DETECTION AND PREVENTION OF WORMHOLE ATTACK ON MULTIPATH ROUTING PROTOCOL OF MOBILE ADHOC 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

RAVINDER

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE-247 667 (INDIA)
JUNE, 2011

CANDIDATE'S DECLARATION

I hereby declare that the work, which is being presented in the dissertation entitled **"DETECTION AND PREVENTION OF WORMHOLE ATTACK ON MULTIPATH ROUTING PROTOCOL OF MOBILE ADHOC NETWORKS"** towards the partial fulfillment of the requirement for the award of the degree of **Master of Technology** in **Computer Science and Engineering** submitted to the Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, Roorkee, India is an authentic record of my own work carried out during the period from July 2010 to June 2011, under the guidance of **Dr. Padam Kumar, Professor, Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee.**

The matter presented in this dissertation has not been submitted by me for the award of any other degree of this or any other Institute.

Date: 29/06/2011
Place: Roorkee

(RAVINDER)

CERTIFICATE

This is to certify that the above statement made by the candidate is correct to the best of my knowledge and belief.

Date: 29/06/2011
Place: Roorkee

(Dr. Padam Kumar)
Professor
Department of Electronics and Computer Engineering
Indian Institute of Technology Roorkee

Acknowledgement

It gives me immense pleasure to express my deepest sense of gratitude towards my guide **Dr. Padam Kumar,** Professor, Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee for his expert guidance, encouragement and support throughout the dissertation work. His suggestions and invaluable ideas provided the platform to the entire dissertation work. In spite of his extremely busy schedule, I have always found him accessible for suggestions and discussions. I look at him with great respect for his profound knowledge and relentless pursuit for perfection. His ever-encouraging attitude and help has been immensely valuable.

Nothing would have been possible without the support of my family members, who have been backing me up throughout my life. I wish to convey my sincere thanks to my parents. I also wish to convey my sincere gratitude to my brother, Pawan and my friend, Vinit. Without their support, it would not be possible to reach this far with my studies.

I would also like to thank all faculty members of Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee for their kind help and support.

Above all, I express my indebtedness to the "**ALMIGHTY**" for all His blessing and kindness.

RAVINDER

Abstract

Mobile Ad Hoc Network (MANET) is a collection of nodes that communicate with each other without any fixed infrastructure. The nodes also act as router which finds routes to other nodes in the network. Routing is an important aspect of MANETs which is used to find the route and to send data from source to destination nodes. Traditionally, routing protocols were focused on performance only. But security is also an important aspect. Due to limited bandwidth, limited storage capacity, dynamic topology, shared medium, open peer to peer communication, security in MANETs is difficult to implement as compared to wired networks. There are number of attacks on routing protocols like routing table overflow attack, black hole attack, wormhole attack, route cache poisoning, sybill attack, modification, fabrication, location spoofing attacks etc. which affect the functioning of MANETs and degrade the performance. So there is need to secure routing protocols so that their functioning is not affected and performance is not degraded due to these attacks.

In this dissertation work, detection and prevention of wormhole attack on multipath routing protocol is proposed. DSR (Dynamic Source Routing) is converted in to multipath routing protocol by changing the way intermediate node forwards the route request packet.

The QualNet 5.0.2 simulator is used to validate the proposed approach. Two new packets Dummy_Request and Dummy_Reply are introduced to check the vulnerability of the path. The format of these packets is same as route reply except the option type. The performance parameters used are packet delivery ratio and throughput. The results show that packet delivery ratio and throughput under wormhole attack is less as compared to protocol without wormhole attack and the MRWDPDP (Multipath Routing Wormhole Detection and Prevention using Dummy Packet) improves the packet delivery ratio and throughput of multipath routing protocol under wormhole attack.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction and Problem Statement

1.1 Introduction

One of most emerging field in today's world is wireless networks. Wireless networks are of two types: Wireless LAN and Wireless Ad Hoc Networks [1]. A Wireless LAN requires the use of access points or base stations to communicate with each other and to provide communication between Internet and other WLANs. In wireless ad hoc networks there is no fixed router and base station. Each node is capable of moving irrespective of another node at his will. Mobile Ad-hoc network falls under this category, and is a set of wireless nodes, which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. Advantages of MANETs [2] are easy deployment, no need of existing infrastructure, low cost etc. and applications of MANETs are search and rescue operation, personal area networks etc. Security is a big issue in today's environment. Due to limited bandwidth, storage capacity and processing capability, it is harder to enforce security in wireless network as compared to wired network.

Routing is important aspect in Mobile Ad Hoc Networks which is used to find the path between nodes and to send and receive packets. Traditionally, routing protocols were focused on the performance but now a day's security is also important. There are number of attacks [3] on routing protocols like packet dropping, modification, fabrication, impersonation, sybill attack, wormhole attack, location spoofing attack etc. But wormhole attack is difficult to identify because it may not modify the packets. It is performed by two or more malicious nodes in conspiracy. Two nodes, even if they are far apart appear single hop away. Therefore routes passing through these nodes are likely to be shorter than normal one. So, source node uses the path through these wormhole nodes. The wormhole nodes then sniff, drop, or selective drop data packets passed through them, due to which performance of routing protocols is degraded.

1.2 Motivation

Traditionally emphasis was on the performance of routing protocol of Mobile Ad Hoc Networks. But security is also important. There are number of attacks like fabrication, modification, wormhole attack, grayhole attack, black hole attack, byzantine attack, rushing attack, etc. that affects the performance of routing protocols. Out of these attack wormhole attack is severe one and hard to detect. It is performed by two or more colluding nodes. There are various solutions given in literature to detect and prevent wormhole attack. Some of them make impractical assumptions like mobility is zero, synchronization between nodes; each node is equipped with special hardware like GPS etc. So solution should be provided so that these attacks should not disturb the functioning of the protocol and does not affect the performance without considering impractical assumptions.

1.3 Problem Statement

The main objective of this dissertation work is to propose an approach for the detection and prevention of wormhole attack on Multipath Routing protocol of Mobile Ad Hoc Networks.

To achieve the main objective, it is further divided in following sub-objectives:

i) To check the effects of wormhole attack on DSR routing Protocol.

ii) To implement Multipath Routing Protocol in QualNet 5.0.2.

iii) To propose and implement approach for detection and prevention of wormhole attack on Multipath Routing Protocol (MRP).

iv) To calculate the performance of MRWDPDP and compare it with Multipath Routing Protocol.

1.4 Organization of Report

The dissertation report is organized in 6 chapters including this chapter. This chapter gives introduction and states the problem. The rest of report is organized as follows.

Chapter 2, overview of Mobile Ad Hoc Networks, Routing in Mobile Ad Hoc Networks and attacks on routing protocol are discussed. The research gaps and literature review is also given in this chapter.

Chapter 3, Proposed Approach is given to detect and prevent wormhole attack on the Multipath Routing Protocol of Mobile Ad Hoc Networks.
Chapter 4, Simulation tool, simulation parameters and the performance metrics are discussed. The QualNet 5.0.2 simulator is used for simulation purpose.

Chapter 5, Results are discussed in this chapter.

Chapter 6 , Concludes the dissertation and discusses the scope for future work.

Chapter 2

Background and Literature Review

2.1 MANETs – Overview

In Latin "ad-hoc" literally means "for this purpose only". Then an ad-hoc network can be regarded as "spontaneous network". A mobile ad hoc network (MANETs) [4] is a collection of nodes that communicates with each other without any fixed infrastructure. Mobile nodes use air as a transmission medium. Nodes which are in transmission range of each other communicate directly. If two nodes are far apart they will relay on other nodes for communication. In MANETs each node also acts as a router. As shown in figure 2.1 Node A relay on node D, B, E to communicate with node C so MANETs is multi-hop.

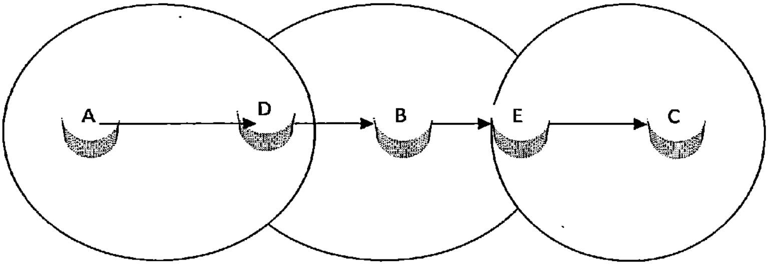


Figure 2.1 Communication between node A and C via node D, B, E.

2.1.1 Characteristics of MANETs

The main characteristics [5] of MANETs are as follows.

- **Dynamic Topology:** In MANETs nodes are free to move so topology of the network changes rapidly at unpredictable times.
- **Bandwidth constraints and variable link capacity:** Wireless links have significantly lower capacity than wired links. Due to the effects of multiple access, multipath fading, noise, and signal interference, the capacity of a wireless link can be degraded over time and the effective

throughput may be less than the radio's maximum transmission capacity.

- **Energy constrained Operation:** Mobile nodes rely on batteries for proper operation. Since an ad hoc network consists of several nodes, depletion of batteries in these nodes will have a great influence on overall network performance. Therefore, one of the most important protocol design factors is related to device energy conservation.
- **Limited physical security:** Mobile wireless networks are generally more vulnerable to security threats than wired networks. The increased possibility of eavesdropping, spoofing, and denial-of-service (DoS) attacks should be carefully considered when an ad hoc wireless network system is designed.

2.1.2 Applications of MANETs

MANETs can be applied to a large variety of use cases, where conventional networking cannot be applied, because of difficult terrain, lacking cost-effectiveness or other reasons. MANET are used in following areas [6]:

- **Tactical Networks:** MANETs are used in military communications and operations and in automated battlefield.
- **Emergency Services:** MANETs are used in emergency services like search and rescue operation, disaster recovery, to help doctors and nurses in the hospitals, replacing fixed infrástructure in case of environmental disasters.
- **Personal Area Network:** The concept of personal area networks is about interconnecting different devices used by a single person, e.g. a PDA, cellular phone, laptop etc. In this case the PDA or the laptop will connect with the cellular phone in an ad hoc fashion. If both the PDA and the printer were ad hoc enabled the PDA could automatically get access to the printing services.
- **Sensor Networks:** Sensor networks [8] are Ad Hoc networks consisting of communication enabled sensor nodes. Each such node contains one or more sensors, example movement, and chemical or heat sensors.
- **Collaborative Networking:** This application of ad hoc networking may be the most intuitive. The simplest example is when a group of people is

attending a meeting and need to share information between their laptops or PDAs. Without ad hoc networking, a great deal of configuration and setup would be required to accomplish this task.

- **Commercial and Civilian Environment:** MANETs can be used in e-commerce for electronic payment anytime, anywhere. It can be used in sports stadium, trade fairs and shopping malls.
- **Education:** It can be used in virtual classrooms, ad hoc communication during lectures.

2.1.3 Advantages of MANETs

There are many advantages of MANETs some of them are listed below:

- **Low cost of Deployment:** There is no need of transmission media, no fixed infrastructure to establish and can be deployed on the fly. Therefore cost of deployment is low.
- **Fast Deployment**: Deployment of Mobile Ad Hoc Networks is fast because there is no set up time for infrastructure.
- **Dynamic Configuration**: It is very easy to change the configuration of mobile ad hoc networks as compared to wired network.

2.1.4 Limitations of MANETs

Some of the limitations that MANETs are [9] are as follows.

- **Bandwidth constraints**: As mentioned above, the capacity of the wireless links is always much lower than in the wired links. Several Gbps are available for wired LAN nowadays while the commercial applications for wireless LANs work typically around 2 Mbps.
- **Processing capability**: Most of the nodes of the MANETs are devices without a powerful CPU. The network tasks such as routing and data transmission cannot consume the power resources of the device, intended to play any other role, such as sensing functions.
- **Energy constraints:** The power of the batteries is limited, which does not allow infinitive operation time for the nodes. Therefore, energy should not be wasted and that is why some energy conserving algorithms have been implemented.

