A THESIS

ON

A FRAMEWORK TO DETECT AND MITIGATE WORMHOLE ATTACK IN MOBILE WIRELESS AD-HOC NETWORK

By

RAJ SHREE

DEPARTMENT OF INFORMATION TECHNOLOGY

Submitted in fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

To the

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A Central University)
Lucknow, India

Dec-2014

A THESIS

ON

A FRAMEWORK TO DETECT AND MITIGATE WORMHOLE ATTACK IN MOBILE WIRELESS AD-HOC NETWORK

By

RAJ SHREE

DEPARTMENT OF INFORMATION TECHNOLOGY

Submitted in fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

To the

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A Central University)
Lucknow, India-226025

Dec-2014

DECLARATION

I, Raj Shree, solemnly declare that this thesis of research on '**A Framework to Detect and Mitigate Wormhole Attack in Mobile Wireless Ad-Hoc Network**' is my original work. The study has been conducted under the guidance of Dr. Raees Ahmad Khan, at Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow (U.P.), India-226025. It is further declared that to the best of my knowledge and belief it has not been submitted earlier for the award of any degree.

Dated:

(Raj Shree)

Research Scholar
Department of Information Technology
Babasaheb Bhimrao Ambedkar University
(A Central University)
Lucknow, (U.P.), India-226025

CERTIFICATE

It is certified that thesis entitled '**A Framework to Detect and Mitigate Wormhole Attack in Mobile Wireless Ad-Hoc Network**' being submitted by Mrs. Raj Shree is a record of bonafide work carried out by her. She was worked under my guidance and supervision. She has fulfilled the requirements for submission of thesis, which to my knowledge has reached the requisite standard. In my view, the contents of this thesis and interpretations have substantially added to the existing knowledge on the subject.

This thesis presented by her, to the best of my knowledge and belief, did not form the basis for the award of any degree earlier.

(Dr. R. A. Khan)

Supervisor
Department of Information Technology
Babasaheb Bhimrao Ambedkar University
(A Central University)
Lucknow, (U.P.), India-226025

Dated:

ACKNOWLEDGEMENTS

I am thankful to **GOD** for providing me this opportunity to express solemn gratitude and regards for **Dr. R. A. Khan**, Associate Professor, Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, for his consistent supervision, valuable guidance and encouraging attitude during the course of this thesis work. His research expertise, his breadth of knowledge, vision for the future, and his enthusiasm for research has been an inspiration to me. He is a motivator, a facilitator, a challenger, and above all a good human being. No words are sufficient to express my thanks and gratitude to **Prof. R. C. Sobti,** Honourable Vice Chancellor, Babasaheb Bhimrao Ambedkar University, Lucknow, for their exemplary cooperation and motivation during the course which helped me to accomplish this thesis. His direction has been invaluable and my life has been enriched personally, intellectually and professionally by working with him.

I would like to thank **Mr. Ravi Prakash Pandey**, Assistant Professor, Dr. RML Avadh University, Faizabad for his insights in wireless sensor networks. His advice in setting up my research directions was a great help while his encouragement, critiques and feedback have greatly enhanced and strengthened my research. I have great love and respect for him who helped me a lot throughout this thesis work.

I would like to thank my brother **Mr. Vivek Shukla** and sister **Ms. Jaishree Shukla** for their love and support, and especially my parents (**Mr. Nageshwar Prasad** & **Mrs. Kusum Shukla**) and my in-laws (**Capt. Ram Prakash Pandey and Mrs. Mithilesh Pandey**) for all they have given me. They taught me the value of knowledge and the importance of family, and have stood by me at all times, providing constant support, encouragement and love.

I would like to thank to all my friends and colleagues for providing moral support. I would like to thank to all the experts from India and abroad for their valuable observation during review process. Finally, I would like to thank to all other **faculty members (Dr. Dhirendra Pandey & Mr. Pawan Kumar Chaurasia) and office staff** of the Department for their cooperation and continuous support extended during the thesis work.

Raj Shree

ABSTRACT

Wireless Networks are formed by a number of static and dynamic nodes to establish communication. Due to ad hoc in nature, they are gaining a lot of popularity in the field of research and users of mobile are increasing day by day. With the advent of these networks, information sharing has become feasible because of easy deploy ability in remote and difficult unattended areas. Mobile Ad hoc Networks can be easily set up because of self-organization characteristics and wireless medium. Other characteristics that attract attention towards Wireless Networks are lack of centralized fixed infrastructure, adaptability to frequent change in topologies etc... Due to nodes mobility and frequent change in topologies, Wireless Networks are susceptible to a variety of attacks. Further, MANET has the open and dynamic operational environment that makes MANET vulnerable to various network attacks. Most of the time, routing protocols are the common target for a common type of attacks. These attacks can involve in damaging, modifying, discarding routing information, manipulating information, advertise fake routes, misrouting information and eavesdropping. The situation may be precarious for confidential communication. There are different types of attacks that can harm Wireless Networks at different layers of communication and degrade network performance. The examples of these types of attacks are as Eavesdropping, Jamming, Traffic analysis and monitoring, Denial of Service, Gray hole attack, Black hole attack, Wormhole attack etc.

Ad-hoc network is a collection of several wireless nodes that are capable of communicating directly with each other without having any infrastructure or any centralized administration. Multihop communication can be created by making nodes as routers. That means all nodes which involve in ad hoc network can be act as router. The wireless node can give wide range of application because of node mobility and frequent topology changes, especially in military operations and emergency & disaster relief efforts. Because of open wireless medium used dynamic topology and distributed & cooperating sharing of channels, ad-hoc networks are more vulnerable to security attacks than conventional wired and wireless networks. In this research, researcher is describing wormhole attack for distributed wireless network. This attack is so powerful that the detection of this attack is so difficult. It can be easily launched by the intruder without having the knowledge of the network or compromising any legitimate nodes. In the wormhole attack, a malicious node captures the packet on one location in the

network and tunnels them to another malicious node at a distant point which replays them locally.

The objectives of the thesis are two-fold: (a) To simulate various scenarios of wormhole attacks at MANET (b) To study the performance and effectiveness of proposed secure routing protocol in these simulated malicious scenarios.

Name of Tables

Name of Figures

TABLE OF CONTENTS

Chapter 1: Introduction

1.1 Background

A mobile wireless ad hoc network is a cluster of self-ruling nodes or terminals that exchanges packets and correspond with each other by establishing a multi hop radio network and providing connectivity in a decentralized way. Since all nodes in the network use wireless linkage to communicate with each other, they have to deal with the consequences of radio communication. These consequences are noise, fading and interference. Every node in a mobile wireless ad hoc network can act as a host as well as a router. The command of the network is allocated among the nodes belonging to that network. In these types of network, topology will be dynamic because of node exit from the network, new node entrance in the network or mobile nature of nodes. Therefore, in other words, the connectivity among the nodes may vary with time due to node exit, arrival, and mobile nodes. Hence, there is a requirement for well-organized routing protocols that can allow all nodes to communicate

over multi-hop pathway during dynamic topology and able to address the issue of dynamic topology, efficiently. These protocols ensure that traveled packet should reach to correct destination.

As the time is passing, people are taking interest in wireless ad hoc networks. With advancements in technologies, the cost of mobile devices like tablets, laptops, mobile phones etc. is decreasing drastically. The most recent trend in wireless networks is in the direction of pervasive computing, providing to both roaming and fixed users, anytime and anywhere. There are a number of standards for ad hoc networks and these standards full fill the needs of every person or institute where they want to use wireless environment. Mobile ad hoc networks can be used to extend connectivity in association with wired or fixed infrastructure in those places where wired infrastructure is hard to establish.

There are several situations in which mobile ad hoc networks can be used as an extension for connectivity. For example, soldiers in battlefield, people affected by flood can contact with each other and outside world with the help of wireless ad hoc networks. With the help of wireless ad hoc network, communication amongst soldiers in battlefield is a very sensitive matter. Because, it is expected that enemy would not be able to hear the conversation. From this point of view, security concept took attention from the research community in mobile wireless ad hoc networks. Now, the researchers tried to start work on secure routing protocols that can ensure secure communication between source and destination. Therefore, researchers want to add security feature with existing routing protocol or develop new security enabled routing protocol.

1.2 Wireless Ad Hoc Network

Ad hoc network is a collection of number of nodes that can forward data packets to other nodes during communication in wireless environment. These nodes can act as a host as well as router. Discovery of next node is a dynamic process based on the protocol used in the network connectivity. Ad hoc networks support multi-hop routing that means when source and destination node is out of radio range then for sending and receiving a message source and destination node use intermediate nodes. Nodes in the network can leave the network or join the network at any instant of time and make the network topology dynamic in nature.

Mobility of nodes and ease of deployment like characteristics of ad hoc network is gaining attention from industrial area, academic world and government. That's why in contrast to traditional infrastructure-based networks, in which nodes use hardware like cables, routers, switches and firewalls to transmit data from one place to another, ad hoc networks are more suitable for disaster situations like natural or human-instigated disasters, military war time, emergency medical situation etc. [1]. Therefore, these networks can be deployed easily where infrastructure establishment is not possible. In wired networks, installing cable is very lengthy and time consuming process and their maintenance is also very difficult. Now a day, wireless communication is rich with a variety of standards with unique frequency band, coverage and range of application. These standards have developed gradually for Local Area Networks, Personal Area Networks, Broadband Wireless Access, Vehicular Ad hoc Networks, as well as Internet Based Mobile Ad hoc Networks.

1.2.1 A Brief History

History of mobile ad hoc networks began with the applications of tactical networks related applications to develop battlefield communications. Military personnel use highly dynamic environment for executing war related operations that's why they cannot rely on access to a fixed infrastructure in battlefield. In wireless communication, radio signals with interference and radio frequency higher than 100 MHz rarely propagate beyond line of sight (LOS) [2]. Mobile ad hoc network creates an appropriate framework to deal with these issues by providing a multi-hop wireless network without pre-placed infrastructure and connectivity beyond LOS.

The whole life-cycle of ad hoc network could be classified into first, second, third and fourth. Present ad hoc networks systems are considered the third-generation which opens the door for fourth-generation ad hoc networks. The first generation of Ad hoc networking applications started with packet radio networks called PRNet with DARPA project in 1972 [2], which was mainly inspired by the effectiveness of the packet switching technology. Packet switching technology has the capabilities like bandwidth sharing and store-and-forward routing, and made possible application in mobile wireless environment. PRNet provides a distributed architecture consisting of network of broadcast radios with minimal central control; a combination of Aloha and CSMA channel access protocols are used to

support the dynamic sharing of the broadcast radio channel and to provide different networking capabilities in a combat environment. In addition, to cover a very large geographical area and to remove radio coverage limitation, protocol use multi-hop store-and-forward routing techniques.

The thought of second generation of ad hoc networks was started in 1980s, with the advancements in ad hoc networks as Survivable Radio Networks (SURAN) being developed by DARPA in 1983. The main motive was to improve PRNet, to scale the areas of network, to provide protection, dealing out capability and to save energy and to develop such type of network algorithms that can scale to tens of thousands of nodes and use small, low-cost, low-power radios that could maintain complicated packet radio protocols [2]. This program proved to be beneficial as it improved the radios' performance by making them small in size, cheap in cost, and durable to electronic attacks and further marks in the plan of Low-cost Packet Radio (LPR) technology in 1987 [3], which characterises a digitally controlled DS spread-spectrum radio with an incorporated Intel 8086 microprocessor-based packet switch.

To sustain network scalability several advanced network management protocols came into existence. At that time, to support network scalability, hierarchical network topology based on dynamic clustering has been also used. Through management of spreading keys, other improvements in radio flexibility, safety, and increased capacity are achieved [4]. Just before late 1980s and early 1990s, the development of the Internet infrastructure and the microcomputer uprising made the initial packet radio network ideas more relevant and practicable [2].

In the 1990s, the concept of commercial ad-hoc networks [5] came with notebook computers and other workable communications equipment. At the same time, the thought of a group of mobile nodes was projected at several research conferences. The IEEE 802.11 [6, 10] subcommittee has approved the word "ad-hoc networks" and the research society has started to look into the options of deploying ad-hoc networks in other areas of application. To influence the worldwide information infrastructure into the mobile wireless environment, DoD began DARPA Global Mobile (GloMo) Information Systems program in 1994 [7], which intended to maintain Ethernet-type multimedia connectivity all time, everywhere among wireless devices. Numerous networking plans were investigated; for example the Space and Terrestrial communications directorate (STCD) started a data radio market survey

in May, 1994. The survey was for off-the-shelf commercial high data networked radio technology that could be used by the Army. The results from the survey were used to prepare a Future Digital Radio Broad Area Announcement (FDR BAA).

Shortly after the release of the BAA, the FDR BAA merged into the Near Term Digital Radio (NTDR) program started by the Army Acquisition Executive [8]. NTDR [9] is the only "genuine" non-prototypical ad-hoc network that is in exercise today. It exploits clustering and link-state routing. Further it is self-organized into a two-tier ad-hoc network [11]. Progress of various channel access methods now in the CSMA/CA and TDMA patterns, and numerous other routing and topology control systems were a few other developments of that time.Wireless Internet Gateways (WINGs) at UCSC sets up a flat peer-to-peer network structural design, while Multimedia Mobile Wireless Network (MMWN) project from GTE Internetworking exercises a hierarchical network architecture that is based on clustering techniques.

Tactical Internet (TI) implemented by US Army at 1997 is by far the largest-scale implementation of mobile wireless multi-hop packet radio network [2]. Direct-sequence spread-spectrum, time division multiple access radio is in use with data rates in the tens of kilobits per second ranges. Whereas, to create networking among nodes, modified commercial Internet protocols are used. It emphasizes the view that commercial protocols for wired infrastructure were not good at handling frequent topology changes with low data rate, and high bit error rate wireless links [12]. Later on in mid-1990s, within the Internet Engineering Task Force (IETF), the Mobile Ad-Hoc Networking working group was structured to regulate routing protocols for ad-hoc networks. The improvement of routing protocol within the operational group and the larger society answered in the discovery of reactive and proactive routing protocols.

In 1999, expanding the Littoral Battle-space Advanced Concept Technology Demonstration (ELB ACTD) was another MANET exploitation to express the feasibility of Marine Corps war fighting thoughts that involve over-the-horizon (OTH) communications from ships at sea to Marines on land via an aerial relay. Around 20 nodes were put together for the network. Further, Lucent’s WaveLAN and VRC-99A were applied to construct the access and backbone network connections. The ELB ACTD was victorious in representing the utility of aerial relays for linking users beyond LOS. In the centre of 1990, with the

description of standards (e.g., IEEE 802.11 [13]), commercial radio technologies have started to come into prominence, and the wireless research society became attentive of the great industrial prospects and advantages of mobile ad hoc networking outside the military domain.

The IEEE 802.11 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals thus making it functional for structuring mobile ad-hoc networks. Wireless local area products (IEEE 802.11, Hiperlan [14]) offer in-building wireless access, though they are generally set up as access connections only, packet spreading being executed by conventional bridges or routers. For short range communication, Bluetooth is a low cost technology. Its target market included appliances, watches, PCs, phones etc. It helps several nodes to join to each other in a multi-hop arrangement.

Attempts are on to regulate the methods offered for different ad hoc networks, organized into a single skeleton which could be established as a standard for the future implementations [15]. Day by day, Wireless devices are getting small in size, cheap in cost, and more sophisticated. As these devices are accepting ubiquitous concept, societies are coming across for economical approaches to stay connected using these devices and Ad-hoc network can provide this successfully [16]. Most of the existing ad hoc networks outside the military arena have been developed in the academic environment followed by commercially oriented solutions.

The main objective for 4G Wireless evolution is to provide pervasive computing environments that can seamlessly and ubiquitously support mobile users in completing their activities, in assessing information or transferring data with other users at any point of time and from any device [17, 18, 19, 20]. The new trend is to help users in the tasks of everyday life by exploiting technologies and infrastructures hidden in the background, exclusive of involving any major alteration in the users' behavior. This new philosophy is the root of the Ambient Intelligence idea [21].

The purpose of ambient intelligence is the combination of digital devices and networks into the daily situation, rendering handy, through simple and ‘‘natural’’ dealings. Ambient intelligence keeps the customer at the centre of the information society. This outlook greatly relies on 4G wireless and mobile communications. 4G is all about an

incorporated, universal network, based on an open systems approach [22]. The main foci of 4G are on to put together diverse types of wireless networks with wired infrastructure as backbone network seamlessly, and union of voice, multimedia and data traffic over a single IP-based core network.

With the accessibility of ultra-high bandwidth of up to 100 Mbps, multimedia facilities can be maintained efficiently. With enhanced system mobility and portability support, ubiquitous computing can be enabled in any network. 4G starts with the assumption that future networks will be entirely packet-switched [23]. For example, voice and data union can be maintained by using readily obtainable VoIP group of protocols such as MGCP, SIP, MEGACOP, H.323, SCTP, etc [5, 22].

1.2.2 Challenges

Ad hoc networks are different from infrastructure-based networks in two ways first ad hoc networks always use peer-to-peer communication secondly each node in the ad hoc networks work as a host as well as router. These differences make base for challenges in ad hoc networks. These challenges are unique from challenges in infrastructure-based networks and open door for research and opportunities for making significant contributions:-.

