf.org/rfc/rfc3756.txt] [Last Accessed on Mar 2010], 2004.

[22] Baruch Awerbuch, Reza Curtmola, Herbert Rubens, David Holmer, and Cristina Nita-Rotaru, "On the Survivability of Routing Protocols in Ad Hoc Wireless Networks", IEEE SecureComm, Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Network, Pages: 327 - 338 , September 2005.

[23] S. A. Razak, S. M. Furnell, P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols", Network Research Group, University of Plymouth,2003.

[24] R. Barr, Z.J. Haas, and R. Van Renesse, "JiST: An efficient approach to simulation using virtual machines," Software Practice & Experience, Volume: 35, no. 6, pp. 539-576, 2005.

[25] Rimon Barr, "JiST– Java in Simulation Time User Guide", http://jist.ece.cornell.edu/docs/040319-jist-user.pdf

[26] Rimon Barr, "SWANS– Scalable Wireless Ad hoc Network Simulator User Guide", http://jist.ece.cornell.edu/docs/040319-swans-user.pdf

List of Publications

1. Rahul M. Mahale, A.K. Sarje, "Detection and Mitigation of Wormhole Attacks in Mobile Ad Hoc Networks", Communicated to International Conference on Computer & Communication Technology (ICCCT-2010), MNNIT, Allahabad, 17-19 September 2010.

2. Rahul M. Mahale, A.K. Sarje, "Mobility based Optimized Link State Routing Protocol for Mobile Ad Hoc Networks", Accepted in Fourth International Conference on Information Processing, Bangalore, 6-8 Aug 2010.

A.1 MANETs have several salient characteristics:

1) Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology, which is typically multihop, may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.
2) Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications is often much less than a radio's maximum transmission rate, because of the effects of multiple access, fading, noise, and interference conditions, etc. One effect of the relatively low to moderate link capacities is that congestion occurs usually.
3) Energy-constrained operation: 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.
4) Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered.

A.2 Advantages and application areas

The different examples where manets are useful can be listed as -

1) A group of people with laptop computers at a conference that wish to exchange files and data without mediation of any additional infrastructure.
2) Deploying ad-hoc networks in homes for communication between smart household appliances.
3) Ad-hoc networks are suitable to be used in areas where earthquakes or other natural disasters have destroyed communication infrastructures.
4) Ad-hoc networks perfectly satisfy military needs like battlefield survivability, operation without pre-placed infrastructure and connectivity beyond the line of sight.

There are many characteristics that are used to classify attacks in the ad hoc networks as given in Paper [23]. These are explained as follows.

A. Passive vs. active attacks

Passive Attacks: These are launched to steal valuable information in the targeted networks. e.g. Eavesdropping attacks, Traffic analysis attacks etc.

Detecting these attacks is difficult because system resources or network functions are not physically affected to prove the intrusions. They do not disrupt the network operations.

Active Attacks: These types of attack alter the data and they disrupt the network operations. e.g. Message Modifications, Message replays, message fabrications, Denial of Service attacks etc.

B. External vs. internal attacks

External attacks: These are launched by the attackers who are not part of the network or not authorized to access network operations. These attacks may cause network congestion, denying access to some functions or to disrupt whole network operation.

E.g. impersonation, denial of service, bogus packet injection.

Internal attacks: These attacks are more severe as compared to external attacks. The attackers are the internal authorized nodes inside the network and may be either misbehaving node or compromised nodes.

The compromised nodes are those which are hijacked by some external node and used to launch attacks in the network.

The misbehaving nodes are authorized to use system resources but they are not using it in the way they should use it. They may misbehave to save their limited resources such as communication bandwidth, processing capabilities, battery powers.

C. Mobile vs. wired attackers

Mobile attackers are attackers that have the same capabilities as the other nodes in the ad hoc networks. Since they have the same resources limitations, their capabilities to harm the

networks operations are also limited. e.g. with the limited transmitting capabilities and battery powers, mobile attackers could only jam the wireless links within its vicinity. Since wired attackers have more resources, they could launch more severe attacks in the networks. e.g. Jamming the whole networks.

D. Single vs. multiple attackers

Attackers may attack individually or colluding with other nodes. Single attackers usually generate a moderate traffic load. Since they also have similar abilities to the other nodes in the networks, their limited resources become the weak points to them. However, if several attackers are colluding to launch attacks, defending the ad hoc networks against them will be much harder. Colluding attackers could easily shut down any single node in the network and be capable to degrading the effectiveness of network's distributed operations including the security mechanisms.