- **High latency:** In an energy conserving design, nodes are sleeping or idle when they do not have to transmit any data. When the data exchange between two nodes goes through nodes that are sleeping, the delay may be higher if the routing algorithm decides that these nodes have to wake up.
- **Transmission errors:** Attenuation and interferences are other effects of the wireless links that increase the error rate.
- **Security:** The authors divide the possible attacks in passive ones, when the attacker only attempts to discover valuable information by listening to the routing traffic; and active attacks, which occur when the attacker injects arbitrary packets into the network with some proposal like disabling the network.
- **Location:** The addressing is the another problem for the network layer in MANETs, since the information about the location the IP addressing used in fixed networks offers some facilities for routing that cannot be applied in MANETs.
- **Roaming:** The continuous changes in the network connectivity graph involve that the roaming algorithms of the fixed network are not applicable in MANETs, because they are based on the existence of guaranteed paths to some destinations.
- **Commercially unavailable:** MANETs is yet far from being deployed on large-scale commercial basis.

2.1.5 Why Security Enforcement is tougher in MANETs

Security enforcement is tough as compared to wired network due to the following characteristics [1].

- **Resource Constraint:** The wireless devices usually have limited bandwidth, memory and processing power. This means high resource consuming security solutions may not be affordable in wireless ad hoc networks.
- **Unreliable Communication:** The shared medium nature and unstable channel quality of wireless links may result in high packet loss rate and rerouting instability, which is a common phenomenon that leads to

throughput drops in multi-hop networks. This means that security solution in wireless ad hoc network cannot rely on reliable communication.

- **Dynamic topology:** The network topology of wireless ad hoc network may change rapidly and unpredictably over time due to node mobility. This requires solution to security to be adaptive to dynamic topology.
- **Scalability:** Due to limited memory and processing power on mobile ad hoc devices, the scalability is a key problem when we consider a large network size. Scalability is one of the major design concerns.

2.2 Routing Protocols of MANETs

Routing in ad-hoc networks involves finding a path from the source to destination, and delivering packets to the destination nodes while nodes in the network move freely. Due to node mobility, a path established by source may not exist after some time. To deal with node mobility nodes need to maintain routes in the network.

2.2.1 Desirable Properties of Routing Protocols

The conventional routing protocols do not meet the requirement of MANET due to its characteristic like self-organizing nature, node mobility. So, there is a need for new routing protocol. Some of the desirable properties [5] are:

- **Distributed Operation:** Due to decentralized operation of MANETs, it requires its operation to be performed in distributed manner. So it requires support from routing protocol.
- **Loop Freedom:** To improve the overall performance, the routing protocols need to guarantee that the routes supplied are loop free. This avoids any waste of bandwidth or CPU consumption.
- **Unidirectional Link Support:** Bidirectional links are assumed in design of routing protocol, but unidirectional link may occur in wireless network. Formation of two unidirectional link in opposite direction forms the bidirectional link which can be utilized to improve the performance.
- **Sleep Period Operation:** In order to conserve energy some nodes may stop sending and receiving packets. So, routing protocols must be adaptive to such situation without having adverse consequences.

- **Demand Based Operation:** Without assuming the uniform traffic distribution in the network (and maintaining routing between all nodes at all times), let the routing algorithm adapt to the traffic pattern on a demand or need basis. If this is done intelligently, it can utilize network energy and bandwidth resources more efficiently, at the cost of increased route discovery delay.
- **Security:** Without some form of network-level or link-layer security, a MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of the transmission media is harder in practice with MANETs. Sufficient security protection to prohibit disruption of modification of protocol operation is desired.

2.2.2 Challenges for Routing

Some of the challenges for routing are as follows.

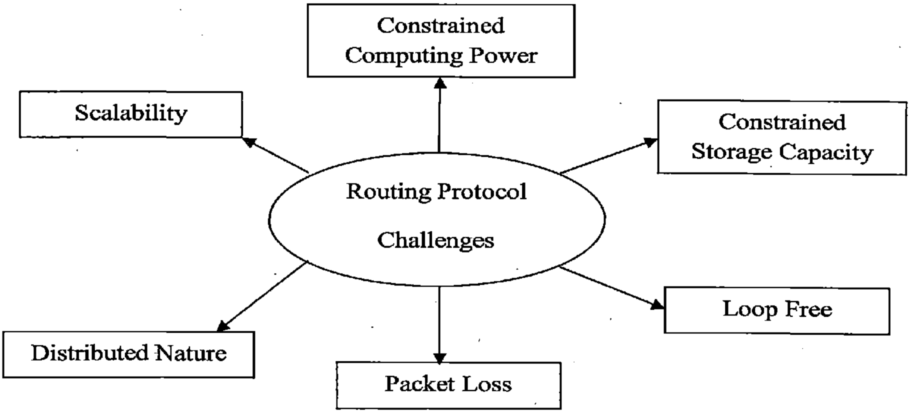

Constrained Computing Power
Scalability
Constrained Storage Capacity
Routing Protocol Challenges
Loop Free
Distributed Nature
Packet Loss

Figure 2.2 Challenges for Routing

- **Distributed Nature:** Due to distributed nature of mobile ad hoc networks routing is difficult to implement.

- **Loop Free:** Routing protocol must be designed in such a way that packets must not be entered in a loop. Otherwise it will decrease the performance.
- **Constrained Computing Power:** Mobile nodes have less computation power. So, routing protocol must be designed in such a way that nodes consumes less power.
- **Packet Loss:** Due to wireless nature of MANETs packet loss rate is high.
- **Constrained Storage Capacity:** Storage capacity of nodes in MANETs is also low. So, routing protocols should be designed so that they require less storage capacity.
- **Scalability:** Routing protocols must be designed so that they are applicable as we increase the number of nodes in the network.

Depending upon how nodes establish and maintains path, routing protocols are divided in to four categories: Proactive [10], Reactive [11], [12], Hybrid [13] and Location Based [14], [15], and [16].

2.2.3 Proactive Routing Protocols: These are also called table driven protocols. It maintains routing table using the routing information learnt from neighbors on periodic basis. Characteristics of proactive routing protocol are as follows.

- Distributed, shortest-path protocols.
- Maintain routes between every host pair at all times.
- Based on Periodic updates of routing table.
- High routing overhead and consumes more bandwidth.
- Example: Destination Sequence Distance Vector (DSDV)[10].

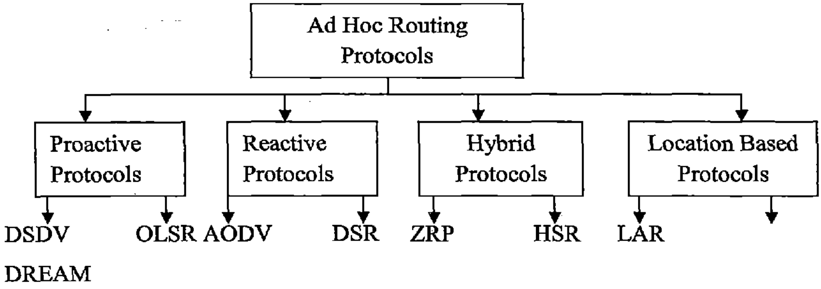


Figure 2.3 Classification of Routing Protocols

DSDV: Destination Sequence Distance Vector **AODV:** Ad Hoc on Demand Distance Vector

OLSR: Optimized Link State Routing **DSR:** Dynamic Source Routing

LAR: Location Aided Routing **ZRP:** Zone Routing Protocol

DREAM: Distance Routing Effect Algorithm for Mobility

HSR: Hierarchical State Routing

2.2.4 **Reactive Routing Protocols:** These are demand driven protocols that finds path as when required. They maintain information about the active routes only. They performs route discovery phase before data transmission by flooding route request packet and destination node reply with route reply packet. A separate route maintenance procedure is required in case of route failure. Characteristics of reactive routing protocol are as follows.

- Determine route if and when needed.
- Less routing overhead.
- Source initiates route discovery process.
- More route discovery delay.
- Example: Ad hoc On-Demand Distance Vector Routing (AODV)[12], Dynamic Source Routing (DSR)[11].

DSR (Dynamic Source Routing): DSR is on demand routing protocol. On demand means it discovers route only when it is needed to send data. It consists of two mechanisms (i) Route Discovery (ii) Route Maintenance

Route Discovery consists of two packets RREQ (Route Request) and RREP (Route Reply). When a source wants send data packet to destination, it will check its cache for route to that destination, if it contains the route to destination then it will use that route for data transmission otherwise it will initiate a route discovery mechanism. In this mechanism it will flood route request (RREQ) packet. Route request packet consists of source address, target address and sequence number. When an intermediate node receives route request it will check its two field source ID and sequence number to know whether it has already processed the route request. If a node already processed the route request then it will discard route request, otherwise node will append its own id to route request and rebroadcast it. This process continues until maximum hop count is reached (and RREQ is discarded) or it will reach at destination node. When a route request is received at destination node it will append its own id and send a route reply back to source along the path through which it received route request. When route reply is received at destination it will stores route in its cache. Some optimization can also be applied, if a node receives a route request it will check its cache for the route to destination specified in route request. If there is route to destination in its cache then it will send a route reply to source instead of broadcasting the route request. An intermediate node can also switch its network interface to promiscuous mode to receive the entire message passing in the network so that node can learn other routes also which are not passing through that node. As shown in figure 2.3 node 1 is source node and node 7 is destination node. Node 1 wants to send data packets to node 7. It will broadcast a route request which is reached to its neighbor nodes i.e node 2 and node 4 which process the route request i.e appends its own id in the route request and rebroadcast it again. In this way route request is reached to destination node 7 which then send back a route reply to node 1 through the same path from which it received route request as shown in figure 2.4

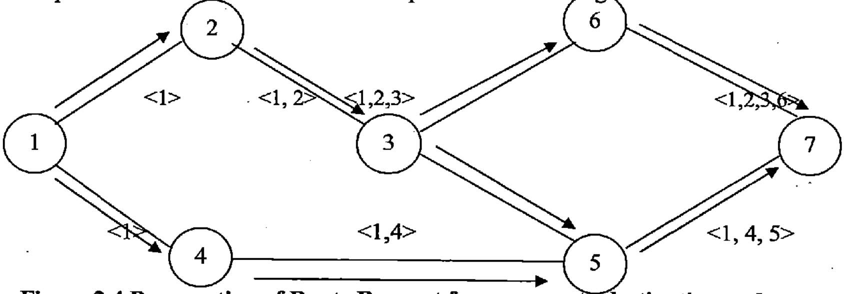


Figure 2.4 Propagation of Route Request from source to destination node.

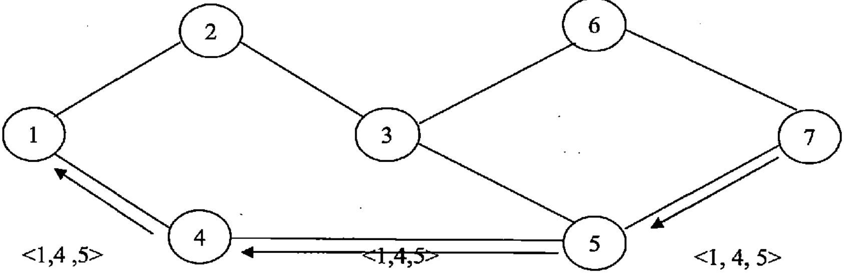


Figure 2.5 Propagation of Route Reply from destination to source node

In route maintenance mechanism any node if found its neighboring node, next hop on the route, is not working then it will send a route error packet which contains its address and address of its neighboring node. Upon receiving a route error packet node will remove the route from its cache which contains the address of node which is not working. Route maintenance can be achieved by passive acknowledgement.