- Nodes working in ad hoc networks have limited resources like bandwidth, energy, computational power, battery, memory [24, 25].
- Mobility in nodes make ad hoc network dynamic in nature and result in frequent route breaks. The sudden change in movement of nodes often occurs with frequent network partitions that creates problem to intermediate nodes [26, 27].
- Discovery of mobile terminals and right routing of packets to and from each terminal while moving are surely challenging [28, 29].
- The limited radio frequency is available for wireless communication. Therefore, reusing frequency in efficient way is a big challenge to increase number of mobile users [30, 31].
- Due to hidden terminals, interference, frequent breakage in paths and unidirectional links, the condition of collisions occur during communication. This results higher packet loss in Wireless Mobile Ad hoc Networks during transmission [32, 33].

- Mobility characteristics of node allows mobile node to join or leave network anytime. There is no need for centralized administration for establishing MANETs. Because of this, these networks are susceptible to variety of attacks [34].
- Apart from above discussed challenges, a very important challenge is security [35, 36].
- The other characteristics of MANETs that make network vulnerable are consistent zero-administration personal environment, the absence of infrastructure and the consequent absence of authorization facilities [36, 37].

Therefore, there is a need of clear guidelines to detach the trusted available solutions for mitigating attacks from the non-trusted solutions. This will be based on an appropriate security policy, control of necessary identification and the capability of nodes to validate them.

1.2.3 Routing

Infrastructureless network and the ability of mobile users to join or leave network are the characteristics of MANETs which make packet routing a challenging task. Previously available techniques for routing can be divided into topology-based routing and position-based routing [38]. Topology-based routing protocols rely on the links that present in the network to perform packet forwarding. They are of three types, first proactive, reactive and hybrid approaches.

Proactive algorithms are traditional routing strategies such as distance vector routing (DSDV) or link state routing e.g. OLSR and TBRPF. Proactive protocols keep information about all the available links in the network even if links are not currently used. The main drawback of these protocols is maintaining unused links occupy some amount of available bandwidth even if network topology changes frequently [39]. To overcome these drawbacks in proactive protocols, reactive protocols were developed e.g. DSR, TORA and AODV. Reactive routing protocols maintain only those paths that are presently in use during communication. Because of this characteristics, only a small subset of available routes is required to store thus reduce the load on the network. However, there are some drawbacks in reactive protocols [40].

Due to the fact that routes are only maintained while in use, there is a need of route discovery process before starting communication or exchanging packets between nodes. This delays first packet to be transmitted and increases a significant amount of network traffic. If destination node is far away from source node then the generated link can be lost due to mobility of nodes. To rectify the drawbacks of proactive protocols and reactive routing protocols, hybrid ad hoc routing protocols were developed. These protocols have the characteristics of both proactive and reactive routing protocols. The example of these types of protocols is ZRP that combine the qualities of proactive and reactive routing protocols and achieve a higher level of efficiency and scalability. However, hybrid protocols combine both the strategies still there are a need to maintain at least those path that are presently in use. This resists maintenance of generated path during communication.

Apart from topology-based routing algorithms, position-based routing algorithms overcome some of the limitations of topology-based routing algorithms by adding extra information. They rely that the information about the physical position of the participating nodes should be available. Each node in the network determines its own position with the help of GPS or any other available positioning approach.

To start communication, sender can use location service to determine the position of the destination. After determining the position of destination, the sender adds destination address in packet to be sent. The routing decision at each node will be based on destination address in the packet and position of intermediate nodes between sender and receiver. Therefore, there is no need to maintain routes in position-based routing that restrict to store routing tables and to transmit messages for updating routing tables. Further, position-based routing can deliver packets to all nodes in a given geographic region in a normal way. This category of service is called as geocasting. Apart from routing approach, there should be an approach that can recover any problem automatically in a finite amount of time without intervening of human. In usual case, routing protocols are intended for fixed infrastructures and assume that routes are bidirectional. But, it is not always possible in the case for ad-hoc networks.

In this thesis, Reactive approach for routing is used. The reason behind with reactive approach is the popularity of using reactive routing protocols by a large amount of masses.

1.2.4 Routing Protocols

As above, mobile user join or leave ad hoc network at any time. This characteristic of ad hoc network makes to use routing protocol in an appropriate manner, a challenging task. Therefore, in this section, some popular routing algorithms, used for MANETs are discussed. Basically, there are two types of routing algorithms, one is a table driven routing protocol and second is on demand routing protocol. In table driven routing protocol, the network rely on links stored in routing table at each node. While in on demand routing protocol, sender initiates for path establishment between sender and receiver. Apart from table driven routing protocol and on demand routing protocol, some other types of routing protocols are available like hybrid protocol [41]. The working of some popular routing algorithms available for MANETs are discussed below: –

Destination-Sequenced Distance Vector (DSDV) Protocol

The Destination-Sequenced Distance Vector (DSDV) protocol is a type of table-driven routing protocol. The base of this protocol is classical Bellman-Ford routing algorithm. Therefore, it is enhanced version of Bellman Ford routing algorithm. The basis for DSDV [42, 43] is Routing Information Protocol (RIP) and distance vector routing. In RIP, all nodes in the network hold a routing table. This routing table stores the information about all the available destinations within the network and also keeps the information about the number of hops to each destination. DSDV uses bidirectional links during communication. To update routing table, each node periodically broadcasts and propagates routing information whenever network topology changes. Each DSDV node [44] maintains two types of routing tables.

One is for forwarding data packets and one for advertising incremental routing packets. Whenever a node sends an updated routing message, the sequence number will be incremented each time. If DSDV have two routes to choose, DSDV [45] will always consider route with greater sequence number. The updated packet will contain a new sequence number, address of destination, number of hops to the destination node and the previous sequence number of the destination. In normal situation, the sequence number will increment in even numbers. If sender find broken link to destination, sender will advertise route to destination with an infinite metric. At this point of time, the sequence number will one greater than its sequence number and make sequence number odd. According to odd

sequence number, all nodes that have information about broken link destination will update the routing table until there have sequence number in even. The advantage of DSDV is that it ensures loop-freedom. The drawback of DSDV is that it establishes only one path for a source to destination pair.

Optimized Link State Routing Protocols (OLSR)

The table driven protocols are also called proactive protocols. Optimised link state routing protocol is type of table driven routing protocols. It is an IP routing protocol for mobile ad hoc networks and other wireless networks. It is also called as link state routing protocol. There are two types of messages used in OLSR [46]. These messages are hello message and topology control message. With the help of these messages, OLSR discover and disseminate link state information within the mobile ad hoc network. Each node uses topology information to find out next hop destination for all nodes in the network. Link state routing protocols like Open Shortest Path first (OSPF) and Intermediate System to Intermediate System (IS-IS) select a router on every link to flood topology information. Hello messages are used to discover 2-hop neighbour information at each node. After that, distributed election of a set of multipoint relays (MPRs) is performed.

If node selects MPRs then there should be a path to 2-hop neighbours via a node elected as an MPR. These MPR nodes can be used to source and forward TC messages that have the MPR selectors. The MPR concept makes OLSR protocol [47] different from other link state routing protocols available. A subset of nodes source link state information that represents MPR selections is eligible to forward path for TC messages. To be coordinated across the network, link state routing uses topology database. Using this database, OSPF and IS-IS execute topology flooding using an efficient algorithm. It is very difficult to design efficient algorithm for topology flooding in ad hoc wireless network. Because of this only, OLSR doesn't worry to include reliability concept in algorithm. It only takes care to flood topology data. OLSR also makes sure that topology database will not remain un-updated for long period of time. Because OLSR is a proactive protocol, all paths to destination will be maintained before use [48, 49].

Therefore, no route discovery delay will be added to find new route. To allow Internet connection within OLSR MANET cloud, HNA messages can be injected into the system. To

ensure life of a message, timeout values and validity information will be added within the message. This message conveying information allows different timer values to be used at different nodes. The present OLSR does not have provisions to evaluate link quality. It simply takes care that a link is up for communication if number of hello packets are present. An open source OLSRd [50] (commonly used on Linux-based mesh routers) is available with link quality sensing (as of v. 0.4.8). OLSR is not suitable for small scale wireless networks. If researchers are using large scale mesh network, OSLRd can run network of thousands of nodes with very little CPU power on 200 MHz embedded devices. To compute optimal paths in the network, OLSR use a large amount of bandwidth and CPU power.

Dynamic Source Routing (DSR)

Apart from DSDV and OSLR, some on demand routing protocols are available for MANETs. DSR is the example of on demand routing protocol. DSR [51] uses source routing rather than relying on the touting table at each intermediate node. The advantage of using source routing is that the nodes between source and destination do not need to update or maintain routing information in order to forward packets. Therefore, in on demand routing protocols, there are no need for the periodic route advertisement and neighbor detection packets. There are two processes involved in DSR protocols. First is Route Discovery and second is route maintenance. In Route Discovery process, the path between source to destination node is discovered. Source node broadcasts RREQ (Route Request) packet to its one hop neighbours and this process continues until route request packet reach at destination node or packet's Time to Live (TTL) counter has not been exceeded. In response to RREQ packet, destination node sends back RREP (Route Reply) packet to source node using discovered path between source node to destination node through intermediate nodes.

To reduce the cost of Route Discovery, cache of source routes is required to store at each node [52]. In Route Maintenance process, the availability of discovered path between source to destination nodes will be ensured during communication. If nodes listed in discovered route have moved out of range of each other, route maintenance will indicate that discovered route is broken. After that, source node will broadcast RERR (Route Error) packet to all its neighbours. Now the sender will use any other route to destination already available in cache or can start Route Discovery process again to find a new route. Dynamic source routing protocol is designed to control the bandwidth consumed by control packets in ad hoc

networks by removing the concept of periodic table update messages required in table driven approach. It is a Beacon less protocol that means there is no requirement of periodic hello packet (Beacon) transmissions that can be used by each node to give information about its presence to neighbours. The drawback of this protocol is that the route maintenance process cannot locally repair a broken path. Out of date route cache information will also result in inconsistencies during the route reconstruction phase. The protocol works in static and low mobility environments. But the performance of the protocol degrades rapidly with the increase of mobility.

Temporally-Ordered Routing Algorithm (TORA)

The basis for TORA [53] protocol is link reversal algorithm. It is a distributed routing protocol used to discover paths on demand. This protocol provides more than one routes to destination and sets up routes quickly. It minimizes communication overhead occurred due to topological changes. For this protocol, Route optimality is considered of secondary importance. That is the cause of using longer routes to avoid the overhead of discovering newer routes in this protocol. The actions of TORA can be visualized in terms of water flowing downhill towards a destination node. Consider a network of tubes that forms the routing state of the real network [54]. The links can be represented by tubes between nodes in the network. Nodes will remain at the joint of tubes. The flow of water in the tubes will represent the packets travel towards the destination. Height of the water fall will be term as weight in the network. In the network, the weight of each node with respect to the destination will be computed by the routing protocol. If a tube between two nodes N1 and N2 becomes blocked or broken and restrict to flow water through it, the height of N1 will be set to greater than that of any other remaining neighbors, so that water will now flow back out of N1.

A logically separate copy of TORA is run at each node for each destination. When a source wants to communicate with destination, source will broadcasts a QUERY packet having the address of destination. Propagation of QUERY packet continues till it reaches to destination node. After receiving QUERY packet, each intermediate node broadcasts an UPDATE packet listing its height to destination. As each node receive multiple UPDATEs, each time, the height of receiver will be greater than the height of the neighbor. These multiple UPDATEs create a series of directed links from sender of the QUERY to the node that initially generated the UPDATE. Whenever a node finds that a link to a destination is no

longer valid, it adjusts its height with respect to its neighbors and transmits an UPDATE packet. Any time a node finds neighbors with no finite height with respect to destination, the node will discover a new route as described above. When a node finds out a network detachment, it generates a CLEAR packet that resets routing state and removes invalid routes from the network.

On top of TORA, IMEP (Internet MANETs Encapsulation Protocol) is layered in stack. IMEP is required to make reliable, in-order delivery of all routing control messages from a node to each of its neighbors and notification to the routing protocol whenever a link to its neighbors is created or broken. To reduce overhead, IMEP attempts to combine many TORAs and IMEPs control messages into a single packet before transmission [55]. TORAs and IMEPs control messages are referred as objects and packets are referred as object block. Each block associates with sequence number and a response list of nodes from which an ACK (acknowledge) didn't received. IMEP retransmits each block again and again after some period of time, and continues to retransmit until the link to each acknowledged node is declared down and TORA is notified. IMEP can also provide service of network layer address resolution. But this service is not used. For network layer address resolution, ARP [56] is used with all four routing protocols. Each IMEP node periodically transmits a BEACON packet for link status sensing and maintaining a list of a node's neighbors. After receiving BEACON packet, each node answers with a HELLO packet.

Ad Hoc On-Demand Distance Vector (AODV)

AODV [57] has combination of both DSR and DSDV characteristics. It uses the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR and combines hop-by-hop routing, periodic beacons and sequence numbers from DSDV [58]. AODV is an on-demand routing protocol that starts a route discovery process whenever a source node wants to communicate with destination. When a source node wants to transmit data packets to a destination node, source broadcasts a Route Request (RREQ) message to its 1-hop neighbors with the last known sequence number for that destination. These neighbors between source to destination are called intermediate nodes. After receiving RREQ message, each node rebroadcast the RREQ message to their neighbors if they do not have a fresh enough route to the destination node. This process continues until the RREQ message reaches the destination node or an intermediate node that has a fresh enough route.

Every node is associated with its own sequence number and RREQ ID. Sequence numbers in AODV guarantee that all routes are loop-free and contain the fresh routing information. RREQ ID with source IP address uniquely identifies a particular RREQ message. Only the first copy of a RREQ message is accepted by the destination node or an intermediate node. The duplicated copies of the same RREQ message will be dropped. Each intermediate node that forwards the RREQ forms a reverse path for itself back to source node. After accepting a RREQ message, the destination or intermediate node updates its reverse path to the source node through intermediate node [59]. This reverse route is used to transmit route reply message to the source node. After receiving RREQ by destination node, destination node answers with RREP (route reply) message. When the source or an intermediate node collects a RREP message, it updates its forward route to the destination node [26]. It also updates the sequence number of the destination node in its routing table to the maximum of the one in its routing table and the one in the RREP message [60]. A Route Reply Acknowledgement (RREP-ACK) message is used to acknowledge RREP message.

In order to maintain paths, each node periodically passes on a HELLO message, with a default rate of once per second [61]. If a node notices not to receive three consecutive HELLO messages from a neighbor, the node will take it as an indication of link failure or broken. This problem can be solved by using physical layer or link layer methods to detect link breakages towards neighbours that are not sending HELLO messages. In AODV, when a link breaks or goes down, any node that has recently forwarded packets to a destination using that link is notified via an UNSOLICITED ROUTE REPLY containing an infinite metric for that destination [57]. Upon receipt of such a ROUTE REPLY, a node must acquire a new route to the destination using Route Discovery as described above. Route maintenance will be done with Route Error (RERR) messages.

Whenever, if a node finds a link break during transmission, it will send out a RERR message to its neighbors. When a node receives a RERR message from its neighbor, it further broadcasts the RERR message to its neighbors. AODV is also termed as stateless protocol. During route reply, when a node to not find the next hop in the reverse routing, it will simply drop the RREP message. As above, AODV establishes route on demand only and to find latest route to the destination it uses destination sequence numbers. AODV has very low connection setup delay. The drawback of this protocol is that inconsistent routes can be present at intermediate nodes due to very old source sequence number and having a higher

but not the destination sequence number. In response to a single route request packet multiple route reply packet can have a heavy control over. Due to periodic beaconing, AODV consume unnecessary bandwidth.

In this thesis, AODV is used as the basis of concept development for protecting mobile ad hoc network. Selection of choosing AODV among the routing protocols is its characteristics. AODV does not allow extra traffic for communication with existing paths. Routing concept and calculation are very simple and don't require much memory. Connection establishment delay is very low. Therefore, because of these qualities, AODV creates attraction among researchers in doing research in the field of AODV based routing.

1.2.5 Threats and Attacks

Mobile ad hoc networks are gaining popularity in the area of research and becoming an important field of research. Applications reaching in all walks of life are making mobile ad hoc networks an attractive technology option, but characteristics of ad hoc networks like dynamic network topology, self administration introduce different security threats. Various conventional security solutions are available for wired networks and now the researchers can think of using these available solutions of wired networks for mobile ad hoc networks. Due to highly dynamic and self configuring nature of MANETs, the solutions available for wired networks are not always effective and efficient for MANETs.

Before developing effective and efficient solution for MANETs, there is a need to understand various attacks that can harm MANETs. There are various attacks that can target different layers of MANETs available and well documented in literature. These different types of threats and attacks [37] can be categorized according to target areas of MANETs. The first category is according to intensity of the attacks, such as attacker broadcasts false information or just observes social behavior to modify decision processes. In second category, the information itself is the target of attacker. In this type of attack, attacker can modify, alter and replace the message when communication is going on. In third category, the target of attacker is to misuse network resources to degrade the performance of network. The first category comes under passive attacks while the second and third categories come under active attacks.

As the research work of this thesis comes under the area of routing of packets in MANETs. Therefore, various attacks that can target routing area of wireless networks will be discussed.

Routing Loop

This attack is implemented by inserting fake routing packets to form a routing loop [62]. This will result in consuming both bandwidth and power for a number of nodes by data packets being sent. In this, the legitimate packets will not get in touch with their intended recipient. Thus, it will be considered as denial-of-service attack.