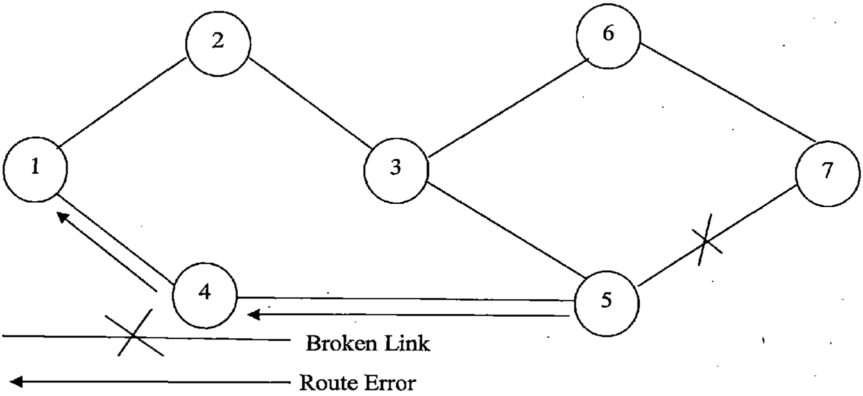


Figure 2.6 Route Maintenance in DSR

Advantages of DSR

- Routes are maintained only between node who need to communicate which reduces overhead of route maintenance.
- Route caching can further reduce route discovery overhead.
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local cache.

Disadvantages of DSR

- Packet header size grows with route length due to source routing.
- Flood of route requests may potentially reach all nodes in the network.
- Care must be taken to avoid collisions between route requests propagated by neighboring nodes– insertion of random delays before forwarding RREQ.

- Increased contention if too many route replies come back due to nodes replying using their local cache.
  - Route Reply *Storm* problem
  - Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route.

Multipath Routing Protocol: DSR routing protocol is modified in such a way that multiple paths are collected. Multipath Routing Protocol [22] on demand routing protocol which builds maximally disjoint path on route discovery. When source wants to send data packet and there is no route to destination it will flood the route request packet. Route request consists of source ID and sequence number that is used to check the duplicity of the packet. This route request is received by various nodes, firstly they will check whether they have processed this route request by comparing source ID and sequence number in the packet with the source ID and sequence number stored in their cache, if they have processed route request packet will be dropped in case of DSR routing protocol. Here modification is done in processing of route request. If the source ID and sequence number is same in the route cache and received route request then node will check hop count in the route cache and received route request, if hop count is less than or equal then it will forward the route request. During forwarding of route request it also appends its own ID in route request. Ultimately destination will receive route request from multiple paths and sends back route reply through all the paths. Now multiple paths are stored in cache of source node and it will transmit data on one of path which it received first from destination node. We also modified DSR by which intermediate node will not send route reply from its route cache only destination node will send route reply. As shown in figure 2.7 node f broadcast a route request for node j, intermediate node receives route request from path f-a-b-c, its hop count is three. After some time it receives route request from the path f-g-h-c its hop count is also three so node c will also broadcast this route request because hop count in this route request is same as of previous route request, but in case of DSR this does not happen. So multiple route requests arrive at destination node and then destination node replies to route request. So multiple routes are collected.

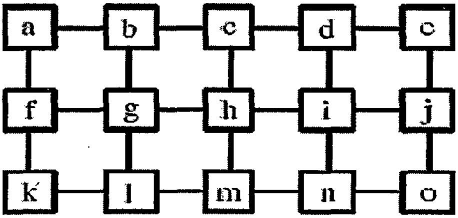


Figure 2.7 Multipath Routing Example

2.2.5 Hybrid Routing Protocols: In this various approaches of routing protocols are combined to form a single protocol. ZRP (Zone Routing Protocol) is one such protocol that combines the proactive and reactive approach. Characteristics of hybrid routing protocol are as follows.

- Combination of selected features of proactive and reactive protocols.
- Example: Zone Routing Protocol (ZRP).
- Adaptive to network condition.

2.2.6 Location Based Routing Protocols: These protocols utilize the position of nodes in the network and use less information about topology of the network. These protocols maintain only one or two hop topology information with the help of hello protocol. Nodes use greedy-forwarding to select next hop towards the destination to send data to the destination node. In greedy-forwarding node selects the next hop towards the destination which is geographically closest to the destination among its neighboring nodes.

There are two parts to position-based routing (a) given position of source node, destination node, and local neighbor table of each node, delivering packets from source to destination node, and (b) given that each node can determine its own position, using some positioning system GPS, obtaining the position of any other node in the system. The former part is called position based routing examples are GFG, GPRS. The later part is called the location service. Examples are GLS, DLM. Advantage of these protocols is that nodes need not establish, maintain routes, and these protocols are more scalable compared to reactive and proactive routing protocols.

2.3 Attacks on Routing Protocols

Attacks on routing protocols can be both active and passive as shown in figure 2.8. In passive attacks an attacker does not actively participate in bringing the network down. Attackers are typically involved in unauthorized listening to routing packets. An attacker just eavesdrops on the network traffic as to determine which nodes are trying to establish routes to which other nodes, which nodes are the center of the network and so on. A major benefit for the attacker is that passive attacks are usually impossible to detect and hence makes defending against such attacks extremely difficult. Further, routing information can reveal relationships between nodes or disclose their addresses. If a route to a particular node is requested more often than to other nodes, the attacker might expect that the node is important for the functioning of the network, and disabling it could bring the entire network down. Such attacks can be prevented mostly by applying cryptographic techniques on messages, to protect the message contents from being exposed to the attacker.

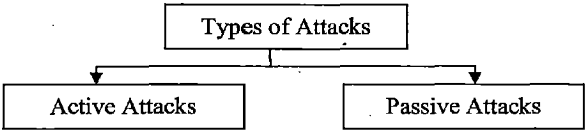


Figure 2.8 Types of Attack

Active attacks involve modification, fabrication of messages, or preventing the network from functioning properly. Further, active attacks can be due to an external attacker(s) and an internal attacker(s). External attackers are unauthorized nodes without a shared cryptography key in the network. Internal attackers are authorized but compromised nodes and are more dangerous and hard to detect as they are in the network and own the necessary cryptography keys. Active attacks can be classified into packet-dropping, modification, fabrication, and other miscellaneous attacks.

2.3.1 Packet Dropping

Malicious nodes may ensure that certain messages are not transmitted by simply forwarding few packets and dropping the remaining one. By dropping packets, an attacker succeeds in disrupting the network operation. Such misbehavior can be hard to detect as valid nodes may, from time to time, drop packets due to congestion/collision. Depending on the strategy of dropping packets, there are two types of attacks:

i) Black hole Attack

The Black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to destination node, even though the route is spurious, with the intention of intercepting packets. Second the attacker consumes the intercepted packets without any forwarding.

ii) Grey Hole Attack

The attacker drops data packets but not control packets. This attack is difficult to detect. A promiscuous mode operation within the routing protocol is required to detect such an attack.

2.3.2 Modification

Most routing protocols assume that nodes do not alter fields of the protocol messages. The protocol messages, or control packets, carry important routing information that governs the behavior of their transmission. Since the level of trust in a traditional ad-hoc network cannot be measured or enforced, malicious nodes may participate directly in route discovery and may intercept and disrupt communication. They can easily cause redirection of network traffic and denial of service attacks by simply altering fields in protocol messages. These attacks can be classified as follows:

i) Remote redirection with modified route sequence number: A malicious node uses the routing protocol to advertise itself as having the shortest path to destination whose packets it wants to intercept. Typically, routing protocols maintain routes using monotonically increasing sequence numbers for each destination. A malicious node may divert traffic through itself by advertising a route to a node with a destination sequence number greater than the authentic value.

ii) Redirection with modified hop count: In some protocols such as AODV, the route length is represented in the message by a hop count field. A malicious node can succeed in diverting all the traffic to a particular destination through itself by advertising a shortest route (with a very low hop count) to that destination.

iii) Denial of Service with modified source routes: DSR routing protocol explicitly states routes in data packets called the source route. In the absence of any integrity checks on the source route, a malicious node can modify this source route and hence succeed in creating loops in the network or launching a simple denial of service attack.

2.3.3 Fabrication

Fabrication of messages means generating false routing messages. Such attacks are difficult to detect. There are three types of such attacks.

i) **Falsifying route error messages:** AODV and DSR have measures to handle broken routes when constituent nodes move or fail. If the destination node or an intermediate node along an active path moves or fails, the node, which precedes the broken link, broadcasts a route error message to all active neighbors which precede the broken link. The nodes then invalidate the route for this destination in their routing tables. A malicious node can succeed in launching a denial of service attack against a benign node by sending false route error messages against this benign node.

ii) **Route cache poisoning:** In DSR, a node can learn routing information by overhearing transmissions on routes of which it is not a part. The node then adds this information to its own cache. An attacker can easily exploit this method of learning and poison route caches. If a malicious node, *m*, wants to launch a denial of service attack on node *X*, it can simply broadcast spoofed packets with source routes to *X* via itself. Any neighboring nodes that overhear the packet transmission may add the route to their route cache.

iii) **Routing table overflow attack:** A malicious node may attempt to overwhelm the protocol by initiating route discovery to non-existent nodes. The logic behind this is to create so many routes that no further routes could be created as the routing tables of nodes are already over flowing.

2.3.4 Other Attacks

i) **Impersonation:** A malicious node masquerades as another node. It does this by misrepresenting its identity by changing its own IP or MAC address to that of some other node; thereby masquerading as that node. Using stronger authentication procedures this attack can be prevented.

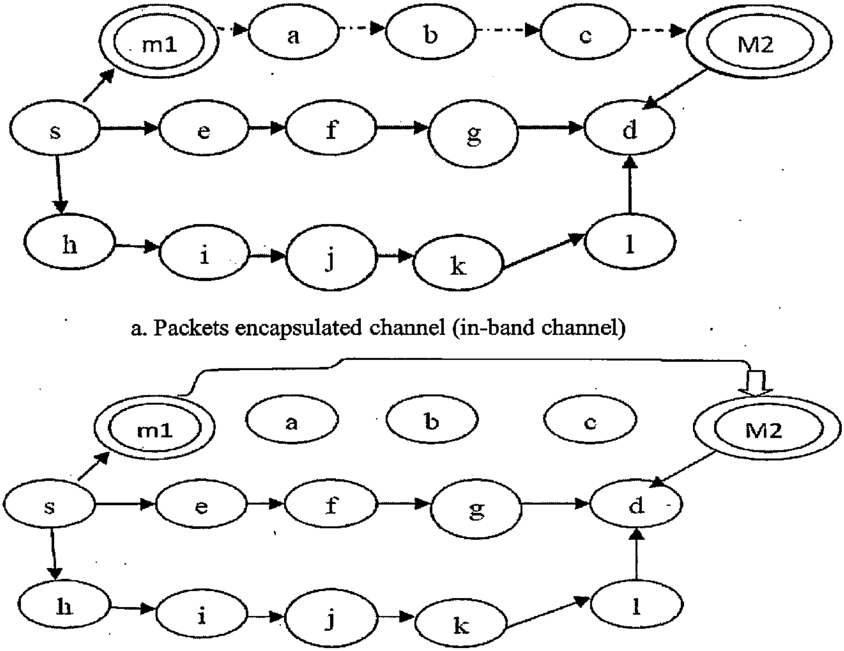
ii) **Sybil attack:** In the Sybil attack, an adversary presents multiple identities to other nodes in the network. This attack disrupts routing protocols by causing nodes to appear to be "in more than one place at once". This reduces the diversity of routes available in the network. It also diminishes the effectiveness of fault-tolerant schemes such as multi-path routing, and topology maintenance.

iii) **Wormhole Attack:** It is performed by the two or more malicious nodes in conspiracy. Two nodes at different location send receive routing message to each other via a secret channel. In this even if the two nodes are far apart, they appear within a single hop distance. Therefore route passing through these nodes are likely to be shorter than regular one. These nodes easily grab the route from the source node to destination node, and then sniff, drop, or selective drop data packets passed by.

In wormhole attack, malicious node *m1* first captures a routing message from neighboring node, and then sends the message to another malicious node, *m2* by means of secret channel, *m2* then broadcast or propagates the message received. In this way tunnel like channel is formed between these nodes. The tunnel like channel can be realized by two methods:

i) **Packet Encapsulated Channel:** It is also called in-band channel. In this a path is built in advance between the two malicious nodes, *m1* and *m2,* when source node s, broadcast a routing message i.e. route request (RREQ) it would be received by the malicious node *m1* and then *m1* encapsulates the RREQ in to the payload of the data packet and transmit it using prebuilt path between *m1* and *m2*. *m2* after receiving encapsulated packet, it will extract the RREQ message and broadcast it until it reaches the destination node. As path is shorter than other paths therefore destination node will reply through this route to source node. As shown in figure 2.9 (a)

ii) **Out-of-Band Channel:** A special channel may be a connection via a wired network between two malicious nodes, or a private channel between the two ends using a high powered transmission to send signals over a long distance. As shown in figure 2.9 (b)



a. Packets encapsulated channel (in-band channel)

b. Out-of-band channel

Figure 2.9 Two possible implementation methods of wormhole attacks

2.4 Literature Review

2.4.1 Packet Leashes

A leash [17] is any information added to the packet designed to restrict the packets maximum allowable distance. Two leashes are defined geographic leashes and temporal leashes. In geographic leashes each node must know its own location and loosely synchronized clocks. When sending a packet, the sending node includes its own location and the time at which packet was sent the receiver will check the time at which it received the packet and location and calculates the upper bound on the limit between sender and itself. A regular signature or other authentication technique can be used to allow a receiver to authenticate location and time in the received packet. 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. In temporal leashes all nodes must have tightly synchronized clocks. To use temporal leashes, when sending a packet, the sending node includes in the packet the time at which it sent the packet, *ts*; when receiving a packet, the receiving node compares this value to the time at which it received the packet, *tr*. The receiver is thus able to detect if the packet traveled too far, based on the claimed transmission time and the speed of light. Temporal leashes can also be constructed by including the expiration time in the packet, after which receiver would not accept the packet. A regular digital signature or authentication mechanism can be used to allow a receiver to authenticate a timestamp or expiration time.

2.4.2 WAP: Wormhole Attack prevention algorithm in MANETs

WAP [18] based on DSR (Dynamic source routing). In this all nodes monitors its neighbor node behavior when they send RREQ (route request) packet to the destination using a special list called neighbor list. When a source receives some route reply messages it can detect a route under wormhole attack among the routes. Once the wormhole node is detected source node records them in wormhole node list. In this radio links are assumed to be bi directional and transmission range of wormhole node is same as normal node. Neighbor node monitoring is used to detect the neighbors that are not within the transmission range of the node but pretends to be neighbors. This is done through route discovery process. An intermediate node cannot reply from its cache if it has route to the destination. Node A sends a RREQ packet and starts a WPT (Wormhole Prevention Timer) when node B receives the RREQ then it broadcast to neighbors because it is not destination. Node A can check whether the RREQ arrives with in the timer, if node A receives the message after timer expires, it suspects B or one of its next nodes to be wormhole nodes. Each node also neighbor node table which contains RREQ sequence number, neighbor node ID, sending time, receiving time and count.

2.4.3 WARP: Wormhole Avoidance Routing Protocol using anomaly detection mechanism

WARP [19] is an extension of AODV for security enhancement. It assumed link disjoint multipath into consideration in route discovery phase however, it chooses only one path to transmit data packets. . In the path discovery phase of WARP an intermediate node will attempt to create a route that does not pass through a hot neighbor, which has a higher rate of route formation than a threshold. It may be that a node is placed at a key position of connectivity in the network but due to mobility it will not stay there for long time. In this protocol if one isolated node behaves normally, it may be recovered from isolation. In this protocol message format of RREQ has been modified and contains an additional field called first_hop which records the first node receiving the RREQ after leaving the source, a new message called RREP_DEC is also introduced whose format is same as RREP. As WARP is multipath, the originator, after receipt of RREP, must send out an RREP_DEC along the route to note the nodes reside on the routing path. In WARP each intermediate node would create only one forward entry toward destination.

Routing Table Format: In WARP routing table has three additional fields (i) "first_hop" to meet the needs of the RREQ (ii) "RREP count" to accumulate the count of receiving RREPs, and the "RREP_DEC count" for the count of receiving RREP_DECs. The latter two are node parameters to calculate its neighboring node's anomaly value.

Anomaly value = (number of RREP_DEC)/ (number of RREP+1) ... *eqn(2.1)*

It represents the probability of malicious node among nodes on the link disjoint multipath, which send RREPs back to the originator to be finally chosen by the originator for transmitting the packets. A higher anomaly value means possibility of the node being a wormhole node.

2.4.4 DelPHI: Wormhole Detection mechanism for Ad Hoc Wireless Network

In DelPHI [20] hop count and delay information of disjoint paths are collected at the sender and delay/hop information is used as a measure for detection of wormhole attack which provides solution to both types of attacks. Delay under wormhole attack is high as compared to normal route delay. Therefore if, a path has a distinguishable high delay/hop, it is likely to be subjected to wormhole attacks. It consists of two phase's data collection phase and data analyses phase. In this receiver replies to each RREQ received. It consists of two messages

DRREQ (DelPHI route request) and DRREP (DelPHI route reply) and includes previous hop field, hop count field and, a timestamp field. Sender broadcast DRREQ and after receiving the DRREQ receiver replies it with the DRREP packet. Sender can receive multiple DRREP packets. Each DRREP contains the hop count information of the path that is associated with it. Round trip time of the path is calculated differencing the time timestamp carried in DRREP and time at which DRREP is received. Then sender is able to calculate the delay/hop value of corresponding path. DPH value is calculated and arranged in descending order and finds whether there is large gap between the two than a threshold value then that path is under wormhole attack.

2.4.5 MHA: A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANETs

In MHA [21] route with wormhole attack has a minimum hop count than normal route. So avoiding route with minimum hop count can avoid wormhole attack. This protocol is based on AODV (ad hoc on demand distance vector routing) protocol. RREQ (route request) packet is modified and contains the CF (Check Flag) field which is used to distinguish the new RREQ (route request) from the old ones. It contains the four parts route establishment, RREP number limit and graylist broadcast, hop count analysis scheme and route selection and route maintenance in MHA routing protocol. It does not require special assumptions and special hardware and overhead is also low but the dynamic field of the packet may change and we cannot use it in battlefield environment.

2.4.6 Detection of wormhole attacks in multipath routed wireless ad hoc networks: A statistical analysis approach

SAM (Statistical analysis of multipath) [22] approach is used to detect the wormhole attack and identify the malicious nodes with different topologies and different transmission range. Certain statistics of discovered route under wormhole attack will be changed dramatically. It assumes that each node can communicate to its neighbor only, and network is bidirectional. It analyses two statistics one is maximum relative frequency that link i appears in set of obtained routes and the difference between the most frequently appeared link and the second most frequently appeared link in set of routes in one route discovery. It is expected that both these parameters will be much higher under wormhole attack than that in normal system and malicious nodes can be located by the attack link which has the highest relative frequency. As compared to other techniques this is not performed as often.

2.4.7 SEEEP: Simple and Efficient End to End protocol to secure Ad Hoc Networks against Wormhole Attacks

SEEEP [23] requires each node to equip with GPS and secret keys which provide secrecy and authenticity of messages between source and destination. It bounds the minimum number of hops on the good route. Any path showing lesser hop count is shown to be under attack. If d is the length between source and destination in terms of the distance travelled by a packet and r is the communication range between two nodes then packet must travel at least d/r hops. If the length k of path in terms of number of hop count is less than d/r then there is a wormhole on the path. Distance d is calculated when the source sends wormhole detection packet and each node attaches its location. This idea works well when the node does not lie about its position.

2.4.8 Wormhole attack detection based on distance verification and the use of hypothesis testing for wireless ad hoc networks

In this approach [24] each node is required to know about its own location through some extra hardware such as GPS. When a node broadcasts the packet it appends its own location to the packet. When a node receives a packet it can compute the distance to the sender node based on the information and RSS measurement for the distance estimation and verification is formulated as a hypothesis testing problem in which a null and alternative hypothesis are used to test whether the measured and computed distance are consistent. If the measured distance is consistent with the computed distance the packet is from the owner node if the distance is inconsistent then the packet may be from wormhole node. The decision of uncertainty means that there is not sufficient information available to arrive at a firm decision and further evidences are needed.

2.4.9 WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks

Wormeros [25] uses two phases to detect wormhole. The first phase is called Suspicion, in this phase it measures the RTT between a node S and all of its neighbors. If RTT(S, D) where D is one of its neighbors, is abnormally higher than average RTT of all links from S to its neighbors, then there might be wormhole link. Secondly, observation is made that in a dense network, two neighbors are likely to have some common neighbors. Based on these techniques in this phase it detects the suspicious link. Second Phase is called confirmation phase; Wormeros launches a series of challenges to make sure that wormhole is correctly identified.

2.5 Research Gaps

Some of research gaps found from literature review are as follows.

- Some approach requires Special hardware like GPS to know its position.
- Some approach make impractical assumptions like no mobility in the network
- Some approaches assumes that links are bidirectional which is not always possible
- Some approach requires clock synchronization
- Some approach cannot detect wormhole for certain amount of time and it says that nodes which has higher route building is wormhole which may not be because a node may be placed in such a position where route building rate is higher.

Chapter 3

Proposed Approach for Detection and Prevention of Wormhole Attack

Multipath Routing protocol is taken into consideration which is based on DSR (Dynamic Source Routing) protocol and constructs multiple paths.

3.1 Assumptions:

- Wormhole nodes will not modify and sniff the data packets; they will only drop data packets.
- Data transmission takes place only on one path.

3.2 Preliminaries

Two new packets i.e Dummy_Request and Dummy_Reply are introduced. Packet format for these new packets are same as route reply packet format of DSR routing protocol except option type field. Option type is 10 for Dummy_Request and 11 for Dummy_Reply.

3.2.1 Dummy_Request Packet Format: A new packet is introduced in this approach whose packet format is same as route reply of DSR [11] routing protocol, but option type and functionality is different. Option type is 10 for dummy_request and 3 for route reply. Reserved bits in route reply packet is used in dummy_request packet to check the vulnerability of path against wormhole attack.

<table>
<tr><td></td><td>Option Type</td><td>Opt Data Length</td><td>L</td><td>Num of packets before next Dummy Request</td></tr>
<tr><td colspan="5">Address [1]</td></tr>
<tr><td colspan="5">Address [2]</td></tr>
<tr><td colspan="5">.......</td></tr>
<tr><td colspan="5">Address [n]</td></tr>
</table>

Figure 3.1 Dummy_Request Packet Format

Option Type: This is unique number that is used to distinguish different types of packets. 10 is given to Dummy_Request

Opt Data Length: It is 8 bit unsigned number representing the length of the option in octects.

Last Hop External (L): Set to indicate that last hop given by the route reply is a path external to DSR network, the route outside the DSR network is not represented in route reply.

Num of packets before next Dummy_Request: This field contains information about the number of data packets to be sent before next Dummy_Request packet. This information is maintained at source node also.

Address [1....n]: This is ordered list of addresses of nodes which occurred during the route request packet from source to destination. This field contains the path which we have to check for wormhole attack. Dummy_Reply will traverse through in a reverse path contained in Dummy_Request packet.

3.2.2 Dummy_Reply Packet Format:

Its packet format is same as packet format of route reply of DSR routing protocol [11]. Only the option type and functionality is different. Option type for Dummy_Reply is 11 and reserve bits are used to check the vulnerability of path against wormhole attack. This packet is initiated by destination node only when it receives Dummy_Request packet from source node.

	Option Type	Opt Data Length	L	Num of data packets received till last dummy_request
Address [1]				
Address [2]				
....				
Address [n]				

Figure 3.2 Dummy_Reply Packet Format

Option Type: This is unique number that is used to distinguish different types of packets. 11 is given to Dummy_Reply

Opt Data Length: It is 8 bit unsigned number represent the length of the option in octects.

Last Hop External (L): Set to indicate that last hop given by the route reply is a path external to DSR network, the route outside the DSR network is not represented in route reply.