Black Hole

The arrangement for the black hole attack [63] is like the routing loop attack in which the attacker advertises shortest route between source to destination among intermediate nodes and attracts all the traffic through it. After receiving packets from neighbour nodes, black hole attacker drops all the received packets. Therefore, it is clear from discussion that black hole attacker can work like black hole in the universe.

Grey Hole

This is a special case of the black hole attack [64]. In this type of attack, attacker does not drop all packets. Rather, attacker use selective approach. In selective approach, the attacker chooses some kinds of packets to drop. For example, the attacker is dropping routing packets but not data packets.

Partitioning

In this type of attack, attacker will restrict a number of nodes of network to communicate with other nodes of network. Because of this, more than one group will be formed in a network. These groups will not able to communicate with each other even they will be in their range. Attacker can use one group to harm or to degrade the performance of network. Making of groups by attacker within the network is called as network partitioning [65]. Network partitioning can be done with the help of inserting fake routing packets or by using physical attacks such as radio jamming.

Blackmail

Many times, nodes using ad hoc routing protocols can handle security problems by making lists of probably malicious nodes. Each node keeps a list of attackers. This list is called as blacklist. The motive behind this is to restrict malicious nodes to perform any activity in the network. Now, what an attacker do for blackmailing legitimate nodes in the network? Attacker simply adds some legitimate nodes in blacklist category. Because of this, the legitimate jail nodes that have added in blacklist by attacker, will not able to perform their normal duties and to interact with neighbouring nodes [66, 67].

Wormhole

In black hole attack and grey hole attack, the attacker can perform malicious activities in the network individually. Wormhole attack is different from these attacks. Attacker launches wormhole attack with the help of making pair with other node present in the network or outside of the network. In other words, the wormhole attack can be launched using a pair of nodes over combination of two nodes connected in a way. To do so, attacker uses a special private connection or tunnel over ad hoc network. Therefore, wormhole attack [68] will work between source to destination and packets will transmit using special private connection or tunnel over the ad hoc network. By establishing this private connection or tunnel, attacker makes shorter route than actual route between source to destination. This type of attack can be launched together with network partitioning attack and tried to gain almost overall control over the network. Whenever, source node sends packets for destination node, attacker forces neighbour nodes to use the established tunnel between source to destination.

Rushing Attack

Many on demand routing protocols use duplicate suppression mechanism in route discovery process between source to destination nodes. Whenever source wants to communicate with destination node, source node starts route discovery process by sending RREQ packet to its neighbours. At this point of time, intermediate nodes keep a sequence number of RREQ packet. Whenever intermediate nodes find RREQ packet with same sequence number, they discard duplicate RREQ packets. In rushing attack [69], attacker tries to exploit this concept of duplicate suppression mechanism. Attacker inserts a great number of RREQ packets with increasing sequence numbers to find corresponding RREP packets from neighbouring nodes.

Therefore, intermediate nodes receive RREQ packets from malicious node before legitimate nodes. After receiving RREQ packet from malicious node, intermediate nodes do not accept RREQ packet from legitimate nodes. Because, intermediate nodes could not differentiate between RREQ packets sent from malicious node and legitimate node, they think that multiple RREQ packets are coming from same source and first RREQ packet will be accepted by intermediate node and second RREQ packet will be discarded because of duplication of RREQ packet. Under the rushing attack, the correct route cannot be find more than 2- hop nodes and this attack outcome will be in denial of service.

Resource Consumption

As mobile ad hoc networks have limited resources and use of these limited resources in effective and efficient manner is a challenging task in ad hoc networks. These resources may be bandwidth, memory or power. In resource consumption as attack, attacker injects false or extra data packets in ad hoc network to consume bandwidth, battery power, memory without having any reason. Injecting false or extra packets can lead to answer packets from receiver. This situation can motivate more consumption of limited resources and increase computation. Sometimes, it is seen that attacker occasionally contacts to other nodes in an ordinary way to exhaust battery power. Stajano and Anderson called this resource consumption attack “sleep deprivation torture” [66].

Dropping Routing Traffic

It is known that to take part in the routing process by all nodes is an essential characteristic in the ad hoc networks. Sometimes, it is seen that some node can show selfish behaviour. To become selfish, a node will process those routing packets that are related to it. Other packets that are not related to selfish nodes will be dropped. This is called dropping routing traffic. Because of this, the node will protect energy. This dropping of routing traffic will lead network instability or network partitioning.

Location disclosure

In location disclosure attack, attacker node will help to expose location related information of a node in a network. Attacker can also expose network topology or structure of the network. By location disclosure attack, the physical location of other adjacent nodes or neighbouring

nodes or participating nodes can be found out like whether the node is adjacent to the destination node or target node. To find out location of a node attacker can use traceroute command in UNIX like systems or with the help of time to live attribute of the routing packet. By sending ICMP error messages, attacker can find addresses of the devices. Therefore, location disclosure attack can find out exact location of intermediate nodes that come during communication between source to destination. By this, attacker can hijack first exact route during communication between source to destination afterwards overall network.
As above, there are various attacks that can harm network or degrade the performance of mobile ad hoc networks. In this thesis, the research work is taking care of wormhole attack due to seriousness of attack [70, 71].

1.3 Security Attributes

As, the demand of mobile ad hoc network is increasing day by day due to various applications in hostile or highly dynamic environments. With the passing of time, mobile ad hoc networks are gaining complexities and increasing its application areas in all walks of life. People are using mobile applications without taking care of pros and cons of it. Now a days, people have taken steps towards technology advancement, battery power advancement etc. they are enjoying in using these new technologies as they feel good in switching over new technologies. It is good to see that people are adopting new technologies easily. But it will be great if the technologies advancement come with added security. Therefore, the following security goals or attributes [66] for ad hoc networks are needed to address here:-.

- **Availability:** The facilities or services offered by the network must be available in a timely manner to legitimate nodes at all-time in spite of any disorder of the system. Resource depletion attacks aim to challenge this property. Therefore, confrontation to this attack should be of primary importance.

- **Authentication:** The identity of the sender or receiver of any message must be always verified. Therefore, the message should be generated from valid node and the message should be accepted by a valid node. There can be possibility that nonmember node can receive or send messages and legitimate node will not able to receive or send messages. This situation can occur only if network is ruled by corrupted node.

- **Integrity:** During transmission, the entity or message must not be modified. If the alteration of message has done, it should be detected and may be let down.

- **Confidentiality:** Massage to be sent is a very important component of communication system. Therefore, secret information must not be revealed to nonmembers or unauthorized nodes during transmission. It should always be tried to keep secret the existence of transmission between source and destination. There are various cryptographic tools available for countermeasure confidentiality threats. As nodes can join or leave network anytime, there is a requirement to tackle backward and forward secrecy during communication. Backward secrecy means that new nodes will not be able to access any data packet sent before their joining in the network. While forward secrecy means that left out nodes will be denied to any future communication to nodes in the network.

- **Non-repudiation:** Originator of the message cannot refuse containing sent message. With this, legitimate nodes stop attacker nodes to conceal their activities followed by isolation of attacker nodes.

In addition to these general requirements, MANETs have following specific requirements:

- **Survivability:** In The presence of power loss, failures or attacks, a minimum level of service must be provided and mission of sending message should be completed in timely manner. Therefore, in other words, even some part of network down, the services should be available as a part of essential functions.

- **Degradation of security services:** As availability of resources, there should be change in security level of network.

1.4 Secure Routing in Wireless Ad Hoc Network

Mobility characteristic allows nodes to join or leave network anytime. Mobility of nodes make packet routing a challenging task in MANETs. There are various protocols available for routing process in ad hoc network. Some protocols [72] allow proactive routing process while other protocols allow reactive routing process. DSDV and OSLR are the example of proactive routing process and AODV and DSR are the example of reactive routing process. All these protocols are not security aware and give exposure for routing attacks. No centralized administration and node's mobility make MANETs, vulnerable to various types of attacks. Routing is a network layer function. To protect network layer, there is a need of secure routing protocol for ad hoc networks. There are certain goals that a secure routing protocol should achieve. These goals are as:-

- Protocol should be able to identify malicious nodes in the network and to restrict them from taking part in routing process.
- Protocol should be able to find correct path between source and destination.
- Protocol should maintain confidentiality of network topology.
- Protocol should be firm against attacks.
- Protocol should be able to take care of security goals as discussed above.

Keeping all above points in mind, researchers proposed some security aware routing protocols [129, 130] for ad hoc networks like Authenticated Routing for Ad Hoc Networks (ARAN) [73], Secure Efficient Ad Hoc Distance Vector Routing Protocol (SEAD) [74], Security-Aware Ad Hoc Routing Protocol (SAR) [75], Secure Zone Routing Protocol (SZRP) [76, 77, 78], Secure Dynamic Source Routing (SDSR) [79], Ariadne [80], Secure Routing Information Protocol (SRIP) [81], Secure Link State Routing Protocol (SLSP) [82]. Nodes of any ad hoc network can also work as routers that find and sustain paths to target nodes in the network. To deliver message in a timely manner, a MANET routing protocol establish exact and efficient path between a pair of nodes. If routing process fails at any instant of time, the whole network will be paralysed. Therefore, in the security of any network, routing security plays an important role.

1.5 Motivation of Research

Ad Hoc networks pose unique security challenges because of their inherent limitations in communication and computing. The deployment nature of Ad Hoc networks makes them more vulnerable to various attacks. Ad Hoc networks are deployed in various applications where they have interacted physically with the surroundings, individuals and other things those make them more susceptible to security threats [83]. Researcher think that Ad Hoc networks would be deployed in operation critical applications like combat zone, security of key terrain marks, building and bridges, measuring traffic run, territory monitoring and husbandry**.** Inherent limitations of Ad Hoc networks can be categorized as node and network limitations. The privacy and security issues in Ad Hoc networks raises rich research questions.

Ad Hoc networks are typically characterized by restricted power supplies, small bandwidth, small memory sizes and restricted power [84]. This directs to a very challenging environment to provide security. Dense deployment of Ad Hoc networks in an unattended environment makes Ad Hoc nodes vulnerable to potential attacks. Attackers can capture the Ad Hoc nodes and compromise the network to admit wicked nodes as legitimate nodes. Inside the network set-up, attackers can rage variety of attacks and wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless Ad Hoc networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Therefore, complete secure Ad Hoc networks require deployment of countermeasures such as light weight encryption techniques, secure routing and secure key management [85].

The foregoing discussion formulates several questions to be answered. Some of the pertinent questions, the researcher will try to answer for, during the course of study is listed in the following section.

- How could the wormhole attack detection be modelled?
- What is the targeted part of the coverage and how can the breach paths be discovered?

- How could the fake alarms be reduced and the conclusions are progressed about destination detection with cooperation?
- What are the parameters that directly control the routing security in MANET?
- Can researcher develop an Algorithm for detecting and preventing malicious node attacks?
- Can a developed framework be really useful, noble and reliable?
- How general are the lessons learned in this study? Can they be applied in situations involving other metrics, or to organizations, which have different operational environment?

1.6 Problem Statement

Security in mobile ad hoc networks has been a burning issue and several solutions are available for various attacks. Sometimes many effective solutions for a particular attack are available and there are also some scenarios where same technique can be used to mitigate different attacks. Implementing these piecemeal solutions increase the operational overheads of MANETs which are already constrained. Development of a framework to mitigate attacks can be more effective, but it is revealed from the review of literature that no such work has been cited or no flexible framework is available to detect and prevent malicious node attacks in hostile environment. Thereby, given the need and urgency of the work, a problem has been formulated with the title, ***"A Framework to Detect and Mitigate Wormhole Attack in Mobile Wireless Ad-Hoc Network",*** to carry out the research.

1.7 Research Objective

In order to achieve the goal of working on a framework of mitigating malicious node attacks in wireless network, following objectives are set:

- To review and critically examine the literature on routing security, various malicious node attacks, different techniques for detecting malicious node in wireless environment and available strategies for preventing of damages from different attacks in wireless Ad Hoc network.

- To develop comprehensive framework for detecting malicious node in a hostile environment in terms of algorithm.
- To compare proposed strategy with existing strategies in already implemented situation.
- To implement a metric for preventing malicious node attacks in wireless environment.

1.8 Research Methodology

The proposed research work encompasses the task of establishment, development and evaluation nature. The development of reliability metric framework, reliability metric, reliability model and estimation of software reliability is a prime objective of this work. It is supposed to accomplish through several phases including following:

- List all solutions for available attacks.
- Enumerate/Select the solutions which are similar or near similar in their approach to mitigate wormhole attack.
- Investigate the possibilities of developing a framework.
- Implement that framework
- Simulate and verify the results.

1.9 Deliverables

The aim of this deliverable is to provide the overview of wireless ad hoc network including a brief history, challenges in wireless ad hoc network, routing and routing protocols, threats and attacks on ad hoc network followed by security attributes, secure routing in wireless ad hoc network. Further, the deliverables is organised as follows. Firstly, the overview of wormhole attack, including types of wormhole attack, available protocols designed to provide security against wormhole attack, then the remainder of deliverable presents in depth analysis of protocols belonging to the existing protocols pool. Protocols are presented with security enhancements in AODV. As far as the architecture, researcher decided to enhance the reference model of AODV in order to integrate in a careful way, the novel view of mitigating wormhole attack in ad hoc networks. This approach is named as SAODV. This approach is

emerging as the most suitable attempt to optimize architecture and protocols for systems with severe attacks.

In SAODV, some specific information, gathered at network layer and used to adapt the behaviour of the node depending on the particular circumstances a node operates in. These circumstances can be node selfishness, node maliciousness or network status. The concept of SAODV can be added to other routing protocols of network layer with little calculation and efforts. The SAODV protocol tries to achieve the advantages of joint collaboration of protocols belonging to different layers to detect and prevent attacks in a network. The remainder of the deliverable presents implementation of experiments with in-band wormhole attack and out-band wormhole attack.

1.10 Significance of the Work

It is observed that the contribution from this proposed study may prove to be important for the following:

- The proposed framework may minimize time and space complexities for attack prevention.
- The proposed framework may lower the cost of implementation and production of MANETs.
- The proposed framework may provide a common base for threat prevention approaches drafted by various researchers. Thus it will help researchers for future implementation.

1.11 Thesis Organization

Chapter 1 provides an introduction of Mobile Ad Hoc Networks (MANETs) that includes a brief history, challenges in wireless ad hoc network, routing in wireless ad hoc network, routing protocols in wireless ad hoc network, further, security attributes and also discuss secure routing in wireless ad hoc network. Motivation, problem statement, objectives of thesis and research methodology is also defined in this chapter.

Chapter 2 discusses the exhaustive review on specific problem of wormhole attack with types of wormhole attack in MANETs and reviews the existing approaches to mitigate wormhole attack, proposed in the literature. Researcher makes two contributions in this chapter. First is to compare existing approaches and second is to separate approaches with security enhancements in AODV.

Chapter 3 shows the major contribution by researcher in the form of SAODV to mitigate wormhole attack in ad hoc networks. The implementation of SAODV in presence of in-band wormhole attack and out-band wormhole attack is described and analyzed in Chapter 4. Conclusions with major findings are drawn in chapter 5 along with discussion of potential future work followed by references. Appendix A includes the abbreviations.

Chapter 2: Wormhole Attack in Ad Hoc Network: A Review

2.1 Background

With the innovations in wireless communication, ad hoc wireless networks are gaining popularity and providing platforms for different sorts of situations particularly where it is high-priced or infeasible to install network infrastructure. These networks are at risk by various attacks because of their open architecture. These attacks can perform miscellaneous awful activities, like packet tampering [86], identity spoofing [87], eavesdropping, rushing attack [69] and the black hole attack [76]. Muti-hop wireless ad hoc networks are limited in resources such as power, bandwidth, or processing, therefore, in comparison to wired infrastructure, it is a challenging task to implement detection and counter techniques in wireless networks.

Out of all the available attacks, wormhole attack is a severe attack in the perspective of ad hoc networks [88, 89, 90]. In this type of attack, attacker or malicious node holds packets from one position in the network, and “tunnels” all the captured packets to another attacker or malicious node at a remote point, which replays them locally. The tunnel between

one malicious node to another malicious node can be set up in various different manners like using a packet encapsulation, through an out-of-band hidden channel (e.g., a wired link), or a high powered transmission. With the help of this tunnel, packet reach the destination with lesser number of hops or sooner as compared to the packets transmitted over normal paths. This makes false impression that these two nodes of the tunnel are neighbour or nearer to each other. This wormhole tunnel can be helpful if only used for forwarding each and every packet.

However, it can be used by attackers or malicious nodes to disturb the normal operation of ad hoc network routing protocols. The two malicious points can use tunnel to pass all the packets by attracting routes through them. The wormhole attack can be set up without having knowledge of any cryptographic keys or making contact with any legitimate node in the network [88, 89]. Further, they can also start various attacks against the routing traffic flowing through the tunnel. These attacks can selectively drop the data packets. Apart from all these, it can affect location-based wireless security systems, clustering protocols and data aggregation. The malicious nodes involved in launching wormhole attack can avoid two nodes from finding out legitimate paths greater than two hops away and finally disturb network function.