Num of data packets received till last dummy_request: This field contains the information that how many data packets has been received till last Dummy_Request.

Address [1....n]: This is ordered list of addresses of nodes which occurred during the dummy_request packet from source to destination.

3.3 Proposed Algorithm for Detection and Prevention of Wormhole Attack

Step1: When a Source node wants to send data packets to destination, it will check its route cache for the path to destination node, if valid route is available then it will use valid route to send data packet. Otherwise, source node will broadcast a route request packet to find the routes to the destination; destination receives multiple route requests from the source and replies to each route request with route reply. Sender will receive multiple route reply from the destination and store multiple paths to the destination in its route cache.

Step2: After route set up, sender wants to send data packets to the destination before that it sends a Dummy_Request packet to check the vulnerability of the path. Now, sender will choose one of the paths whose hop count is minimum. It will set number of packets before next Dummy_Request field in Dummy_Request packet, which will represent how many data packets will be sent before sending next Dummy_Request packet. Sender will set a timer and wait for Dummy_Reply packet.

Step 3: Destination node will receive the Dummy_Request packet and form a Dummy_Reply packet and set the Num of data packets received till last dummy_request field. Destination node will reverse the path received in Dummy_Request and send Dummy_Reply packet on this path to source node.

Step 4: If source node receives the Dummy_Reply packet before timeout of Dummy_Request packet than it will compare the Num of data packets received till last dummy_request field received in Dummy_Reply with set number of packets before next Dummy_Request field sent in previous Dummy_Request. If it matches, path is not under wormhole attack and it starts sending data packets. In the meanwhile if sender has to send data packets then it will start buffering data packets until it receives wormhole free path from source to destination. If sender does not receive Dummy_Reply packet then it will delete the path from its route cache and selects another path for checking the vulnerability of path.

Step 5: Source node will send fixed number of data packets to destination node which is contained in Dummy_Request packet and then whole process is repeated to check vulnerability of currently using path against wormhole attack.

This approach only checks that whether the wormhole nodes are dropping the data packets or not. It may be that the wormhole nodes only drop the Dummy_Request packet. This approach cannot identify the wormhole link on the route.

3.4 Flowchart:

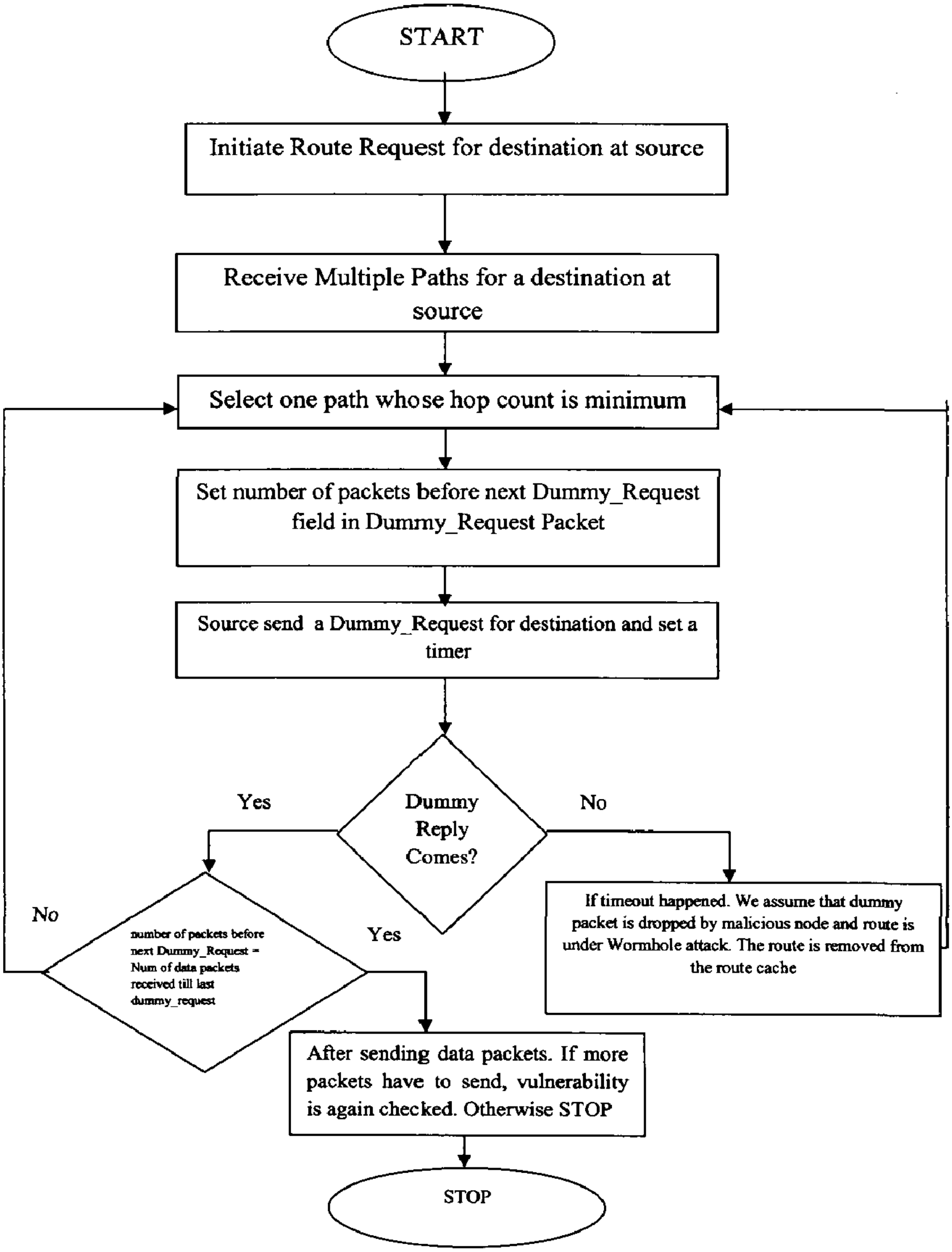

START
Initiate Route Request for destination at source
Receive Multiple Paths for a destination at source
Select one path whose hop count is minimum
Set number of packets before next Dummy_Request field in Dummy_Request Packet
Source send a Dummy_Request for destination and set a timer
Dummy Reply Comes?
Yes
No
If timeout happened. We assume that dummy packet is dropped by malicious node and route is under Wormhole attack. The route is removed from the route cache
No
number of packets before next Dummy_Request = Num of data packets received till last dummy_request
Yes
After sending data packets. If more packets have to send, vulnerability is again checked. Otherwise STOP
STOP

Figure 3.3 Flow Chart of Proposed Algorithm

Chapter 4

Simulation Tool, Parameters and Performance Metrics

4.1 QualNet 5.0.2 Simulator: An Overview

QualNet [26] is a comprehensive suite of tools for modeling large wired and wireless networks. It uses simulation and emulation to predict the behavior and performance of networks to improve their design, operation and management. QualNet enables users to:

- Design new protocol models.
- Optimize new and existing models.
- Design large wired and wireless networks using pre-configured or user-designed models.
- Analyze the performance of networks and perform what-if analysis to optimize them.

Key Features of QualNet that enables creating a virtual network environment:

- **Speed:** QualNet can support real-time speed to enable software-in-the-loop, network emulation, and hardware-in-the-loop modeling. Faster speed enables model developers and network designers to run multiple "what-if" analyses by varying model, network, and traffic parameters in a short time.
- **Scalability:** Qualnet Developer supports thousands of nodes by taking advantage of the latest software, hardware and parallel computing techniques. The base Qualnet Developer product can run two threads simultaneously to benefit from the latest dual-core processors from Intel® and AMD®. Advanced versions of Qualnet Developer can run on cluster, multi-core, and multi-processor systems to model large networks with high fidelity.
- **Model Fidelity:** Qualnet Developer uses highly detailed standards-based implementation of protocol models. It also includes advanced models for the wireless environment to enable more accurate modeling of real-world networks.
- **Portability**: Qualnet Developer and its library of models run on a vast array of platforms, including Linux, Solaris, Windows XP, and Mac OS X

operating systems, distributed and cluster parallel architectures, and both 32- and 64-bit computing platforms. Users can develop a protocol model or design a network in Qualnet Developer on their desktop or laptop computer and then transfer and run it on a powerful multi- processor Linux server to perform capacity, performance, and scalability analyses.

- **Extensibility:** Qualnet Developer can connect to other hardware and software applications, such as OTB, real networks, and third party visualization software like STK, greatly enhancing the value of the network model.

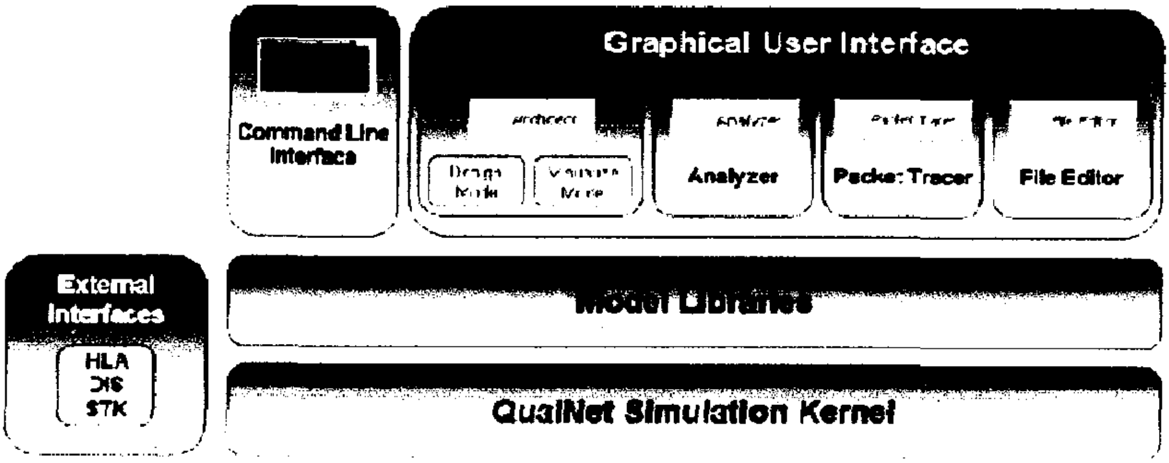


Figure 4.1 QualNet Architecture

4.2 QualNet Components

The various components of QualNet are given below:

i) **QualNet Kernal:** -It is a parallel discrete event scheduler that provides the scalability and portability to run hundred and thousand of nodes with with high-fidelity models on a variety of platforms, from laptops and desktops to high performance computing systems.

ii) **QualNet Model Libraries:** - QualNet includes support for a number of model libraries that enable you to design networks using protocol models developed by Scalable Network Technologies. Purchase of QualNet includes the Developer, Wireless, and Multimedia and Enterprise Model Libraries; additional libraries for modeling WiMAX, network security, sensor networks, satellite, and cellular models are also available.

iii) **QualNet Graphical User Interface:** - QualNet GUI consists of Architect, Analyzer, Packet Tracer, and File Editor.

a. Architect is a network design and visualization tool. It has two modes: Design mode and Visualize mode. In Design mode you can set up terrain, network connections, subnets, mobility patterns of wireless users, and other functional parameters of network nodes. You can create network models by using intuitive, click and drag operations. You can also customize the protocol stack of any of the nodes. You can also specify the application layer traffic and services that run on the network. In Visualize mode, you can perform in-depth visualization and analysis of a network scenario designed in Design mode. As simulations are running, users can watch packets at various layers flow through the network and view dynamic graphs of critical performance metrics. Real-time statistics are also an option, where you can view dynamic graphs while a network scenario simulation is running.

b. Analyzer is a statistical graphing tool that displays the metrics collected during the simulation of a network scenario in a graphical format. You can customize the graph display.

c. Packet Tracer provides a visual representation of packet trace files generated during the simulation of a network scenario. Trace files are text files in XML format that contain information about packets as they move up and down the protocol stack.

d. File Editor is a text editing tool that displays the contents of the selected file in text format and allows the user to edit files.

iv) **QualNet Command Line Interface:** - The QualNet command line interface enables a user to run QualNet from a DOS prompt (in Windows) or from a command window (in Linux or Mac OS X). When QualNet is run from the command line, input to QualNet is in the form of text files which can be created and modified using any text editor. Building and running scenarios with the command line interface takes less memory and scenarios typically run faster than with the GUI. With the command line interface the users have the flexibility to interface with visualization and analysis tools of their choice.

v) **QualNet External Interfaces: -** QualNet can also interact with a number of external tools in real-time. The HLA/DIS module, which is a part of the Standard Interfaces Model Library, allows QualNet to interact with other HLA/DIS compliant simulators and computer-generated force (CGF) tools like OTB. The QualNet STK interface, which is a he information from one part of the Developer Model Library, provides a way to interface QualNet with the Satellite Toolkit (STK) developed by Analytical Graphics, Inc. (AGI) and function in a client-server environment.

4.3 Simulation Parameters

The QualNet 5.0.2 simulator is used to simulate and validate the proposed heuristics. Four scenarios are created to evaluate the performance of DSR (Dynamic Source Routing) and Multipath routing protocol. Four scenarios taken are described by the tables given below:

Scenario I:

Table 4.1 Simulation Parameters Taken for DSR Routing Protocol for varying node mobility

Parameter	Value Taken
Number of Nodes	50
Maximum Speed	10, 20, 30, 40 mps
Minimum Speed	0 mps
Simulation Time	300 seconds
Traffic Type	Constant Bit Rate
Terrain	1000X1000 m
Mobility Model	Random Waypoint
Pause Time	10 seconds
Packet Size	512
Packet Rate	4 Packets/second
Routing Protocol	DSR

Wormhole Link	Node 18 and Node 19

Scenario II:

Table 4.2 Simulation Parameters Taken for DSR (Dynamic Source Routing) protocol for varying number of wormhole links

Parameter	Value Taken
Number of Nodes	50
Maximum Speed	10 mps
Minimum Speed	0 mps
Simulation Time	300 seconds
Traffic Type	Constant Bit Rate
Terrain	1000X1000 m
Mobility Model	Random Waypoint
Number of Wormhole Links	1, 2, 3, 4
Packet Size	512
Packet Rate	4 Packets/second
Routing Protocol	DSR
Wormhole Link	14-29, 21-38, 37-50, 28-42

Scenario III

Table 4.3 Simulation Parameters Taken for Multipath Routing Protocol for varying number of wormhole links

Parameter	Value Taken
Number of Nodes	30
Maximum Speed	10 mps

Minimum Speed	0 mps
Simulation Time	300 seconds
Traffic Type	Constant Bit Rate
Terrain	1000X1000 m
Mobility Model	Random Waypoint
Number of Wormhole Links	1
Packet Size	512
Packet Rate	4 Packets/second
Routing Protocol	Multipath Routing Protocol
Wormhole Link	18-19
Pause Time	30, 60, 120, 240, 300

Scenario IV

Table 4.4 Simulation Parameters Taken for comparison of MRWDPDP with Multipath Routing Protocol by varying number of wormhole links

Parameter	**Value Taken**
Number of Nodes	30
Maximum Speed	10 mps
Minimum Speed	0 mps
Simulation Time	100 seconds
Traffic Type	Constant Bit Rate
Terrain	1000X1000 m
Mobility Model	Random Waypoint
Pause Time	30 seconds

Packet Size	512
Packet Rate	4 Packets/second
Routing Protocol	Multipath Routing Protocol, MPR with proposed approach
No. Of Wormhole Links	1, 2, 3, 4
Wormhole Link	4-19, 16-21, 23-30, 9-20

4.1 Performance Metrics

There exists various performance metrics for evaluating routing protocols.

4.4.1 Packet Delivery Ratio (PDR): Packet Delivery is calculated by dividing the total data packets received at destination node to the total data packets sent by source node.

4.4.2 Throughput: Throughput is the successful transmission rate of the network and defined as number of data packets successfully transmitted to destination per time unit.

Throughput = No. of bytes received*8*100/ (Time when last bytes received- Time when first byte received)

Chapter 5

Results and Discussions

The scenarios given in section 4.3 of chapter 4 are used to measure the network performance.

5.1 Results of DSR with and without Wormhole Attack with variable node mobility

In this performance of DSR (Dynamic Source Routing) under wormhole attack is measured and compared with DSR protocol without wormhole attack. Scenario I of section 4.3 of chapter 4 is taken. Network size is 50 nodes and mobility is varied from 10 mps to 40 mps. Traffic model taken is CBR (Constant Bit Rate) which is in between node 1 and node 46. In this wormhole attack with threshold value 75 is taken. Wormhole node with threshold means that packet size greater than or equal to threshold value will be dropped by the wormhole nodes. Threshold can be any value which you want to set. We have taken two wormhole nodes i.e one wormhole link. Wormhole link between node 18 and node 19 is created in the network. Node 18 is near the source node and node 19 is near the destination node.

a) **Packet Delivery Ratio:** It is calculated by dividing the number of packets received by the destination node through the number of packets originated by the source node. It specifies the packet loss rate, which limits the maximum throughput of the network. Better the delivery ratio, the more complete and correct is the routing protocol. Packet delivery ratio is less when the routing protocol is under wormhole attack as compared to protocol without wormhole attack shown in figure 5.1. Packet delivery ratio of DSR without wormhole attack varies around 0.9 but in presence of wormhole attack it varies around 0.6. So, presence of wormhole nodes decreases the packet delivery ratio because packets passing through wormhole nodes are dropped.

b) **Throughput:** It is the average rate of successful message delivery over a communication channel. It is measured in bits per seconds or bps. As shown in figure 5.2 throughput of DSR routing protocol without wormhole attack is around 4000 bps to 3600bps while in the presence of wormhole attack throughput varies around 2500 bps. Throughput of DSR decreases as we increase the mobility because it is difficult to find the route from source to destination. Although the throughput of DSR is higher without wormhole attack than the throughput with wormhole attack. This is because wormhole nodes drop the packets and available bandwidth is not being utilized for transmission of data packets. So presence of wormhole nodes decreases the throughput of the DSR routing protocol.

5.2 Results of DSR with and without Wormhole Attack with variable Wormhole Links

Scenario II given in section 4.3 of chapter 4 is taken for evaluating the performance on the basis of packet delivery ratio and throughput of DSR routing protocol by varying the number of wormhole links (one wormhole links contains two nodes). In this scenario network size is 50 nodes, simulation time is 300 seconds and wormhole links are varied from 1 to 4. Wormhole links are created between nodes 14-29, 21-38, 37-50, and 28-42. One wormhole node is placed near source node and another wormhole node is placed near destination, rest three wormhole links are placed randomly in the network. Threshold value of all wormhole links is set to 75.

a) **Packet Delivery Ratio:** It is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source. Figure 5.3 shows that if there is only one wormhole link in the network then packet delivery ratio is about 63%. If there is increase in number of wormhole links then packet delivery ratio is decreased.

b) **Throughput:** It is the average rate of successful message delivery over a communication channel. It is measured in bits per seconds or bps. Figure 5.4 shows that if we increase the number of wormhole links then the throughput is decreased. As shown in figure 5.4 when there is only one wormhole link throughput is around 2400 bps as we increase the wormhole links throughput decreases.

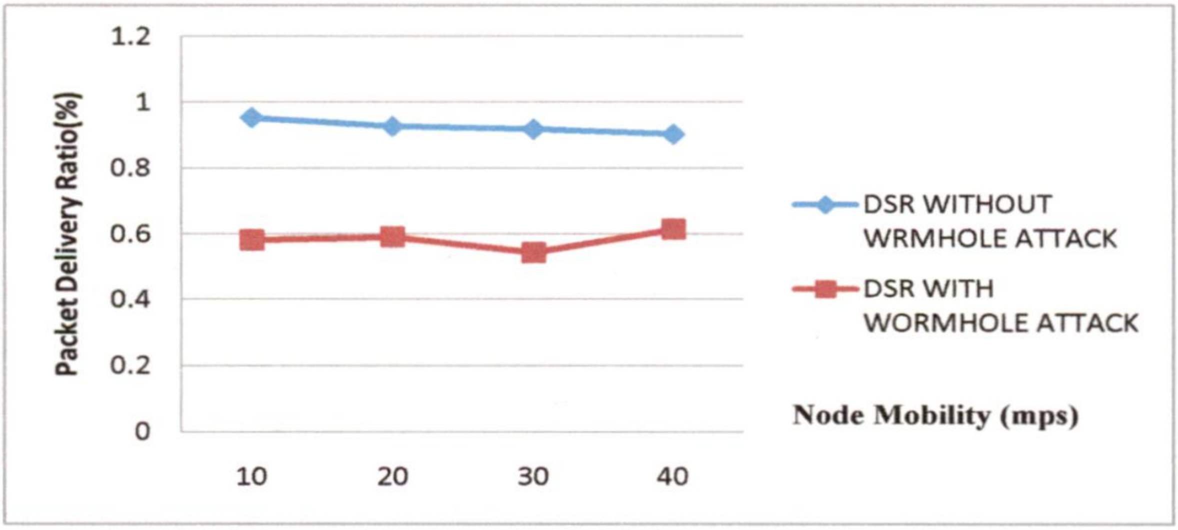


Figure 5.1 Packet Delivery Ratio for Dynamic Source Routing with and without wormhole attack

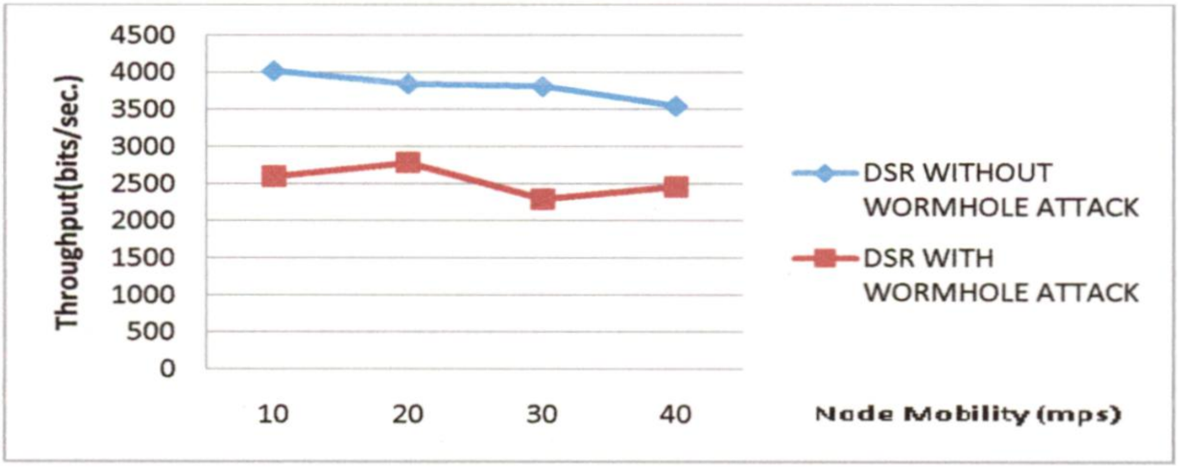


Figure 5.2 Throughput for dynamic source routing with and without wormhole attack