2.2 Working of Wormhole Attack

As above, two malicious nodes are needed to launch wormhole attack in ad hoc network. These two malicious nodes can use private connection or high power link to establish tunnel for passing packets through them. Therefore, an opponent creates a direct link known as wormhole link between two nodes in the network. This link can be in the form of a long-range wireless transmission, a fibre optical link, or a wire line. At this point of time, other node think that the distance between origin point and destination point is one hop. Once the created wormhole link become functional, the attacker snoop all the data packets at one end, called as origin point, and forward all the received packets in timely manner through tunnel at other end, called as the destination point. To minimize delay created by wormhole, the attacker does not wait to receive entire packet, it simply forward each bit directly over the wormhole link. Due to wireless transmission, attacker can overhear data packets not addressed to it and use this wormhole link to replay these packets. If the attacker does not

perform malicious activities after establishing wormhole link, this link can be used to fast speed of communication. This attack can try to gain control all over the network because the wormhole link keeps attackers at a powerful position apart from other nodes in the network.

To create routing problems in the network, nodes form shortest paths for the actual routing in the ad hoc network. It may be possible that all data can be transferred in a selective manner to gain control over ad hoc network to a great coverage area. Further, if attacker combines this attack with a partitioning attack, it can control almost whole network traffic. In the wormhole representation, it is believed that the attacker involved in creating wormhole link, will not compromise genuineness of the communication or integrity of message. If it happens, it could do with no support from wormholes. Other drawback is that like malicious node used by routing protocol at network layer, this attack is not visible at higher layers. This attack can create havoc against many ad hoc network routing protocols in which nodes of the network attend to receive packets straight from some other node assuming that other node is neighbour of that node. For example, in on demand routing protocols such as AODV [91], DSR [51], the wormhole attack can target each RREQ packet by tunnelling all RREQ packets from originator to other end of the wormhole link.

Whenever the neighbours of the other end node of the wormhole link listens this RREQ packet they will take it as legal packet and perform normal routing procedure to forward the copy of the RREQ packet. Afterward, if the neighbours of the acceptor end of the link listens the RREQ packet, they will discard RREQ packets thinking that all these RREQs are duplicate copies from the same Route Discovery. Due to this attack, all the valid routes will be restricted other than through the wormhole link. If the attacker is closer to the originator of the Route Discovery, this attack will restrict routes more than two hops lengthy from being searched, thereby constructing a sure Denial of Service attack or selectively modifying and discarding some data packets.

In table driven routing protocols, neighbour discovery mechanism is used by broadcasting of packets in DSDV [52] OLSR [47] and TBRPF [92]. Wormhole For example, the routing protocols OLSR and TBRPF sends HELLO packets to find out neighbour in the network. If attacker A1 hears the HELLO packet from valid node N1, attacker A1 will tunnel this HELLO packet through worm hole to attacker A2 that is near to valid node N4. Because

of this attack N1 will notice N4 as neighbour even they are far away from each other. This will stop routing protocol to find paths normally.

Furthermore, the nodes between the malicious nodes A1 and A2 will never communicate to N1 and N4 till wormhole exist. The wormhole attack can also be harmful for other types of wireless networks and applications. For example, any wireless access control system based on physical proximity, such as wireless car keys, or proximity and token based access control systems for PCs [93, 94]. In all these systems, an attacker could spread the authentication exchanges to get unauthorized access.

2.3 Severity of Wormhole Attack

Wormhole attacks try to make isolated nodes trust that they are neighbour to each other by transmitting neighbour discovery packets to other part of the network. By this, malicious nodes are able to control networking systems like topology-control algorithms, control nodes and routing to send more and more traffic through them. This traffic can be used to make possible other types of attacks such as sinkhole attack [95] by dropping or recording packets. For as long a wormhole attack survive in the network, it can be a centre of attraction and gain access a lot of routing traffic in the network. This wormhole attack shows more severity as it can work without the support of MAC layer protocols and cryptographic techniques that means the malicious node does not require to know about the MAC protocol or decode encrypted packets to be capable of replay them. Further, the attacker does not need to accept the whole packet and it can be managed on bit-by-bit level [96].

If a wormhole is placed at the position where attacker can collect a large number of packets, these packets can be used in traffic analysis or encryption compromise. Wormhole attack can create problems even if other malicious nodes are normally transmitting or forwarding all packets without interruption at any level. Therefore, nodes involved in creating wormhole attack can control network's security and work unreliably whether they are involved in interrupting routing or not.

2.4 Wormhole Effects on Routing Protocols

The great effect of the wormhole attack is on the fundamental routing structure. It is seen in [97], how wormhole can create problems in routing protocols and degrade the effectiveness and stability of network performance. As before, protocols for neighbour discovery play an important role in wireless systems and for neighbour discovery and data forwarding, it is essential to perform multihop communication effectively. Therefore, from previous section, it is clear that wormhole attacks can work against the routing protocol and will try to abuse accuracy in terms of network functionalities including physical access control, topology control, energy-efficient communication, as well as network access control. There are various dangerous acts that can be performed by wormhole attack in other wireless networks. For example, periodic communication of link quality can be estimated to construct a routing tree near the base station in proactive routing protocols for wireless networks like MintRoute and MultiHopLQI [98, 99]. These types of networks use route update packets mechanism for neighbour detection. But, this neighbour detection technique is very susceptible to the wormhole attack.

Similarly, the wormhole attack can be dangerous for on demand routing protocols like DSDV [43], DSR [52, 100] and AODV [101]. In these protocols, whenever a source node wants to communicate with destination, the source node sends RREQ packets that consists sequence of intermediate nodes they passed through. Once a RREQ packet reaches the destination node then RREP packet will generate that simply follow the path from the RREQ packet and travels backwards. Therefore, to enable wormhole attack in the network, there is no requirement of compromising any node in the network. That means wormhole attack can work by staying invisible. Hence, it is clear that protecting a network of against these types of problems is a tough task to attain. But, due to nice applications of wireless networks, it becomes an important task to detect and prevent network from such types of attacks.

2.5 Types of Wormhole Attack in Ad Hoc Network

There are various methods that an attacker can use to implement wormhole attacks in wireless network environment. These methods can use encapsulation, out of band channels, packet relay or protocol deviation and high power transmission to tunnel packets deviation [102]. Therefore, the types of wormhole attack are discussed as follows: –

2.5.1 Wormhole Attack using Encapsulation

This type of attack can be launched with the help of two or more malicious node. These malicious nodes can create tunnel between them and give impression that the path through them is the shortest, but in real they are very far away from each other. To create tunnel between them they take help of normal nodes of the network using encapsulation. During transmission from source to destination through intermediate nodes of tunnel that creates wormhole, the hop count does not increase due to this encapsulation [94].

2.5.2 Wormhole Attack using High Power Transmission

In this attack, only one malicious node is required to create wormhole. That means there is no need of involving any other colluding node. Whenever malicious node hears a route request, it broadcasts this request to neighbouring nodes with high power in comparison of normal nodes. Any node that receives high power broadcast, forward route request towards the destination. With the help of this method, malicious node always tries to take a chance to be in the path set up between source and the destination [94].

2.5.3 Wormhole Attack using Out-of-Band Channel

In this attack, malicious nodes use an out-of-band high bandwidth channel to launch wormhole tunnel between the malicious nodes. This channel may be a direct wired link or a long-range directional wireless link. This type of attack can be launched with the help of specialized hardware. Therefore, this attack is very tough to establish in comparison of encapsulation attack [94].

2.5.4 Wormhole Attack using Packet Relay

In this attack, attacker tries to influence far away situated nodes that they are one hop count near to each other by relaying packets between them. This can be launched using one malicious node or more malicious nodes. If more than one malicious node is involved in establishing wormhole then this will increase number of neighbours for victim nodes to different hops [94].

2.6 Existing Approaches to Mitigate Wormhole Attack

Till date, various protocols have been offered to shield against wormhole attacks in wireless networks. These protocols can be implemented by using directional antennas, calculation of RTT between intermediate nodes, positioning systems, synchronized clocks or specialized hardware. These prerequisites and suppositions restrict their applicability in mobile ad hoc networks where the degree of joining and leaving network is comparatively very high. There are other protocols available that has been implemented by modifying well known routing protocols. They are their own requirements and assumptions that restrict their applicability in ad hoc networks. The protocols that deploy an intrusion detection system (IDS) are also available in literature to protect network from wormhole attack. These also create a lot of efforts and problems in implementation part. Therefore it is clear that in literature, three types of categories to secure network against wormhole attack are available. These categories have been decided on the basis of solutions proposed by different researchers. First is to amend a pre-existing routing protocols such as dynamic source routing [103], ad hoc On Demand distance vector [60] to avoid wormhole during route discovery [104, 105, 106, 107, 108].

The second category added extra hardware such as time synchronization mechanism, specialized hardware, positioning system, directed antenna with modification in routing protocols [102, 109, 110, 88, 111]. The third and last category is to install an intrusion detection system without or with hardware support [89, 112, 113, 114]. Present work is a novel lightweight approach called SAODV (Secure Ad Hoc On Demand Distance Vector) towards detection and prevention of wormhole attack. In this computationally exhaustive encryption and decryption technique is not used. This approach uses commonsense and exploits the concept that whenever wormhole node will receive route request, the attacker reply back with shortest route to destination. SAODV is not limited to less mobile networks but widen to highly dynamic and mobile networks. Exact argument confirms the suitability of SAODV. Correctness of this approach is added with detailed performance estimation along with an implementation on mobile ad hoc networks that reveals its effectiveness in terms of operating costs, memory requirements and processing overhead. In this section, some existing approaches against wormhole attacks in wireless ad hoc networks are reviewed.

The theory of temporal and geographical packet leashes, to sense wormhole attacks would be set up as described by researchers in [88]. They put a leash in the packet with

additional information to shield against wormholes. This approach was based on the location of nodes and synchronised clocks. The geographical leashes make sure that sender and recipient should be within definite confines. The temporal leashes make sure that all packets should have a greater bound on its lifetime to restrict the maximum travel distance. In this, all nodes keep tightly synchronised clocks and an assumption that the delays in packet sending, receiving and processing will be negligible. Both schemes, temporal and geographical, use authentication data for each packet to guard the leash that include large amount of communication and processing overhead. Mostly, researchers use a hash tree based authentication scheme that is called Merkle hash trees [115] that requires a large amount of storage. Wormhole attack detection approach that do not require any clock synchronisation offered [90] through the application of MAD (Mutual Authentication with Distance Bounding).

This can be understood with the help of example. Suppose there are two nodes i and j in the network. The node i calculates the distance of j by sending it a one bit challenge. After receiving one bit challenge from i, node j reply immediately. With the help of time of trip, node i identify that node j can be neighbour or not. The researcher use specialised hardware module to reply one bit challenge immediately without the delay forced by normal message processing with the help of temporarily taking control over the radio transceiver unit of the node. In static sensor and ad hoc wireless networks, a researcher offered an approach, called LITEWORP [102], to defend against wormhole attack. This lightweight protocol applied local monitoring of control traffic and secure two hop neighbour discovery to detect wormhole. This also offers a countermeasure that separates malicious nodes or attackers from the network. To implement LITEWORP, researchers didn't use any special type hardware like fine granularity clocks, directional antennas or time synchronisation between the nodes. During initialisation and detection of a wormhole, LITEWORP does not rely on increasing the size of packet and acquire very less bandwidth overhead.

During detection and separation of wormhole, LITEWORP minimise the chance of abusing nodes due to say alarms created by usual collisions in the wireless medium or due to malicious framing. In another approach [116], a researcher took two assumptions. First, a lot of distributed nodes are in the network and second, the distance between two node is rT, where rT represents the transmission range. To limit attackers from minimizing hop count, a packet hop count is protected using a hash chain. In this approach, distances and number of

hops between two legitimate nodes are examined. By this analytical approach, the effect of wormhole can be computed. This approach is not suitable when the malicious node plan to analyse the traffic of network and do not disturb network traffic by forwarding or dropping data packets selectively.

To protect ad hoc networks against wormhole attacks, a routing protocol called WARP is offered [117]. WARP is an enhanced form of AODV routing protocol. It adopted link disjoint multipath routing between initiator and acceptor and all neighbour's anomaly values are recorded by each node. Anomaly values means, a node figured a number of paths from different source to destination. This approach exploits great capability to take routing paths of wormhole attacks. For this, threshold value of occurrence of path between two nodes will be estimated. If the anomaly value increases from the threshold value for path between two nodes, these two nodes will be marked as a wormhole nodes and the neighbour for these wormhole nodes will be discarded.

In 2010, a scientist introduced an approach that was based on Reputation Evaluation (RSSRE) to protect ad hoc network [118]. Researchers took a hierarchical model of ad hoc network based on functions and roles of participating nodes. The correlations and behaviours of the node will build the reputation relation. Reputation evaluation is used to choose secure node in routing and this reputation can be updated through nodes relationship. The researcher also claimed that the proposed approach can be added in any routing protocol and provide routing security. Statistical analysis of multipath (SAM), based upon statistical routing analysis is offered [119]. In this approach, analysis of an assembly of multipath routes will be done at the base station. The approach prohibited doubtful paths with higher frequency for more diverse alternative pathways. The approach can be used successfully even if malicious nodes are involved in modifying route establishment messages and it can also provide expansion to multi-sink scenarios. If the application is not using multipath routing, it can have as unnecessary overheads.

Based on a modification of the split multipath routing (SMR) protocol, a scientist offered a new routing protocol [119, 120]. In this approach, multiple copies of RREQ message are allowed till the received hop counts are not greater than the hop counts of previously received copies. After receiving many copies of the RREQ message, the destination will make a list of all possible paths from the source. This information provides a

layout of the network and this layout will be used by the WIM-DSR protocol in finding out of possible wormhole nodes. In this approach, the destination node takes a path and broadcasts the information of a path towards the source. After this, one copy of a given RREQ message will be rebroadcasted. During this process, intermediate nodes can validate the information. An algorithm WRTTGDD was introduced based on calculating the RTT and geographic distance [121]. This approach has two steps first hop counting technique and second RTT between successive nodes. Every node in the network calculates the set of hop counts for its neighbour nodes.

The shortest route for each pair based on the RTTS and hop count can be estimated using Dijkstra algorithm. A local map will be reconstructed by using multidimensional scaling (MDS) and diameter feature or hop counting can be used to detect distortions in local maps. As in the normal network without wormholes, the all RTTs will be same or nearly same. But in network with wormhole, attacker will create highest value due to fake link. This approach can be helpful to detect wormhole by giving significant information about every node that are in the same range of the network. This approach claimed to detect wormhole attack but it didn't tell about how to separate attacker nodes to keep away future wormhole nodes.

An algorithm, in which, specific coefficients (CS) for its neighbour on each node can be estimated, is offered [122]. Researchers assumed that each node will maintain a list of one and two hop neighbours. A HELLO message together with its identity will be sent by each node. Whenever, a node listen the HELLO message from sender, this node will be added to neighbouring list of sender. After listening HELLO message, the reply message will be sent to sender of HELLO message.

Further, every two consecutive nodes will share neighbour list together. After sharing neighbour list, nodes will match it with own neighbour list. If at least one common neighbour is in the list then the node will be considered as a normal node otherwise it will be considered as a malicious node and will be kept in red list. The node that discovered malicious node will further broadcast back alert message to all its neighbours to drop the malicious node. From the approach it is clear that a single wormhole can be detected in classical networks. Another topological based approach to evaluate the wormhole issue is offered [123]. This approach is useful to observe unavoidable topology deviations by wormholes. This approach only took

topological information of the network and detected wormhole with the help of non-separating loops or pairs. Authors also find this approach suitable in continuous geometric domains and expand it into isolated domains.

A scientist took AODV routing protocol for analysis and offered solution called as Transmission Time based Mechanism (TTM). In TTM [114], two successive nodes are taken to calculate round trip time (RTT) throughout the path. The RTT can be estimated by subtracting the RREQ forwarding time from the RREP receiving time. Every node puts record of sending time of RREQ. Whenever, the node hears the RREQ, the node transmit messages all its neighbours and keep record of sending time. This process continues till the message arrives at target destination. Further, destination node generates RREP massage that can be received by each node that participated during route discovery. At this time, RREP receiving time has been recorded by participating node. Therefore, RTT with destination will be calculated by each node and this value will be appended as extensional part in the RREP. After receiving RREP, source node starts detecting process to confirm validity of the route by calculating RTTs between two successive nodes against the route based on RTT values in the extensional part of RREP. Whenever source node finds higher value of RTTs between successive nodes than threshold value, source node assume that it will be because of wormhole.

2.7 Comparison of Existing Approaches

As from the previous discussion it is clear that ad hoc networks have the various characteristics like insecure operating environment, lack of association, shared broadcast radio channel, absence of infrastructure, lack of central authority, resource constrains, limited resource availability, dynamically changing network topology, and lack of clear line of defence, make them vulnerable to a wide range of security attacks. Two types of attacks namely, passive and active attack is present in ad hoc networks. In passive attack the malicious node watch the data transfer in the network without modifying it whereas the active attack make an effort to modify or tear down the data being transferred in the network. These malicious activities could involve identity spoofing, message tampering, or eavesdropping. For an attacker to be able to initiate damaging activities in a network, one alternative is to control a huge number of powerful malicious nodes scattered over the network. This controlling of nodes can be done by controlling data traffic in the network. Distributed

location determination, topology discovery, routing and monitoring freshness of a node are a number of examples of control traffic. Wormhole attack is one of the severe traffic control attack that involves in controlling routing functionality of wireless networks.