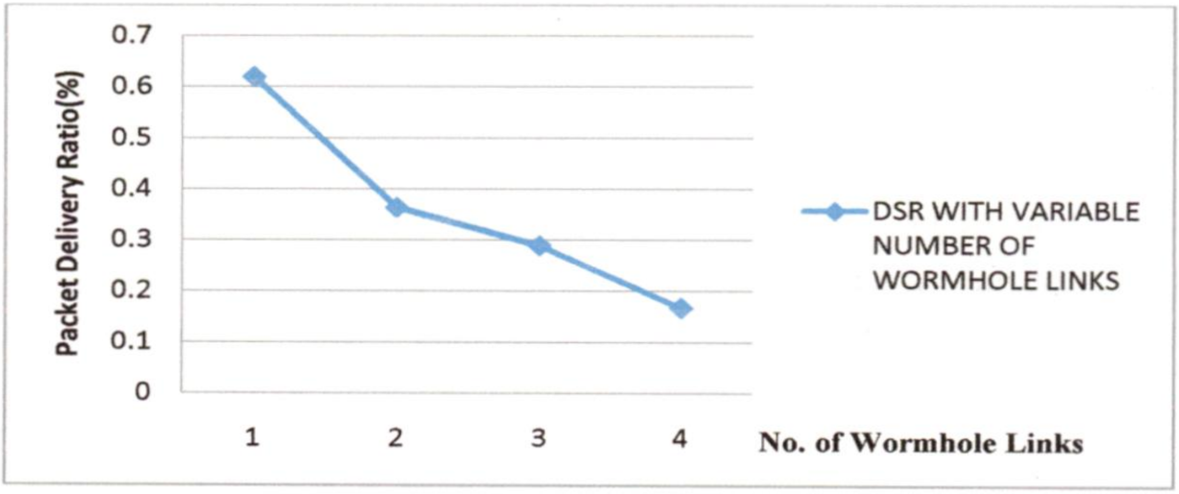


Figure 5.3 Packet Delivery Ratio for DSR protocol with variable number of wormhole Links

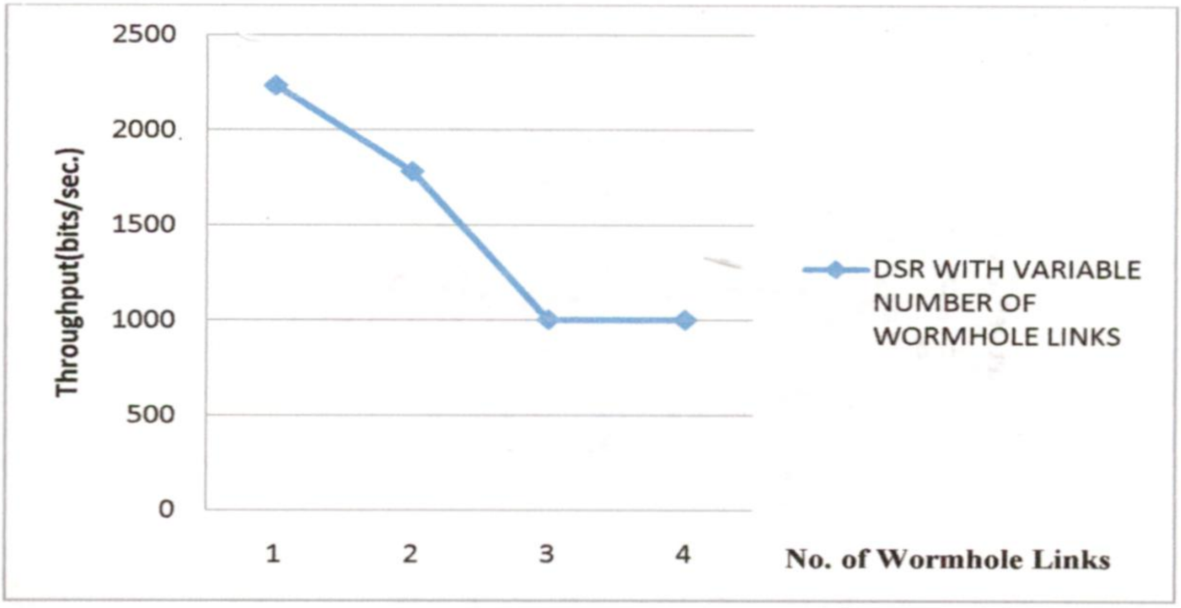


Figure 5.4 Throughput for DSR protocol with variable number of wormhole Links

5.3 Results of Multipath Routing Protocol with and without Wormhole Attack with varying Pause Time

Scenario III given in section 4.3 of chapter 4 is used to simulate the behaviour of network. In this simulation pause time is varied. Pause time is used in random waypoint mobility model. In this nodes moves in a random direction and stay in a position for certain amount of time. This stay time is called pause time. Previously, performance is measured by varying the node mobility making the network unstable. In this we have varied the pause time making the network stable. As we increase the pause time network becomes stable. Threshold value of wormhole is taken 75.

a) **Packet Delivery Ratio:** It is the ratio of number of packets delivered to the destination to the number of packets sent by source. In this only one wormhole link is created between node 18 and node 19. Number of nodes taken is 30. Figure 5.5 shows that in the presence of wormhole link packet delivery ratio of multipath routing protocol is decreased. This is because the wormhole nodes drop the data packets passing through them.

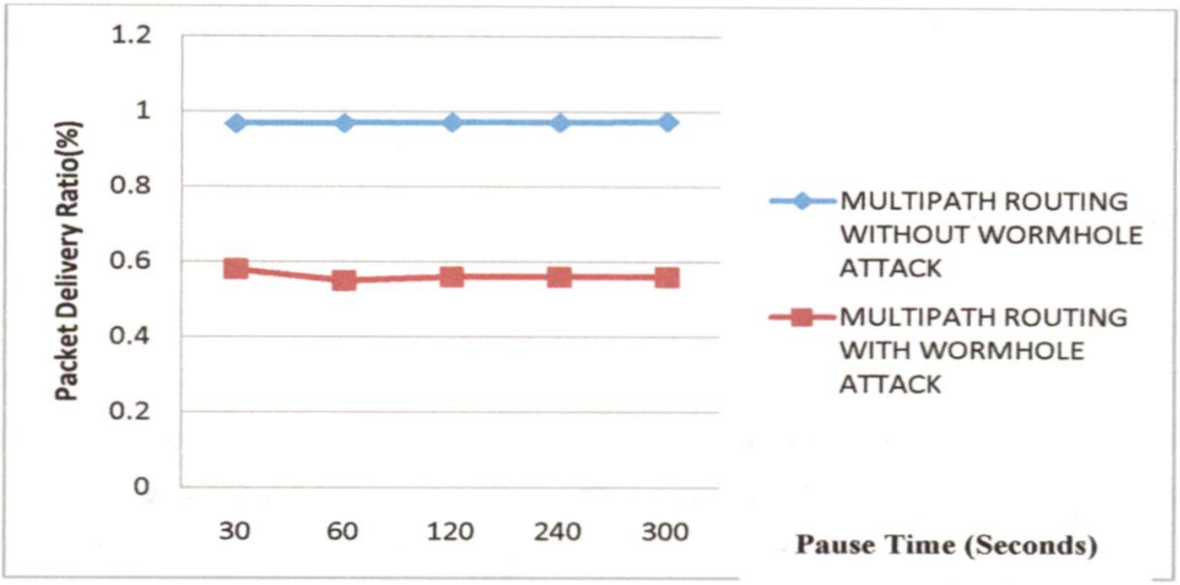


Figure 5.5 Packet Delivery Ratio for Multipath Routing with and without wormhole attack

b) **Throughput:** It is average rate of successful message delivery over a communication channel. It is measured in bits per seconds. Figure 5.6 shows that in the presence of wormhole link throughput of multipath routing protocol have been decreased. It almost half the throughput of the network without wormhole attacks. This is because the data packets are dropped by wormhole nodes and bandwidth available is not being used for transmission of data packets. So wormhole attack also decreases the performance of multipath routing protocol.

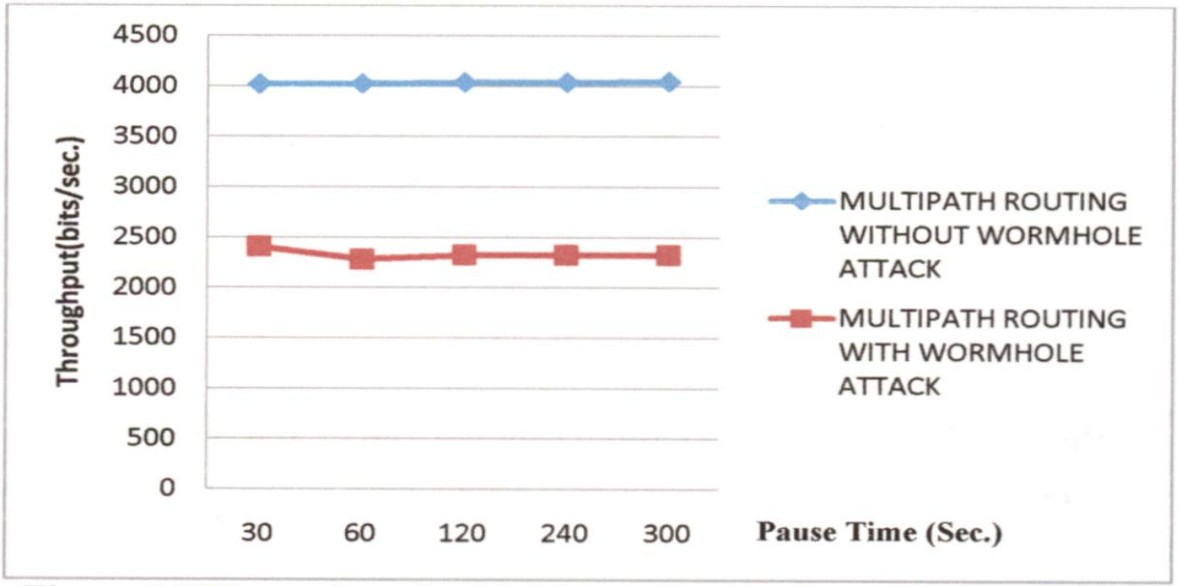


Figure 5.6 Throughput for Multipath Routing Protocol with and without Wormhole Attack

5.4 Results of MRWDPDP with Multipath Routing under Wormhole Attack with variable Wormhole Links

Scenario IV given in section 4.3 of chapter 4 is taken in to consideration. Number of nodes taken is 30 and simulation time taken is 100 seconds. Numbers of wormhole links are varied from 1 to 4. Wormhole links are created between nodes 4-19, 16-21, 23-30, 9-20. One wormhole link is placed near the source and destination node. Other wormhole links are placed randomly in the network.

a) **Packet Delivery Ratio:** It is the number of packets received at the destination to the number of packets sent. Figure 5.7 shows the comparison of MRWDPDP with the multipath routing protocol under wormhole attack. Figure 5.7 shows that multipath routing protocol with MRWDPDP delivers more data packets than multipath routing protocol without new approach and as there is increase in wormhole links the performance of both is decreased but still MRWDPDP delivers more data packets. So effects of wormhole attack on packet delivery ratio of multipath routing protocol are reduced with this approach.

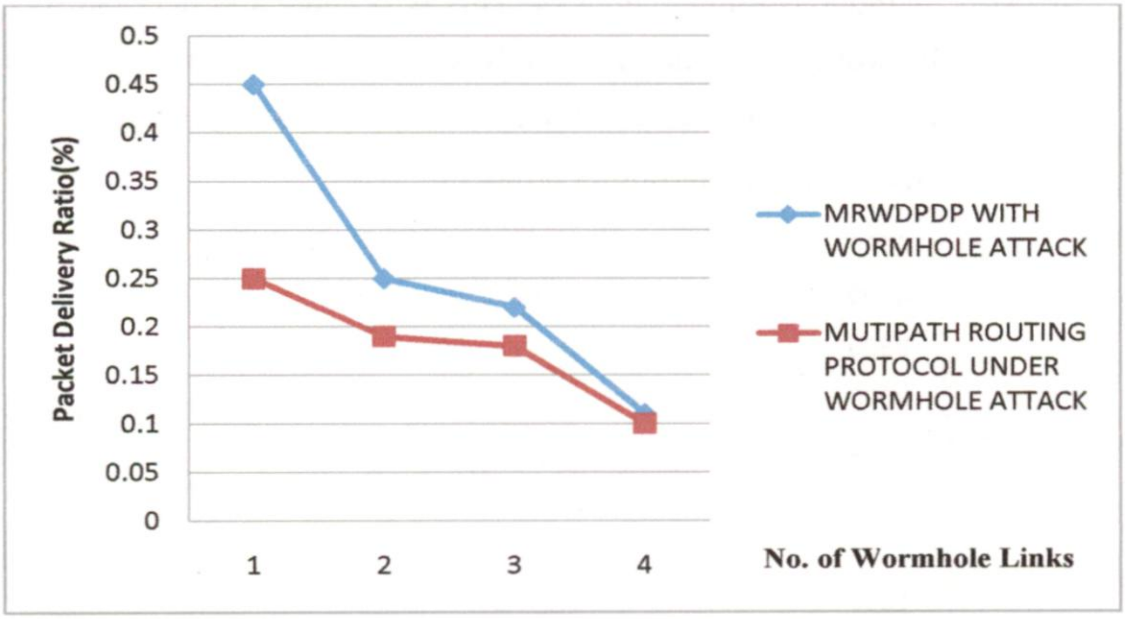


Figure 5.7 Packet Delivery Ratio Comparison of MRWDPDP with Multipath Routing Protocol under wormhole attack with varying number of wormhole link

b) Throughput: It is average rate of successful message delivery over a communication channel. It is measured in bits per seconds. Figure 5.8 shows the results of MRWDPDP and multipath routing protocol. It shows that in the presence of one wormhole link throughput of multipath routing is less as compared to MRWDPDP and as number of wormhole links increases throughput of both decreases but MRWDPDP still have higher throughput than the multipath routing protocol. So the solution has eliminated the effects of wormhole on the multipath routing protocol.

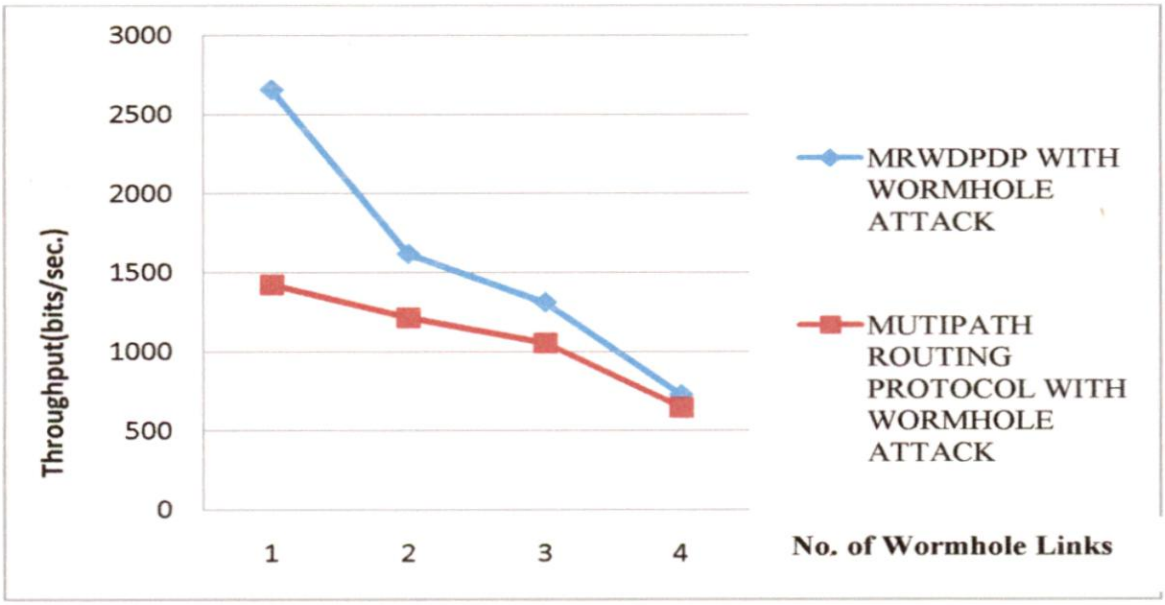


Figure 5.8 Throughput Comparison of MRWDPDP with Multipath Routing Protocol under wormhole attack with varying number of wormhole link.

Protocol	Based on	Extra Hardware	Clock Synchronization	Mobility	QoS Parameters
Packet Leashes[17]	None	Yes	Yes	No	No
WAP[18]	DSR	No	No	Yes	Throughput,PDR
WARP[19]	AODV	No	No	Yes	Packet Loss Rate
DelPhi[20]	AODV	No	No	No	No
Distance Verification and Hypothesis Testing[24]	None	Yes	No	Yes	No
SEEEP[23]	None	Yes	No	Yes	No
MHA[21]	AODV	No	No	Yes	Not Considered
SAM[22]	DSR	No	No	Cluster and Uniform Topology is considered	Not Considered
Wormeros[25]	None	No	Time Synchronization not considered, RTT between nodes is considered	Topology Change is not Considered	Not Considered
MRWDPDP	Multipath Routing	No	No	Yes	PDR, Throughput

Table 5.1 Comparison between MRWDPDP and related

Chapter 6

Conclusions and Scope for Future Work

6.1 Conclusions

In this dissertation work, approach for detection and prevention of wormhole attack on multipath routing protocol is proposed called MRWDPDP (Multipath Routing Wormhole Detection and Prevention using Dummy Packet). Two new packets Dummy_Request and Dummy_Reply are introduced. DSR protocol is firstly converted to multipath routing protocol by changing the way intermediate node forwards the route request. By changing DSR it becomes multipath routing protocol and during discovery of route from source to destination multiple routes are collected. Effects of wormhole attack are measured on both DSR routing protocol and multipath routing protocol. Performance of DSR routing protocol is measured by changing the node mobility (making network unstable) and varying the wormhole links. Performance of multipath routing is measured by changing the pause time (making the network stable) and performance of MRWDPDP and multipath routing is evaluated and compared by varying the wormhole links. Two parameters (Packet Delivery Ratio and Throughput) are taken in to consideration to measure the effects. Results show that:

i) Performance of DSR routing protocol is decreased to half in the presence of wormhole attack.

ii) Performance of DSR routing protocol decreases with the increase in wormhole links.

iii) Performance of multipath routing protocol also decreases in the presence of wormhole attack.

iv) MRWDPDP increases the packet delivery ratio and throughput of multipath routing protocol in the presence of wormhole attack as compared to multipath routing protocol under wormhole attack.

6.2 Scope for Future Work

In this dissertation work, wormhole detection and prevention approach is proposed. The following domains can be considered for future work.

i) A new procedure should be invented by which malicious nodes can be identified.

ii) Proposed Approach fails in scenarios where multiple paths are not possible and large numbers of wormhole nodes are available.

iii) Digital Signature can be applied on the Dummy_Request and Dummy_Reply packets for authentication of sender.

REFERENCES

[1] Klara Nahrstedt, Wenbo He, and Ying Huang, "Security in Wireless Ad Hoc Networks". Guide to Wireless Ad Hoc Networks pp no. 391-425© Springer-Verlog London Limited 2009

[2] Tuan Anh Nguyen, B.S "Evaluations of Secure MANET Routing Protocols
in Malicious Environments" THE UNIVERSITY OF HOUSTON-CLEAR LAKE May, 2006

[3] Yang Xiao, Xuemin Shen and Ding-Zhu Du " Wireless Network Security" Springer International Edition 2007.

[4] Joseph Macker and Scott Corson Mobile ad-hoc networks (MANET). http://www.ietf.org/proceedings/01dec/183.htm, December 2001

[5] J. Mackar and S. Corson, RFC 2501, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF 1999.

[6] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester " An Overview of Mobile Ad Hoc Networks: Applications and Challenges"
*www-di.inf.puc-rio.br/~endler/.../**Mobile**/.../MANET-**Challenges**.pdf*

[7] C. Perkins, Ad Hoc Networking, Addison-Wesley 2001, ISBN 0201309769

[8] J.M.Kahn, R.H.Katz and K.S.J.Pister, " Next Century Challenges: Mobile Networking for Smart Dust". ACM Press 1999
http://www.saab.se/future/node2567.asp.

[9] Chim Yuen Chong, Raymond Seah Kwang Wee, Sim Soon Lian, Tan Jia Hui "Moblie Ad hoc Networking"
http://www.dsta.gov.sg/DSTA_horizons/2006/Chapter_7. html

[10] C.Perkins and P. Bhagwat. Highly dynamic destination sequenced distance-vector routing for mobile computers. *Computer Communication Review*, pages 234-244, October 94.

[11] D. Johnson and D. Maltz and Yih-Chun Hu. . *http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-07.txt. Dynamic Source Routing,*

[12] C. Perkins and E. Royer. Ad-hoc on-demand distance vector routing. *In Proc. Of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90-100, Feb 1999

[13] Z. Haas and M. Pearlman. The performance of query control scheme for the zone routing protocol. *ACM/IEEE Transactions on Networking, 9(4) pages 427-438*, August 2001

[14] S. Basagni, I. Chlamtac, V. Syroutik, and B. Woodward. A distance effect routing algorithm for mobility (DREAM). *In proceedings of the 4th annual ACM/IEEE Int. Conf. on Mobile Computing and networking (MOBICOM)*, pages 76-84, Dallas, TX, USA, 1998

[15] Karp, B., and Kung. H. T. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. *Proc. 6th Annual International Conference on Mobile Computing and Networking (MOBICOM 2000), 243-25*

[16] Young-Bae Ko, Nitin H. Vaidya. Location-aided routing (LAR) in mobile ad-hoc networks. ACM/Blatzer Wireless Networks journal, 6(4) pages 307-321, 2000

[17] Y.-C. Hu, A. Perrig, and D.B. Johnson. "Packet Leashes: A defense against Wormhole Attacks in wireless networks. IEEE INFOCOM, Mar 2003.

[18] Sun Choi, Doo-young Kim, Do-Hyeon Lee, Jae-il Jung" WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks" © IEEE 2008.

[19] Ming-Yang Su" WARP: A wormhole- avoidance routing protocol by anomaly detection in mobile ad hoc network" Computers and Security 29(2010) 208-224 © 2009 Elsevier Ltd.

[20] Hon Sun Chiu and King-Shan Lui "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks"© 2006 IEEE.

[21] Shang-Ming Jen 1, Chi-Sung Laih 1 and Wen-Chung Kuo" MHA: A Hop count analysis Scheme for Avoiding Wormhole Attacks in MANETs" *Sensors* 2009.

[22] Lijun Qian, Ning Song, and Xiangfang Li" Detection of Wormhole attacks in multi-path routed wireless ad hoc networks: A Statistical analysis approach"© 2005 Elsevier.

[23] Neelima Gupta and Sandhya Khurana " SEEEP: Simple and Efficient End-to-End protocol to Secure Ad Hoc Networks against Wormhole Attacks" © 2008 IEEE.

[24] Yifeng Zhou Louise Lamont Li Li " Wormhole Attack Detection Based on Distance Verification and the Use of Hypothesis Testing foe Wireless Ad Hoc Networks" © 2009 Crown

[25] Hai Vu, Ajay Kulkarni, Kamil Sarac, and Neeraj Mittal " WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks" WASA 2008, LNCS 5258, pp. 491-502, 2008

[26] Qulanet available online http://scaleable-networks.com

LIST OF PUBLICATIONS

[1] **Ravinder Ahuja** "Simulation based Performance Evaluation and Comparison of Reactive, Proactive and Hybrid Routing Protocols based on Random Waypoint Mobility Model", International Journal of Computer Applications, vol. 7, no. 11, pp. 24-31, October, 2010 published by Foundation of Computer Science.
DOI: 10.5120/1291-1765.
URI: http://www.ijcaonline.org/archives/volume2/number9/1291-1765.

[2] **Ravinder Ahuja** and Padam Kumar, "Performance Evaluation and Comparison of on demand Routing Protocol with or without Wormhole Attack " Second International Conferences on Advances in Computer Engineering-ACE 2011 is scheduled to held on 25-26 August, 2011 at Trivandrum, Kerla, India (Accepted).

[3] **Ravinder Ahuja** and Padam Kumar, "A New Approach for Detection and Prevention of Wormhole Attack on Routing Protocol of MANETs", In ACEEE International Journal on Network Security-IJNS (Accepted).