As per section 2.6, it is clear that there are various approaches available to detect wormhole attack and prevent network by restricting wormholes to receive packets. Some solutions are based on altering the existing routing protocols like AODV, DSR and using extra hardware. Some approaches are modifying routing protocol without using extra hardware. Some methods are based on deployment of intrusion detection nodes or system with or without using extra hardware. Therefore, from section 2.6 it is clear that the available solutions regarding wormhole attack are divided into three categories: the first category of solutions is based on modifying the routing protocols such as AODV, DSR, and OLSR. The solutions given in [104, 105, 106, 107, 108] are the example of this category. The second category of solutions is based on modifying routing protocol without using extra hardware. The examples of this category are in [102, 109, 111, 88, 110].

The third and final category of methods is based on deployment of intrusion detection nodes or system with or without using extra hardware. The examples are in [89, 113, 114, 112]. Table2.1 shows differences of approaches with taking parameters such as extra hardware, clock synchronisation, wormhole node detection, out of band wormhole detection, or in-band wormhole detection. Furthermore, approaches in [102, 109, 111, 88, 113, 89, 110, 112] are solutions that require extra hardware facilities. Whereas, Approach discussed in [106] do not require extra hardware facilities. An approach in [106] also requires loose time synchronisation mechanism.

There are two solutions that claimed to prevent wormhole attacks, but they are not capable of identifying wormhole. These approaches are in [111, 105]. There are several methods that can defend in band wormhole attack or out of band wormhole attack. The approaches that can defend against in band wormhole attacks, but not out of band wormhole attack are in [111, 88, 107, 108, 114, 112]. The examples for out of band wormhole attacks are in [104, 105, 117, 110]. Apart from above mentioned approaches there are some other solutions available in literature.

The overall summary of all the available solutions with described parameters are given in Table2.1.

Protocol	**Based on**	**Implemented on**	**QOS Parameters**	**Extra H/W**	**Clock Synchronization**	**wormhole attack Detection**	**out of band wormhole detection**	**in-band wormhole detection**
DelPHI (Chiu and Lui, 2006) [105]	AODV	NS-2	No	No	No	No	Yes	Yes
WARP (Ming-Yang Su, 2010) [117]	AODV	NS-2	No	No	No	Yes	Yes	Yes
EDWA (Wang and Wong, 2007 [110]	AODV	NS-2	No	Yes	Yes	Yes	Yes	Yes
SAM (Song et al., 2005)[104]	DSR	NS-2	No	No	No	Yes	Yes	Yes
Lee et al. (2008) [106]	DSR	NS-2	No	No	Yes	Yes	Yes	Yes
LITEWORP (Khalil et al., 2005) [102]/ MOBIWORP (Khalil et al., 2006) [106]	DSR	NS-2	No	Yes	Yes	Yes	Yes	Yes
Secure DSR (Qazi et al. 2013 [51]	DSR	No Info	No	Yes	Yes	Yes	Yes	Yes
Naıt-Abdesselam et al. (2007)[108]	OLSR	NS-2	No	No	No	Yes	No	Yes
Su et al. (Su and Boppana, 2007) [107]	Ariadne	NS-2	No	No	No	Yes	No	Yes
TIK (Hu et al., 2006) [88]	None	NS-2	No	Yes	Yes	Yes	No	Yes
Lazos et al. (2005) [111]	None	NS-2	No	Yes	Yes	No	No	Yes

MSDN (Stoleru et al. 2012) [126]	None	purpose-built simulator	No	Yes	Yes	Yes	No	No
LDAC (Thanassis Giannetsos, Tassos Dimitriou, 2014) [125]	None	None	No	No	Yes	Yes	No	No
Gorlatova et al. (2006) [89]	OLSR	NS-2	No	Yes	No	Yes	Yes	Yes
Wang (2006) [113]	AODV	NS-2	No	Yes	N/A	Yes	Yes	Yes
TTM (Phuong et al., 2007) [114]	AODV	NS-2	No	No	No	No	No	Yes
Azer et al., 2008) [112]	AODV	NS-2	No	Yes	No	Yes	No	Yes

Table2.1: Comparison of Various Approaches of Wormhole Attacks

2.8 Approaches with Security Enhancements in AODV

As section 2.4 clears that all available solutions, against wormhole attack, can be put into three categories. First category is to enhance existing routing protocols like ad hoc on demand distance vector (Perkins et al., 2004 [57]) or dynamic source routing (Johnson et al., 2004 [100]) to keep away wormhole nodes during route discovery such as (Song et al. 2005 [104], Chiu and Lui 2006 [105], Su and Boppana 2007 [107], Naıt-Abdesselam et al. 2007 [108], Lee et al. 2008 [106]). The second category contains those solutions that needed extra hardware such as time synchronization mechanism, directed antennas or positioning system. In these approaches, modification of routing protocols is involved. The examples are (Khalil et al. 2005 [102], 2006 [109], Lazos et al. 2005 [111], Hu et al. 2004 [128], 2006 [88], Wang and Wong 2007 [110]). Finally, the third category relies on deploying an intrusion detection system (IDS) using hardware support such as (Gorlatova et al. 2006 [89], Wang, 2006 [113], Phuong et al. 2007 [114], Azer et al. 2008 [112]).

Since the proposed approach in this research has enhanced AODV protocol to make network secure against wormhole attack without using extra hardware, only those researches belonging to the first category are introduced as follows:

Song et al. (2005)[104] offered a solution that modified DSR (Johnson et al. 2004) [100] protocol to protect network against wormhole nodes by using a multipath routing method. In this approach, source node starts route discovery process and sends RREQ message. When the destination node receives copies of RREQ messages from different nodes, it will calculate the section of each link between two successive nodes in the entire paths. Further, it is known that wormhole node has high ability to take control of routing paths. If the rate of taking control on one link crosses the threshold value, the two ends of that link will be declared as wormhole nodes. The destination node starts a test data packet to check abnormality of the link. If it is validated that the link is established by wormhole nodes, destination node will convey a warning message to all the neighbours of malicious nodes, reporting them not to involve in communication with malicious nodes. By this, attackers would be separated and then restricted.

Chiu and Lui (2006) [105] offered a solution, called DelPHI, to protect network against wormhole attacks. The basis for this approach was AODV routing protocol. This approach applied a multipath approach and keeps record of delay and hop counts in broadcasting DREQ and DREP (similar to RREQ and RREP) through the routes. With this process, the average time, obtained by each hop will be estimated. If the route is controlled by wormhole attack, the value of delay will be higher than valid route with common hop count that means heavy load will be produced by wormhole nodes and the processing of packets will be slow. Therefore, the route with higher delay would not be chosen for sending data packets and wormhole nodes would be ignored.

Lee et al. (2008) [106] also gave an approach against wormhole attack to protect network. In that approach, it is mandatory to transmit messages over two hops. With this, each node maintains the record of neighbouring list of one hop and two hop counts with corresponding session keys. When a node accepted a message without having a valid Message Authentication Code (MAC), then it is assumed that this can be because of wormhole attacks. The aim of keeping record of two hops neighbouring list by each node is to permit the node to identify hidden wormhole attack or exposed wormhole attack. The

wormhole node can act as host wormhole attack, while later it will be hidden (Lee et al., 2008) [106].

Su and Boppana (2007) [107] proposed a protocol to lessen the effect of wormhole attacks. This protocol was an enhanced version of the Ariadne (Hu et al., 2002) [80] routing protocol. This approach can only be meant for defending against in-band wormhole attack. This approach is used to find out the value of average time in broadcasting RREQ through valid node. So that a malicious nodes, that involve for in-band wormhole attacks, can be separated because of high interval in transmitting RREQ from valid node. Naıt-Abdesselam et al. (2007) [108] proposed a solution to protect a network against wormhole attack by enhancing optimised link state protocol (OLSR) (Clausen and Jacquet, 2003) [127]. This approach used four message exchanges. For creating high delays, wormhole node would be involved in processing of large number of packets. To confirm the delay, the authors used Hello and ACK messages.

Another approach offered by Ming-Yang Su (2010) [117] that is based on AODV (Ad hoc On-demand Distance Vector) routing protocol. That is called as (Wormhole-Avoidance Routing Protocol). In this approach, link-disjoint multipath would be considered for route discovery and given path selections to ignore malicious nodes but finally, nodes exercised only one route to send data. A novel lightweight countermeasure to protect network against wormhole attack presented by Thanassis Giannetsos, Tassos Dimitriou, (2014) [125]. This approach named LDAC (Localized-Decentralized Algorithm for Countering wormholes). This approach used connectivity information as given by underlying communication graph for making sure that no attack is working. This approach is totally localized and looked for simple evidence.

LDAC is open for highly dynamic and mobile network that means this approach is not only has application for static networks. Qazi et al. (2013) [51] offered a solution that can detect attacks and identify malicious nodes on the basis of statistical analysis of multipath, called as, SAM. The malicious nodes with different topologies and with different transmission range can be successfully detected by this approach. Further, SAM can enhance its capability by acting as a module of local detection agents in an intrusion detection system (IDS) for ad hoc networks. Stoleru et al. (2012) [126] presented a solution named Mobile Secure Neighbor Discovery (MSND). This approach works on evaluation of detection of

wormhole attack in network. This approach allows contributing nodes to determine neighbouring nodes securely and use wormhole localisation protocol for determining location of wormhole.

2.9 Conclusion

In this chapter, a review on wormhole attack is done. The review included the working of wormhole attacks in ad hoc network and impact of well-known attack in wireless ad hoc network followed by types of wormhole attacks. After that, the chapter explored all available solutions against wormhole attack in wireless ad hoc network. The researcher came to know that all solutions can be categorized in three sections. First section explored all solutions that are implemented after the modification of routing protocols such as DSR, AODV. The second section examined about solutions that are supported by extra hardware with or without enhancement in routing protocols. The third section gave place to those solutions that are based on intrusion detection systems (IDS). Furthermore, all solutions are tabulated and compared with proposed approach in this research. It is also said that the proposed solution comes under first category and it used AODV as enhancement. The proposed solution works without the support of extra hardware and it takes care about quality of service parameters with no clock synchronization.

Chapter 3: Proposed Methodology

3.1 Background

Ad hoc On-Demand Distance Vector (AODV) Routing is a popular routing protocol used in mobile ad hoc networks (MANETs) and other wireless ad hoc networks. It was the joint venture of Nokia Research Center, University of California, Santa Barbara and University of Cincinnati by C. Perkins, E. Belding-Royer and S. Das [57]. The Ad-Hoc On-Demand Distance Vector routing protocol is also available in RFC 3561[60]. The concept of AODV, like all other reactive protocols, is based on topology information that is only transmitted by nodes on-demand. Whenever, a node wants to send traffic to a destination, to which there is no path, it will firstly send RREQ message to its entire neighbours. This process continues till RREQ reaches to destination node. Therefore, to initiate such communication, an initial delay occurs. When RREQ message gets in touch with the destination, or, an intermediate node makes a valid route entry towards the destination, a path will be established. For as long as this path remains active between two nodes, AODV stays in passive mode. Whenever the path is broken or lost, again RREQ message will issue with the use of AODV protocol. During establishment and maintenance of an ad hoc network, the Ad Hoc On-Demand

Distance Vector (AODV) protocol permits self starting, dynamic, multihop routing between participating mobile nodes [131].

AODV lets mobile nodes to establish path rapidly for fresh destination and do not allow nodes to keep routes to destinations that are not in use. As in [60, 132], AODV routing protocol comes under reactive routing protocol category, therefore routes can be established only when required. To discover and observe paths to neighbours, a node sends hello messages and afterwards each node broadcasts a hello message periodically to all its neighbours. If a node does not receive hello messages from a neighbour two or more times, a link will be declared broken. After receiving RREQ message, each intermediate node creates a route to the source. If the RREQ message is received by destination node, it sends RREP message in unicast manner using hop by hop fashion towards the source. After receiving a RREP message, each intermediate node creates a route to the destination. When RREP message is received by the source node, it maintains the route to the destination and start sending data. If more than one RREP messages are received by the source, the path with the shortest hop count will be chosen. Wormhole attacker takes the benefit of this concept and creates a wormhole link with the help of two malicious nodes or legitimate nodes nearer to source and destination nodes.

3.2 AODV Routing Attacks

AODV gives lots of chances to attackers. There are a number of misuse objectives that an inside attacker may desire to attain [59].

3.2.1 Misuse Goals

The misuse goals can be one or more of the following:

Route Disruption: In this, attacker involves in trying to break down an existing link or stopping a new path from being set up. The aim is to target only route between two endpoints.

Route Invasion: In this, an insider attack includes himself as a part of a route between source and destination points of communication channel.

Node Isolation: In this, an attacker separates a particular node from network and prevent node to participate in communication process with other nodes in the network. The aim is to target all possible routes.

Resource Consumption: In this, an attacker tries to consume available bandwidth in the network and storage space available at every node to disrupt transmission process. For example, an inside attacker may consume the network bandwidth by flooding bogus messages in the network.

Denial of Service: In this, an attacker tries to stop legitimate nodes to utilize part of network or whole network connection. Denial of service can be broadened itself to all layers of protocol stack. They can attack on legitimate users' access to a service provider or service availability [133].

3.2.2 Attacks

To achieve these goals that are described in previous section, the following misuse actions or attacks may be performed:

Packet Dropping Attack

In a packet dropping attack, the received routing messages are simply dropped by the attacker. This can be detected by monitoring whether a neighbor node is broadcasting packets towards final destination or not. To enable the monitoring of neighbour nodes, it is required to keep neighbor table. This attack is available in different forms. Various subcategories are as follows:

If an attacker wants to apply packet dropping attack [134] on the RREQ messages it receives, RREQ messages can also be selectively dropped by an inside attacker. Such types of misuses by attackers are similar in nature to the selfish nodes. If an attacker concerns on

applying this attack on RREP messages, it can be the case of route disruption. This attack can also apply on other data packet and will prevent affected node from taking data packets from neighbouring nodes for a small period of time. After receiving RREQ message, an attacker can make modifications like to increase RREQ ID, to change the destination IP address with other IP address, to add the source sequence number by one, to put non-existent IP address in place of source IP address. After doing this, fake message can be forwarded by an attacker.

When all neighbours of an attacker get the fake RREQ message, they modify the next hop of the source node to the non-existent node because faked RREQ message have a larger source sequence number. Because of non-existent destination IP address, the fake message will travel to the extreme nodes in the ad hoc network. Whenever any node requires sending data packets towards the source node, they will follow route created using the fake RREQ message. Due to non-existent node, data packets may be dropped. With the help of local repair mechanisms in the AODV protocol, this attack cannot totally separate the victim node. Whenever a node observes unsuccessful delivery of data packets, nodes will again start route discovery process.

Sequence Number Attack

The freshness of route coupled with a node will be indicated by using sequence number. If an attacker transmits an AODV control packet with a large sequence number of the compromised node, the route will be directed towards compromised node. The sequence number may be reduced to restrain updating in the table or increased to renew other nodes' reverse route tables. This attack can also be apply on both either Source Sequence Number or the Destination Sequence Number. A RREQ message can be uniquely identified by RREQ ID along with the source IP address. The combination of this shows the freshness of a RREQ message. At any time, a node only considers the first copy of a RREQ message. If another node accepts the increased RREQ ID along with source IP address, that means node will accept faked RREQ message. Sequence number attack can only consider sequence number field, available in RREQ message [135].

Field Modification Attack

As it is known that data packet will be sent with the header. In layering process, data packets go through different layers and add headers accordingly. The field modification attack [129, 136] is responsible for changing the field values in header at network layer. As above, sequence number attack is modifying sequence number field therefore it can be said that sequence number attack is a part of field modification attack. The other fields that an attacker can modify are highlighted below. The table given below will show impact of changed field during normal routing process.

RREQ Message Field	**Modifications**
RREQ ID	To make faked RREQ message acceptable or unacceptable, attacker increases or decrease RREQ ID.
Type	Message type will be changed.
Hop Count	To invalidate the update, hop count will be decreased or increased to update other nodes' reverse routing tables.
Destination IP Address	Replace with another IP address
Source IP Address	Replace with another IP address to change the reverse route

Table3.1: Field Modification Attack on RREQ Message Field

When several fields have been modified by attacker, it shows immediate security repercussions in the network. For ensuring loop freedom in AODV, a node after receiving RREQ message modifies its reverse routing table. This modification occurs only if source sequence number is greater than the value in its routing table or source sequence number is equal but hop count value is smaller than that in the routing table for RREQ message. To affect other node's routing table, an inside attacker can also involve in changing these fields. Same procedure will be used for a RREP message. In this, if the destination sequence number in RREP message is greater than the value one in its routing table or destination sequence number is the same but the hop count plus one is smaller than the value in routing table, a source node or an intermediate node modifies its forward routing table. Now take attacker point of view, if the destination sequence number in the RREP message is greater than the one in its routing table, or the destination sequence numbers are the same, but the hop count in the RREP message plus one is smaller than the one in its routing table, the attacker can contain the legitimate RREP message by increasing the destination sequence number.

Field Addition Attack

In this attack, an attacker can build a RREQ message without receiving an RREQ message. For launching this attack, there is a need to collect some basic information to build faked RREQ messages (e.g., by listening to the traffic). In theory, to cause disruption in routing process, the attacker may add any field in a RREQ message [59, 138].

3.3 AODV Algorithm

In this section, AODV algorithm is presented in brief. The ad hoc on demand distance vector (AODV) routing algorithm [57, 60] is an on demand algorithm, intended for ad hoc mobile networks. It is suitable for both multicast and unicast routing. Here on demand means that it helps in building routes when source node wants to communicate with destination node or target node. These routes will be maintained so long as they are required by the source. To guarantee the freshness of route, the sequence number is used by AODV. With the help of route request/route reply cycle, AODV builds routes. Whenever a source node wants to communicate with destination node for which no route is existed, it broadcasts a route request packet to all its neighbours. This process continues till route request packet reaches up to destination node. After receiving route request packet, each node updates information for the source node and establishes backward routes to the source node in the route tables.

RREQ packet contains source node's IP address, current sequence number, broadcast ID and most recent sequence number for the destination of which the initiator is aware. After receiving RREQ packet, a node can send the route reply (RREP) packet only if it has either a route to the destination with corresponding sequence number equal to or greater than that contained in the RREQ or it is the destination node. At this point of time, RREP packet will be unicasted back to the source. If any time error in transmission occurs, the RREQ packet will be rebroadcasted. Each node maintains track of the broadcast ID and RREQ's source IP address. If any time nodes receive already processed RREQ packet, they reject the RREQ and never forward it. Now, the RREP spreads back to the source and nodes will establish forward pointers to the destination. After receiving a RREP packet by source node, source node will start to send data packets to the destination. After this, if any point of time the source node collects a RREP containing the same sequence number with smaller hop count or a greater sequence number, it will update its routing table or the destination and start with the better

route. The route will be maintained as long as there are data packets to send from source to destination.

If there are no data packets to send, the established route will be timed out and deleted from routing tables of intermediate nodes. If route break takes place during transmission of data packet, the node will propagate route error (RERR) packet to the source node to inform about unreachable destination. After receiving the RERR, source node can reinitiate route discovery process if there is any packet to send. This is the scenario for unicast route. Multicast routes can also be established in a similar manner. These similar rules can be applied for establishing multicast routes. Whenever, a node wants to connect a multicast group, it broadcasts a RREQ with a destination IP address with appropriate field setting Multicast and flag setting 'J' to indicate that it wants to join the group. Any node, which is the member of the multicast group and has a sufficient sequence number, sends a RREP packet. As the RREP packet circulates back to the originator node, the intermediate nodes update pointers in their multicast route table. After receiving the RREPs, the source node keeps follow of the route with the newest sequence number and minimum hop count to the next multicast group member. Now, the source node unicasts a MACT (Multicast Activation) message [139] to all selected next hop. This massage is sent to activate the route between nodes.

If the intermediate nodes, which are part of the multicast group, do not obtain the MACT message within required time, they remove pointer from their routing table. If nodes which are not part of the multicast group receive MACT message, they will also keep track of the RREPs message and unicast MACT to its entire next hops. This process continues till message will reach to a node member of the multicast tree. AODV retains routes till the route is active. This is requires to maintains multicast tree for the life of the multicast group as the nodes in the network are mobile and during the lifetime of that route, many link breakage can occur.

Therefore, the section is going to tell about the steps involved in AODV routing algorithm below:-

- Path Discovery
  - Forward Path Setup

- Reverse Path Setup

- Route Table Management
- Path Maintenance
- Local Connectivity Management

3.3.1 Path Discovery

- Done When No Information on Some Node to Which Communication Is Requested
- Each Node Has Two Counters
  - Node sequence number
  - Broadcast ID
- Path Discovery Process
  - Source Node broadcasts a Route Request (RREQ) Packet to its neighbors
  - Neighbors forward the Request to their neighbors, and so on until either the Destination or an Intermediate Node with a "Fresh Enough" Route to the Destination is located
  - broadcast_id is incremented for new RREQ
  - RREQ from same Node with same broadcast_id will not be broadcasted more than once
  - RREQ generates Backward Path to Source
  - RREP generates Forward Path to Destination

3.3.2 Route Table Management

- Route Request Expiration Timer
  - Cleans Reverse Paths that do not lie on Active Route
- active_route_timeout
  - Is used to determine if Neighboring Node is Active i.e. Sends at least one packet in this time
- Route Cache Timer
  - Cleans Inactive Routes
- Each Route Table Entry Contains
  - Destination
  - Next Hop

- Number of Hops
- Sequence Number for the Destination
- Active Neighbors for This Route
- Expiration/Termination Time for the Route Table Entry

- When a Route Entry is used to transmit data from Source to Destination, Timeout for each entry is reset to Current Time + active_route_timeout
- When a new Route is available, Route Table will be updated only if new route has
  - Larger dest_sequence_#

    Or
  - identical dest_sequence_# but with lesser hop_cnt to the Destination

3.3.3 Path Maintenance

- If Source Node travels during an Active Session
  - It can redo Path Discovery
- If Destination or Intermediate Nodes travel
  - A particular RREP is sent to affected Source Node
  - On link breakage, affected node propagates an unsolicited RREP < dest_sequence_#+1, ∞> to all active neighbors
  - Source may resurrect Route Discovery procedure

3.3.4 Local Connectivity Management

- Two Approaches for a node to find its neighbors
  - Receiving transmit from its neighbors
  - Send its neighbors Hello Messages having its Identity and Sequence Number
    - Sequence number is not changed for hello message
    - Nodes cannot rebroadcast hello messages (TTL=1)
- Local Connectivity is changed if
  - getting a Hello or a Broadcast from a New Node
  - Failing to Receive allowed_hello_loss Consecutive Hello Message from a Node previously in the neighborhood
- Neighbors only communicate when heard each other's Hello Message
  - It ensures the Link is Bidirectional

3.4 AODV Working

Full form of AODV is Ad hoc On Demand Distance Vector routing. It is network layer protocol. This protocol comes under the category of on demand routing protocols. This protocol can be used even there is no paths available between sender and receiver. The working of AODV is very simple. Because of its simplicity, this protocol is very popular and many researches are going on. Various modified versions of AODV [91] are available in literature. To understand these modified versions, it is necessary to know the working of basic AODV.

Therefore to understand the working of AODV, an example is presented. In AODV [60], when a source node A wants to send data for a destination node B, node A firstly find out the availability of route in its cache table. If there is no route between node A and B, A will transmit a RREQ message through all its neighbour nodes and intermediate nodes for B. whenever any node between A to B receive RREQ message, the intermediate nodes will rebroadcast the RREQ messages. This process will continue till RREQ reaches destination node B. During the process every intermediate node checks if it is not the destination node, whether there is a cached route to B, whether first time they are receiving RREQ, and the value for TTL field is not equal to zero. Each node will also record the uniqueness of the one-hop neighbours that will further broadcast the RREQ. Once the RREQ message reaches the destination node B, B replies with a RREP message. Node A send RREQ in broadcast manner while replying with RREP is a unicast manner.

Therefore, RREP message is unicasted to the one-hop neighbour of node B that has forwarded the RREQ first. In the similar manner, the RREP will be unicasted back to the source node A, using the recorded one-hop neighbours that originated the RREQ. In the AODV route finding process, the path nodes do not fully aware of the path from the source to the destination, including the source and the destination node. Because the review module requires knowledge of personal security domain, the path can become be familiar with after it established, as an auxiliary service. An example of the route discovery process outlined in algorithm in section 3.3 is shown below –

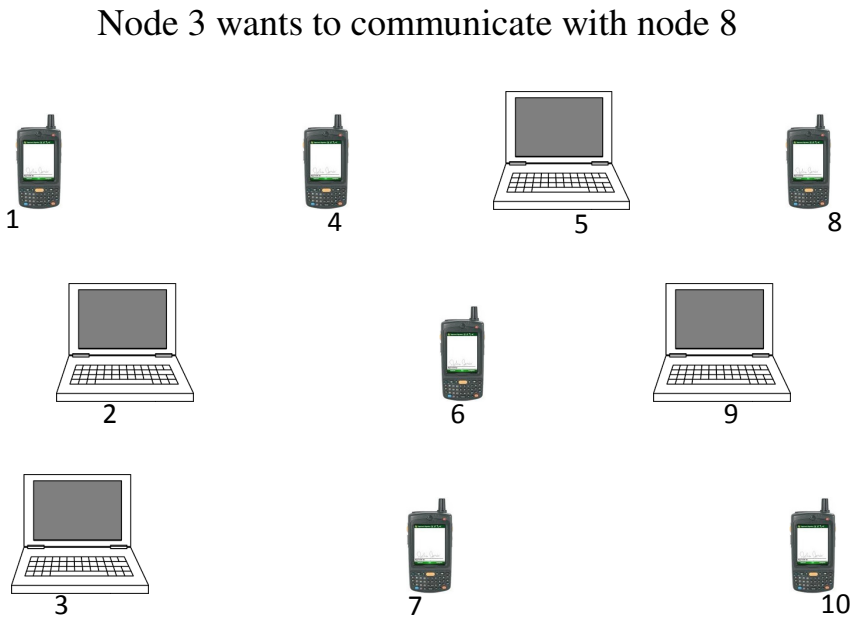

Figure3.1: Example of AODV in a MANET

In the figure 3.1 it is clear that there are ten mobile nodes in a network. Now, node 3 wants to transmit data packets to node 8 with the use of AODV routing protocol. Now, Node 3 will check the availability of route in its cache table. If there is no route between node 3 and 8, node 3 will transmit a RREQ message through all its neighbour nodes and intermediate nodes for node 8.

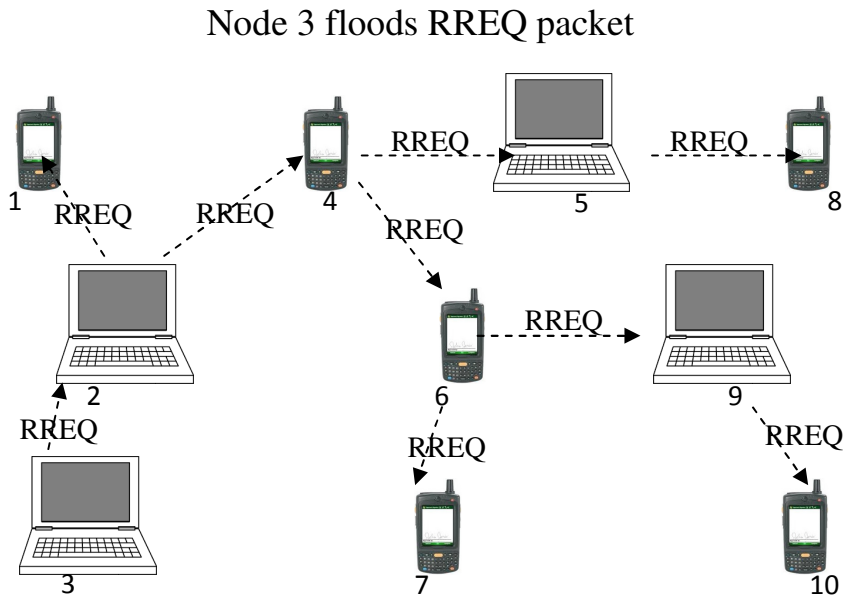

Figure3.2: Example of AODV in a MANET – Route Request

In the figure 3.2, node 3 is broadcasting the RREQ message to its one hop neighbours. After receiving RREQ messages, neighbours will also further forward RREQ message. This process continues till RREQ will reach to destination node. Sending RREQ message is a broadcast process.

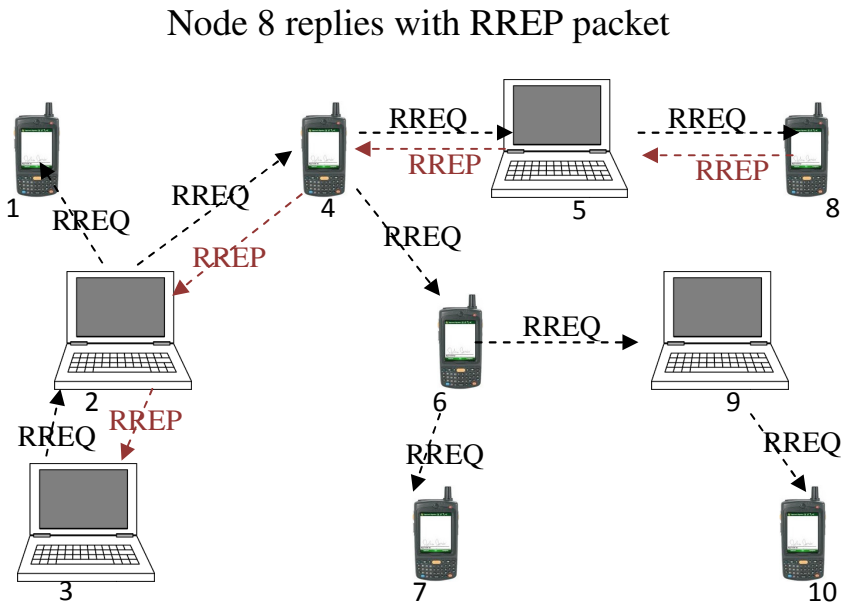

Figure3.3: Example of AODV in a MANET – Route Reply

In the figure 3.3, after receiving RREQ by destination node 8, node 8 will send back reply with RREP message to the source node 3. As before, this source node sends RREQ message in broadcast manner while RREP message will be sent in unicast manner. Therefore, node 8 is replying back with RREP in unicast manner to node 3.

During communication between source node and the destination node, three types of control messages can be sent. These messages are given below:-

- RREQ - A route request message (Source node initiate communication by sending RREQ message)
- RREP - A route reply message (after receiving RREQ, destination node reply back RREP message)
- RERR - A route error message (it is generated when any fault occurs during transmission)

AODV uses the following fields with each route table entry in the AODV Routing Table**:**

- Routing table of each node maintains
  - Next-Hop (Node Pointer)
  - Sequence number (Integer)
  - Hop Count (Integer)
- Values updated on receipt of RREQ, RREP, or RRER
- Partial order constraint.
  - Seq(A) < Seq(B) or
  - Seq(A) = Seq(B) ^ HopCount(A) > HopCount(B)
    - Intermediate node (B) either has a newer route to endpoint than the start node, or it has a shorter route that is equally recent.
- Destination IP Address
- Other state and routing flags (e.g., valid, invalid, repairable, being repaired)
- Network Interface
- List of Precursors
- Lifetime : Expiration or deletion time of the route
- Active neighbor list : Neighbour nodes that are actively using this route entry
- Request buffer : Makes sure that a request is only processed once

3.5 Secure AODV (SAODV): Design Enhancement in AODV

The secure AODV is the extended version of AODV. The objective of SAODV is to provide secure environment during transmission between source to destination. As AODV is mostly used because of its speed of transmission but it does not provide security during transmission. Therefore, there is a need of secure environment to send data packets between two nodes. Researcher is presenting a protocol with adding security feature. This is called 'Secure AODV'.

3.5.1 Packet Format

In AODV, there are four types of packet formats available in literature [60]. Those are Route Request (RREQ) Message Format, Route Reply (RREP) Message Format, Route Error

(RERR) Message Format and Route Reply Acknowledgement (RREP-ACK) Message Format. Researcher is not going to elaborate on all types of packet format except Route Request (RREQ) Message Format as it is modified to detect and prevent wormhole attack during transmission process. In AODV, RREQ message format is used when sender node wants to establish the path with destination node.

In response to RREQ, destination node use RREP message format to reply sender's RREQ. Apart from these two formats RREQ and RREP, RERR is used when any time link break occurs during transmission. At this time, the destination node becomes unreachable from one or more of the node's neighbors. The Route Reply Acknowledgment (RREP-ACK) message format is used in reaction to a RREP message with the 'A' bit set. This is done whenever there is risk of unidirectional links preventing the completion of Route Discovery Cycle. For SAODV, the modified RREQ message format is given below. In the modified RREQ message format, all fields are same except Destination IP Address and Destination Sequence Number. In place of destination IP address, researcher is using address for false node that means address of nonexistent node in the network.

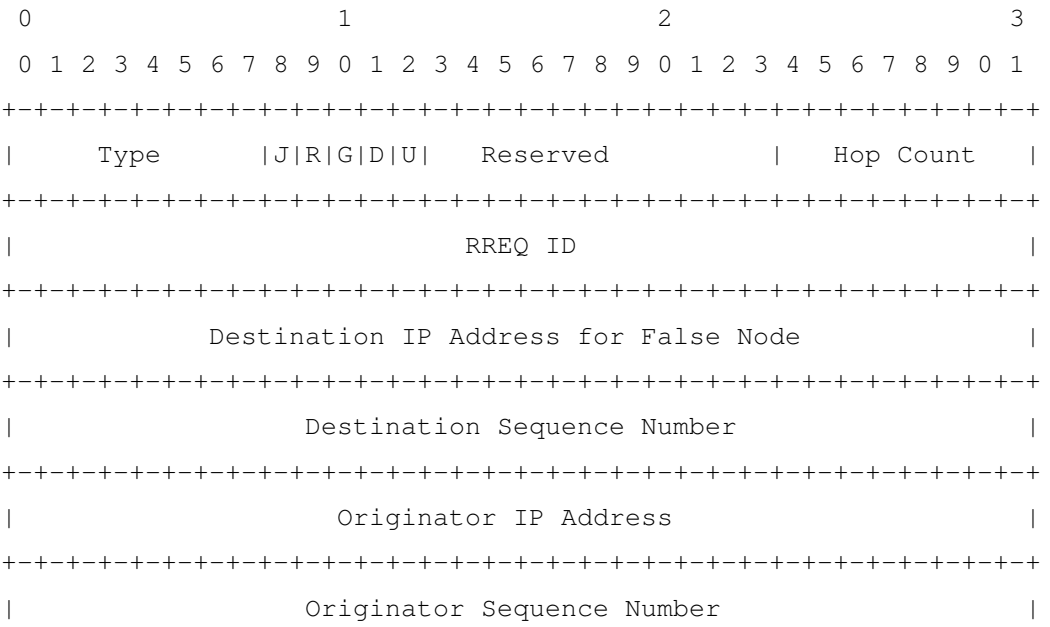

Figure3.4: Modified Route Request (RREQ) Message Format

The format of the Modified Route Request message is illustrated in figure3.4, and contains the following fields:

Type	1
J	Join flag; reserved for multicast.

R	Repair flag; reserved for multicast.
G	Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address field.
D	Destination only flag; indicates only the destination may respond to this RREQ.
U	Unknown sequence number; indicates the destination sequence number is unknown.
Reserved	Sent as 0; ignored on reception.
Hop Count	The number of hops from the Originator IP Address to the node handling the request.
RREQ ID	A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address.
Destination IP Address for false node	The IP address of the false destination node for which a route is desired.
Destination Sequence Number	The latest sequence number received in the past by the originator for any route towards the false destination.
Originator IP Address	The IP address of the node which originated the Route Request.
Originator Sequence Number	The current sequence number to be used in the route entry pointing towards the originator of the route request.

3.5.2 Algorithm

In this section, the algorithm of SAODV is given. Steps are as under:-

Secure-AODV (SAODV) Protocol

Notations Used:

SN : Source Node

DN : Destination Node

IN : Intermediate Node

FN : False Node

RREQ : Route Request

RREP : Route Reply

Functions Used:

initiateRREQ()	:	Source node Initiates route establishment process by sending initiateRREQ().
acceptRREQ()	:	intermediate node receiving acceptRREQ for destination node.
createRouteEntry()	:	nods create or update the route entry in the routing table
validateRREQ()	:	check if node knows the route to FN
promoteRREQ()	:	Forwarding RREQ for FN
initiateRREP(DN)	:	Generating RREP by DN
promoteRREP(DN)	:	Forwarding RREP from DN
acceptRREP(DN)	:	Receiving RREP from DN
includeBlackListTable(DN)	:	Insert DN into BlackListTable
confirmBlackListTable(DN)	:	Check Values of DN in BlackListTable
hinderRoute(DN)	:	Disable Route for DN

Tables Used:

RoutingTable	:	Stores route entry for valid routes
BlackListTable	:	Stores entry of black-listed (Wormhole) nodes

Functions Description:

- Source Node SN:

a. initiateRREQ(FN)

Step 1. CHECK IF no route exists

Step 2. THEN

Step 3. check request buffer for requests already sent for destination

Step 4. CHECK IF no request sent already

Step 5. THEN

Step 6. create a RREQ packet

Step 7. add values of destination address, broadcast ID to request buffer

Step 8. locally broadcast RREQ

Step 9. set timer for RREP_WAIT_TIME before rebroadcasting RREQ

Step 10. increment broadcast ID

Step 11. ELSE

Step 12. buffer packet from stream or discard, according to need

- Intermediate Node IN:

a. acceptRREQ (FN)

Step 1. CHECK IF source address, broadcast ID exists in request buffer

Step 2. THEN

Step 3. discard request -- already heard and processed

Step 4. ELSE

Step 5. add source address, broadcast ID to request buffer

Step 6. Call createRouteEntry(FN)

b. createRouteEntry(FN)

Step 1. CHECK IF no route to source address exists in RoutingTable

Step 2. THEN

Step 3. create a route entry in RoutingTable for source address

Step 4. ELSE CHECK IF source seqno in RREQ > source seqno in RoutingTable

Step 5. THEN

Step 6. update route entry in RoutingTable for source address

Step 7. ELSE CHECK IF source seqno in RREQ = source seqno in RoutingTable AND hop count in RREQ < hop count in RoutingTable

Step 8. THEN

Step 9. update route entry in RoutingTable for source address

Step 10. Call promoteRREQ(FN)

c. validateRREQ(FN)

Step 1. CHECK IF current node is destination of RREQ

Step 2. THEN

Step 3. create a RREP packet

Step 4. unicast RREP to source of request

Step 5. ELSE CHECK IF exists route to destination AND destination seqno in RoutingTable >= destination seqno in RREQ

Step 6. THEN

Step 7. create a RREP packet

Step 8. unicast RREP to source of request

Step 9. ELSE

Step 10. Call promoteRREQ

d. promoteRREQ (FN)

Step 1. CHECK IF current node is destination of RREQ

Step 2. THEN

Step 3. create a RREQ packet

Step 4. copy all fields from received RREQ into new packet

Step 5. increment hop count field

Step 6. locally broadcast new RREQ packet

Step 7. discard received RREQ

- Destination (Worm holeNode) DN:

a. initiateRREP(DN)

Step 1. create a RREP packet

Step 2. unicast RREP to source of request

- Intermediate Node IN:

a. promoteRREP (DN)

Step 1. CHECK IF route to requested destination does not exist

Step 2. THEN

Step 3. create a route entry in RoutingTable for requested destination

Step 4. ELSE CHECK IF destination seqno in RREP > destination seqno in RoutingTable

Step 5. THEN

Step 6. update route entry in RoutingTable for requested destination

Step 7. ELSE CHECK IF destination seqno in RREP = destination seqno in RoutingTable

AND

hop count in RREP < hop count in RoutingTable entry

Step 8. THEN

Step 9. update route entry for requested destination

Step 10. CHECK IF route to requesting source exists

Step 11. THEN

Step 12. Call promoteRREP (requesting source)

- Source Node SN:

a. acceptRREP (DN)

Step 1. CHECK IF route to destination does not exist
Step 2. THEN
Step 3. create a route entry for destination
Step 4. ELSE CHECK IF destination seqno in RREP > destination seqno in RoutingTable
Step 5. THEN
Step 6. Call BlackListTable(DN)
Step 7. ELSE CHECK IF destination seqno in RREP = destination seqno in RoutingTable AND hop count in RREP < hop count in entry
Step 8. THEN
Step 9. Call BlackListTable(DN)
Step 10. ELSE
Step 11. discard RREP

b. includeBlackListTable (DN)

Step 1. find insertion point in BlackListTable
Step 2. CHECK IF entry is already there in the precursors list
Step 3. THEN
Step 4. don't need to add another
Step 5. ELSE
Step 6. increment size of blacklistTable
Step 7. allocate memory for newNode
Step 8. assign address of Nn to newNode
Step 9. insert newNode in blacklistTable

- Intermediate Node IN:

a. confirmBlackListTable (DN)

Step 1. search for destination address in blackListTable
Step 2. CHECK IF current address = destination address
Step 3. THEN
Step 4. Call hinderRoute (DN)
Step 5. return TRUE

Step 6. ELSE

Step 7. return FALSE

b. hinderRoute (DN)

Step 1. set destination to DN

Step 2. empty the precursors table for the route

Step 3. set last hop count to hop count

Step 4. set destination hopCount to INFINITY

Step 5. set destination activated to FALSE

Step 6. set destination lifetime to DELETE_PERIOD

Step 7. increment destination sequence number

Step 8. check and set routeExpireHead and routeExpireTail to correct position

Therefore, the above given algorithm is suitable for detecting wormhole nodes present in the data transmission process.

3.6 Working of SAODV

The full form of SAODV is Secure Ad hoc On Demand Distance Vector. It is the extension of already available routing protocol AODV. It is based on the algorithm given in section 3.5.2. The aim of this protocol is to detect and prevent wormhole attack during transmission between sender and destination nodes. Whenever, sender wants to communicate with any node in the network, it will firstly send the Modified RREQ message that contains the IP address of the false node, which is not present in the network, to the all its neighbors.

All neighbors checks whether they are destination nodes or not. If they are not destination node, they forward this modified RREQ message to all its neighbors. If suppose there is a wormhole tunnel during communication then the nodes creating tunnel will reply that they have path towards the destination node. By this they will be trapped and prevented to send packets in future. This can also be understood by the figure3.5 given below:-

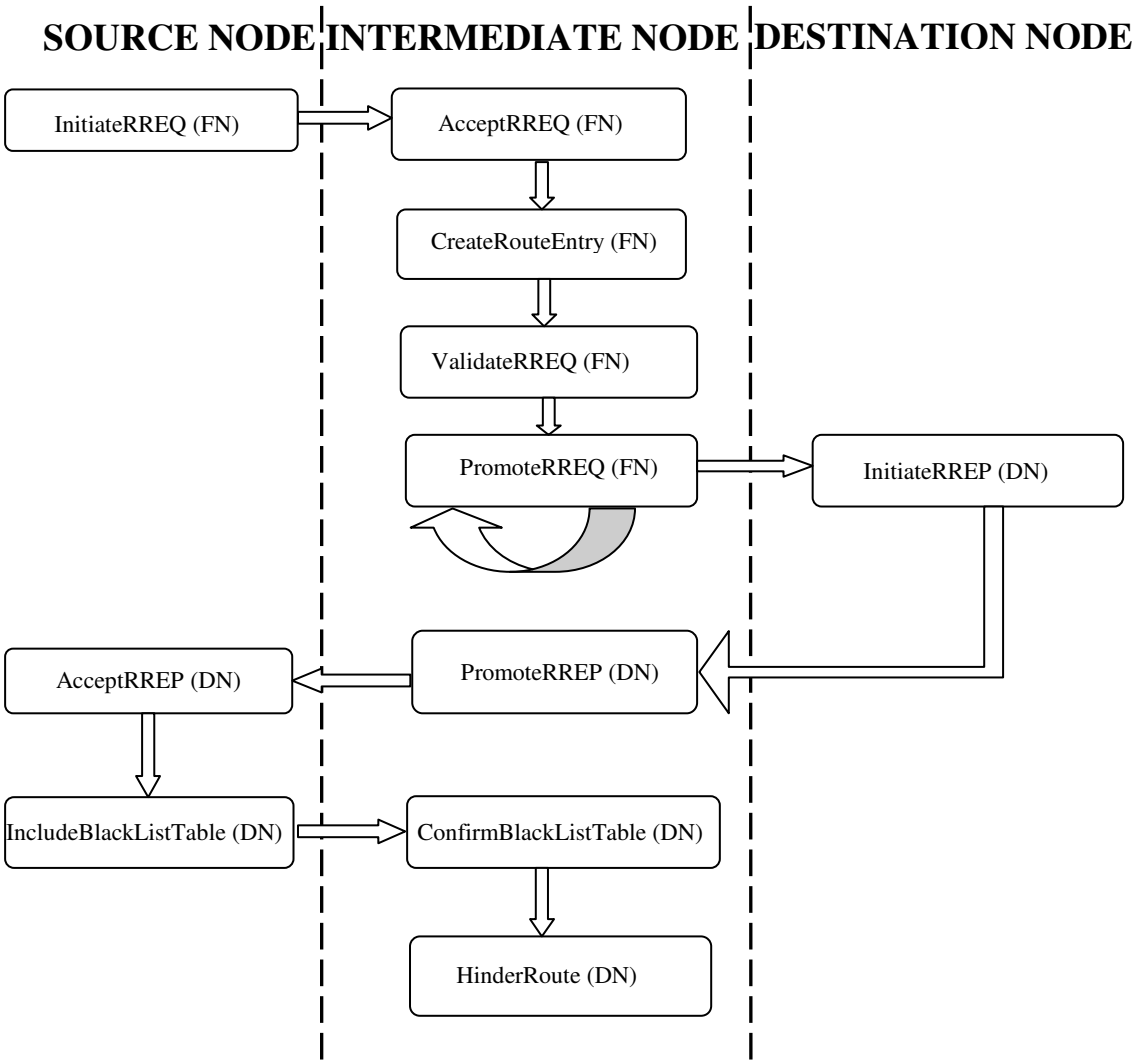

Figure3.5: Flow Chart showing Working of SAODV

In this protocol, Security is considered in two parts. Firstly, when communication takes place within the network which is called local communication. Secondly, when two nodes, that belongs to different networks are communicating. This is called as inter network communication. When local communication is continuing, at that time source node broadcast the RREQ packet which contains the IP address of false node. Now the message will be received by the direct neighbours. They check their entries in the table if they are not wormhole node than they will forward message to the next neighbour. If the malicious node present in the network it will give immediate response to the source node by the intermediate node. As it will give response, the source node catches it as a wormhole node and blocks the wormhole node. After this, the source node sends information to the direct neighbour for updating their entries.

Here, the both type of security that means for local communication and for inter network communication have implemented. Suppose, $N_1, N_2, N_3, \ldots\ldots\ldots, N_{n-1}$ are the nodes between the source N_0 and the destination N_n in a network (it is considered, N_i and N_j are wormhole nodes and making wormhole tunnel). The algorithm works as-

To detect wormhole node, origin N_0 sends modified RREQ packet which contains the address of the false node, to the nearest node N_2. It will check its table for entry of false node. If it is not in its table it will propagate this RREQ message to the intermediate nodes till N_i node. As N_i node receives the RREQ message, it will reply that it has the shortest route to destination false node through N_j node. Because of this declaration by N_i node, the whole traffic will diverted through the N_i node and N_j node. N_i node and N_j node are connected with each other through tunnel. Whenever, the N_i node declares against the modified RREQ packet that it has shortest route to destination false node with the help of RREP packet, the N_i node will be detected as wormhole node and prevented further involvement in communication. After receiving RREP packet, N_0 node will broadcast BLOCK $(N_i, N_j)^{AODV}$ packet information to all other nodes in the network for N_i node and N_j node as wormhole nodes. Each node other than N_i node and N_j node will update entries in their table.

The same procedure will be followed for inter network communication. Therefore, from the above discussion it can be said that this algorithm may be helpful for detecting and preventing wormhole node.

3.7 Conclusion

This chapter outlines about various types of routing attacks present in mobile ad hoc networks. Out of all the available attacks, the wormhole attack is described in an explorative manner. With the wormhole problem, solution that can protect MANETs is also given in the form of algorithm. The proposed algorithm is based on the AODV algorithm. Therefore, the already available AODV is described followed by the SAODV. The aim of the SAODV is to detect and prevent wormhole attack during transmission in mobile ad hoc networks. In the next chapter, implementation of SAODV is shown. It is shown that SAODV is compatible for both the scenarios whether it is local communication or inter network communication.

Chapter 4: Implementation and Validation

4.1 Background

The previous chapter presented a Security Framework that presents the design of an ample and end-to-end security solution for MANETs. In order to attain the aims of the security

requirements defined in this framework, there is a need to propose a set of mechanisms to enforce these security requirements [137] and prevent any attempts to avoid them. To show the efficiency and correctness of the proposed protocol, there is a requirement of implementing the protocol in an effective manner with certain parameters. Here, researcher has taken two parameters to see the correctness of the protocol these are packet delivery ratio and average end-to-end delay. It also shows that the proposed mechanism can be useful in both the scenarios i.e. In-Band wormhole attack and Out-of-Band wormhole attack and also provides a high level of secure, available, scalable services for MANETs.

4.2 Hardware and Software used

For the simulation purpose, a Simulation tool QualNet 4.0 is used. QualNet is a commercial version of GloMoSim developed by Scalable Networks Technology (SNT). The recommended platform requirements to run QualNet on a Windows system are listed below:

- 3.2 GHz Pentium 4, or an equivalent AMD chip
- 1 GB memory
- 700 MB free disk space
- Sun Java™ 2 SDK, Standard Edition, version 1.4.2
- Microsoft Visual C++ .NET 2002 or higher

Listed next is the table which shows hardware and software resources required for QualNet and the resources:-

RESOURCES	RECOMMENDED (AS PER QualNet 4.0)	USED
CPU	3.2 GHz Pentium 4, or an equivalent AMD chip	Intel Pentium Core 2 Duo
Memory	1 GB memory	3 GB for simulations of networks with up to 1000 nodes.
Disk	700 MB free disk space	160 GB free disk space.
Operating System	Microsoft Windows 2000/ XP, Linux, Sun Solaris 10, Mac OS	Microsoft Windows Vista

	X 10.4	
Java	Sun Java™ 2 SDK, Standard Edition, version 1.4.2 or higher	Sun Java™ 2 SDK, Standard Edition, version 1.4.2.
C++ Compiler	Microsoft Visual C++ .NET 2002 or higher	Microsoft Visual C++ .NET 2002.

Table4.1: QualNet Resources – Recommended vs. Used

4.3 Choice of Development Tool

There are several different simulation-programs that can be used for the simulation. Researcher has performed a survey of the commonly used simulators NS2, GloMoSim, QualNet and OPNET in order to determine the most suitable simulator for implementing scenarios. Researcher did survey based on the following criterias:

- Which protocols does it support?
- How well is it documented?
- Is it complicated to install?
- How frequent is the simulator used in research-papers regarding MANETs?
- Can the existing code be extended in any way?
- How user-friendly is it?

4.3.1 NS2

This simulator is probably the most commonly used software of the four. NS2 stands for the Network Simulator 2 [140] and is developed by ISI, the Information Sciences Institute at the USC School of engineering. The source code can be downloaded, free of charge, and compiled on different platforms, e.g. UNIX and Windows. There is an extensive manual for the installation and use of the software on the NS2 homepage. Other people have also put tutorials for this program on the Internet. The software is for the larger part text-based and might therefore be a bit complicated to use if you aren't familiar to Unix-commands. Some parts are managed with GUIs, which makes it easier to understand what's happening. There are also many different extensions developed by varies researchers to this software.

Many wireless extensions have been contributed from the UCB Daedelus, the CMU Monarch projects and Sun Microsystems. The documentation to these extensions is not always as extensive as you would like and the developers of NS do not always support them. In NS2 it's possible to alter and write your own code to make it more suitable for your own scenarios. The most recent version of NS2 is NS-2.26 which is released the 26 of February 2003 and supports AODV, DSDV, DSR and TORA. If you want to simulate on other protocols there are extensions that support ADMR, AODV+, AODV-UU, Ariadne, MAODV, ODMRP, SEAD and ZRP. NS2 is constantly under development and you can monitor its progress on its homepage. There is also a bug report form where you can report any problems and bugs you encounter while using NS2. In addition to these features there are also a FAQ and the possibility to sign up to three different ns-related mailing lists.

4.3.2 GloMoSim

GloMoSim [141] stand for Global Mobile information systems Simulation library and supports protocols for a purely wireless network. It's developed at UCLA Parallel Computing Laboratory (UCLA PCL) and is intended for academic institutions for research purposes. It's only possible to download the current version, GloMoSim 2.0 (December 2000), from the GloMoSim homepage if you are within the edu domain. If commercial users want to use GloMoSim they have to obtain the commercial version called QualNet. This version is extended in some areas.

In order to get GloMoSim to work you have to install Parsec, which is a C-based simulation language developed by PCL at UCLA. There is very little documentation of the installation procedure. Either it's very easy to install or it's poorly documented. In any case, if you would run into trouble while installing you won't get much help from the documentation. Also the documentation of how to use the software is poorly described. GloMoSim support some protocols, which lies in our interest. These are AODV, DSR, Fisheye, LAR, ODMRP and WRP. If you want to develop your own protocols in GloMoSim, it's possible. But to do so you should have some familiarity with Parsec. Although the code to the protocols will be written purely in C code, with some Parsec functions for time management, you will need to use the Parsec compiler. As mentioned earlier the last version was released in December 2000 and the homepage was last updated in February 2001. There

is no FAQ, forum or a mailing list on the homepage. Although there are some papers in which GloMoSim have been used, it's not as frequently used as NS2.

4.3.3 QualNet

QualNet is developed by SNT (Scalable Network Technologies) and is network simulation software. SNT claims that you can use QualNet when you design a network or network device to optimize it, saving time and money. The QualNet software [142] consists of five tools plus integration modules and model libraries. QualNet Animator allows for graphically designing the network model (using a wide library of components) and can be used to display the simulation as it runs or later on. QualNet Designer is for streamline code development. You can generate code for your own protocol from scratch and make special statistic reports. You can also make adjustments to already made protocol models.

QualNet Analyzer is a graphic tool that presents statistics of different experiments in graphs. The QualNet model library is a large library of networking options and contains the MANET library. It includes models for providing wireless dynamic routing, shadowing, fading, mobility, detailed physical layer effects such as steerable directional antennas and complex modulation schemes. Routing protocols provided are DSR, Fisheye, LAR, OLSR, STAR, ZRP and ODMRP. At their homepage you can find much documentation and help. There are manuals as well as a FAQ and a forum. You can also get support by emailing or phoning SNT. QualNets customers include companies like Microsoft and Boeing and it is used by the military. There are also some publications done featuring QualNet as the simulation tool.

4.3.4 OPNET

OPNET is a simulation tool that is developed by OPNET [143] Technologies Inc. They are a leading provider of management software for networks and applications. OPNET have a number solutions that aims to help the customer in different areas like, application performance troubleshooting, application deployment planning, network configuration auditing, network capacity and resiliency planning and network technology R&D. For simulating a MANET, OPNET provides a software platform called the OPNET Modeler. This software also contains a large number of different models for simulating network

protocols, technologies and applications. There are a wireless model included that provides the two routing protocols DSR and TORA. Although OPNET is rather intended for companies to diagnose and organize their networks, you could develop and implement your own protocol or modify existing implementations of standard protocols. The software tends to be well documented and there shouldn't be any problems either with the installation or support. On the homepage there are technical resources with a FAQ and product updates as well as a forum for OPNET users. To be able to participate in the forum and download the documents you have to have a license since they are protected by passwords. On the negative part the software is very expensive and not easy to obtain for single individuals.

4.3.5 Simulator selected for Simulation

When choosing a simulation program the question of what you want to simulate and which resources you have to conduct these simulations are of great importance. What researchers want to simulate should work in any of the four simulators, if you have the right tools and knowledge [144]. QualNet and OPNET are well-developed commercial software products and should be easier to use than the other two. The problem is that they cost a lot! Researchers haven't got the financial support to buy these products. The question also arises of how much open source code that is publicly available. This is an important factor since researchers haven't got the time and knowledge to implement the protocol or write the simulation code on our own. GloMoSim is available for downloading only if your IP address resolves to an academic domain name. The documentation isn't very good and it seems to be hard to get any kind of support. Even though some papers have used

GloMoSim to simulate MANET protocols, the questions how to validate and compare our results with other works are an issue of concern. The developing of new software for GloMoSim also seems to be quite sparse. NS2 is free to download and researchers for simulating mobile ad hoc networks commonly use it. It has an extensive manual and some support in the mailing list. New features are developed continuously and added functions for protocols are available for downloading. None of the four simulation programs are currently including the possibility to simulate the security protocols. If you want to simulate them you have to implement them on your own, writing your own source code. There are projects that have used the simulation programs for simulating their security routing protocol, like the

Monarch Project that has implemented Ariadne in NS2. Altogether the choice of simulation program was quite clear; NS2 provided the best overall solution for our purpose.

4.4 Design of Experiment

There are two scenarios implemented using QualNet Simulator 4.0. The first scenario is implemented for In-Band Wormhole Attack. For this, three conditions have been taken. These are 1) Ad hoc Network with no Attack, 2) Ad hoc Network with Attack using AODV and 3) Ad hoc Network with Attack using SAODV. All the three conditions are implemented to compare the performance of the AODV and SAODV under wormhole attack.

4.4.1 Scenarios for In-Band Wormhole Attack

In an In- Band Wormhole Attack, tunnel is created by using the already available nodes in the network. This condition makes the MANET more critical because of the involvement of the nodes in the network. That means apart from the two nodes that are working as initiator nodes for creation of wormhole node, other legal nodes are helping initiator nodes in performing mischievous activities in the network. At that time it is difficult to trust on legal nodes also. Therefore, the motive of this solution is to block the whole path after detecting the malicious nodes that are creating wormhole tunnel. This situation mostly occurs in local communication. The scenarios implemented for In-Band wormhole attack are discussed below:

Ad Hoc Network with no Attack: In this set up, an ad hoc network is designed with no attack using AODV routing protocol. That means no mischievous activities are going on during transmission.

Ad Hoc Network with Attack using AODV: In this set up, an ad hoc network is taken in to account in which wormhole attack is present. The AODV routing protocol is used for this scenario.

Ad Hoc Network with Attack using SAODV: In this set up, ad hoc network is available in which wormhole attack is present. At this time, SAODV routing protocol is used.

4.4.2 Scenarios for Out-of-Band Wormhole Attack

The working of out-of-band wormhole attack is different from the in-band wormhole attack in the sense that out-of-band attack do not use the other legal nodes present in the network. The motives of both attack either in-band attack or out-of-band attack is same. In out-of-band wormhole attack, the tunnel is created using two nodes that are wormhole nodes. Therefore, a virtual connection is established between these wormhole nodes. This situation mostly occurs in inter network communication. The scenarios implemented for out-of-band wormhole attack are discussed below:

Ad Hoc Network with no Attack: In this set up, an ad hoc network is implemented with no attack using AODV routing protocol. That means no mischievous activities are going on during transmission. In this situation, two networks are taken to show inter network communication.

Ad Hoc Network with Attack using AODV: In this set up, an ad hoc network is taken in to account in which wormhole attack is present. The AODV routing protocol is used for this scenario. In this situation, two networks are taken to show inter network communication.

Ad Hoc Network with Attack using SAODV: In this set up, ad hoc network is available in which wormhole attack is present. At this time, SAODV routing protocol is used. In this situation, two networks are taken to show inter network communication.

4.5 Simulation Report

Total six experiments are implemented to verify the effectiveness of the protocol. First three experiments are implemented with in-band wormhole attack and rest three experiments are implemented with out-of-band wormhole attack. The thesis has implemented all the scenarios in a QualNet simulator. In all the scenarios, following settings are taken:

- Net diameter : 35m
- Node Traversal Time : 40MS
- Active Route Timeout : 3S

- Local Repair : YES
- Max Buffer Packets : 100
- Max Buffer Size (Bytes) : 100
- MAC Layer : 802.11, peer-to-peer
- Radio : No Fading with radio range set to 250m

4.5.1 In-Band Scenario: Network Performance using AODV without Wormhole Attack

The simulated network consists of 23 randomly allocated wireless nodes in a 1500 by 1500 square meter flat space. Random waypoint model is used for scenarios with node mobility. The selected pause time is 30s. All nodes are considered as legal nodes. There are no wormhole nodes in this scenario. This scenario is taken to see the performance of AODV before enhancement. How the actual AODV works in the normal conditions. This is taken to see the comparison among (1) the network without malicious node & previous AODV protocol (2) the network with wormhole attack & previous AODV protocol (3) the network with wormhole attack & SAODV. This simulation executed 208752 events in 16.6423 seconds with 2 sec pause time. The X- axis shows the number of nodes with node ID like 1, 2, or 3 etc. the Y- axis shows number of packets in the multiple of 10. This thing regarding X- axis and Y- axis is applicable for all the scenarios. Results of these experiments are shown in following figures-

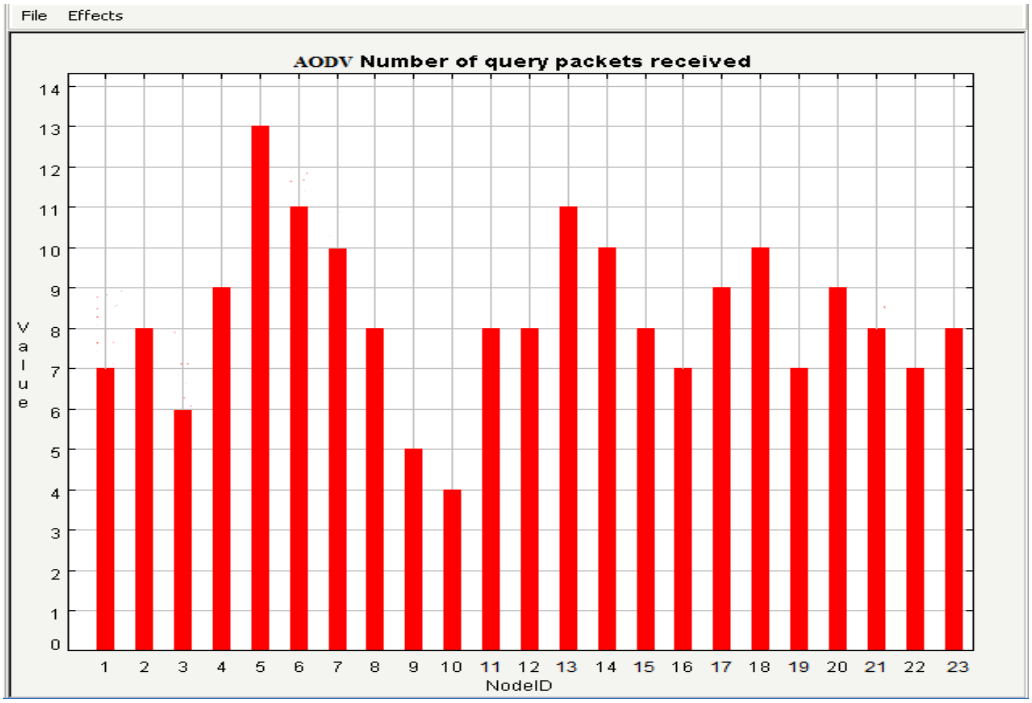

Figure4.1: MANET with No Wormhole Node – Number of Data Packets Received

Description- In this figure4.1, there are 23 mobile nodes in a network. There is no wormhole node in the network. The figure shows no. of query packets received by each node.

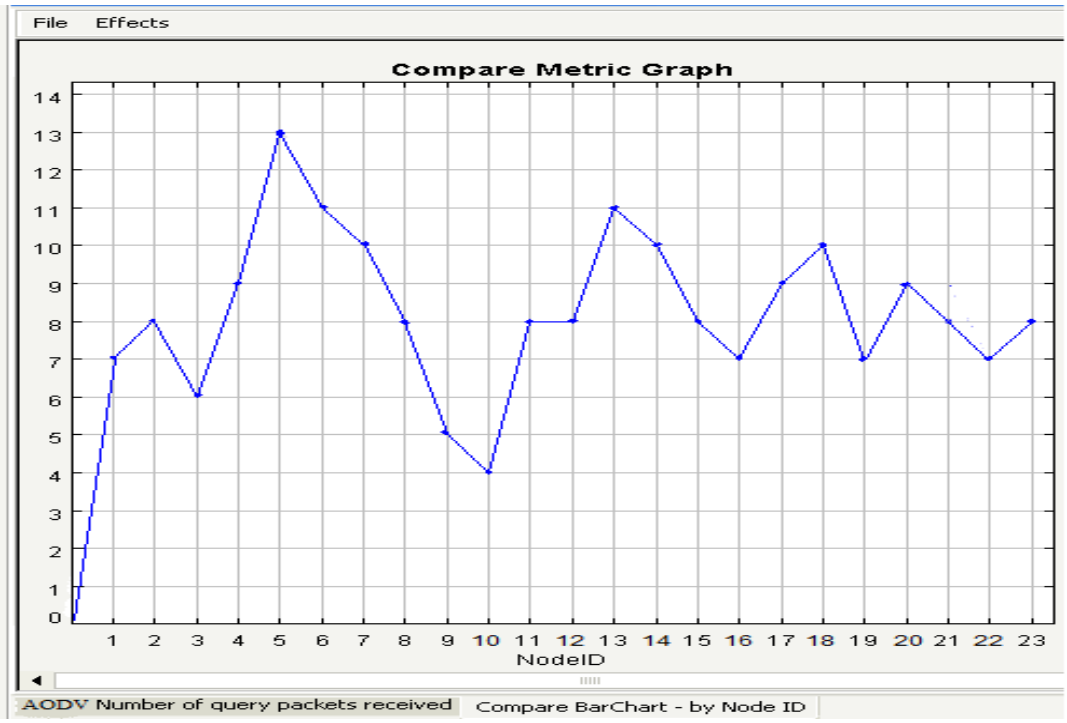

Figure4.2: MANET with No Wormhole Node – Number of Data Packets Received (Compare Metric Graph)

Description- This figure4.2 is a Compare Metric graph of the figure4.1.

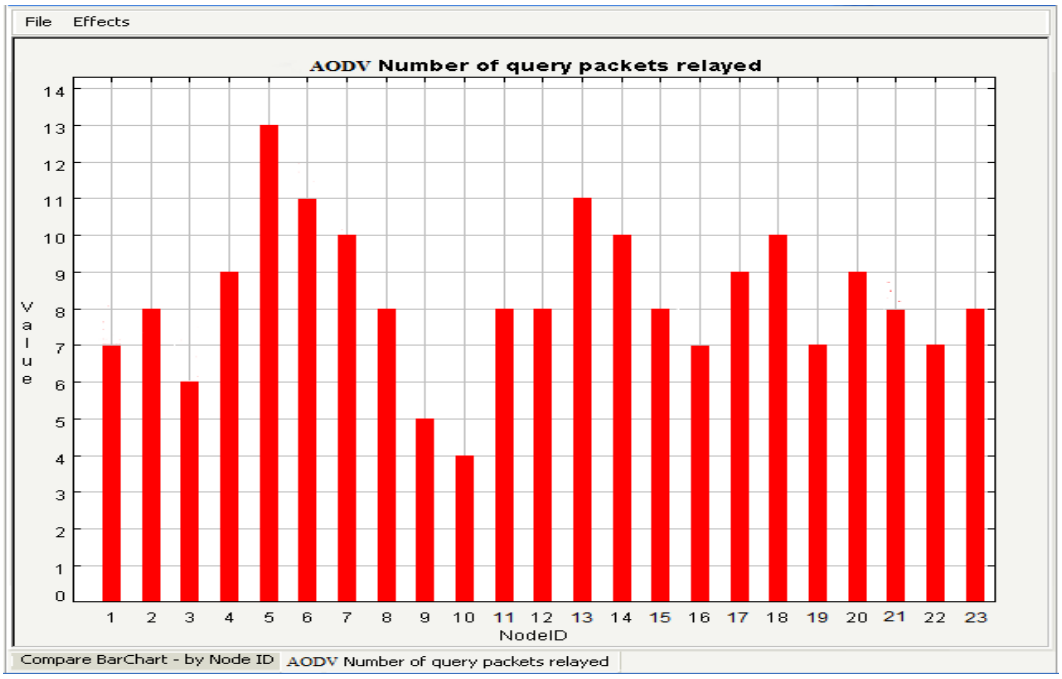

Figure4.3: MANET with No Wormhole Node – Number of Data Packets Relayed

Description- In this figure4.3, there are 23 mobile nodes in a network. The figure shows no. of query packets relayed by each node.

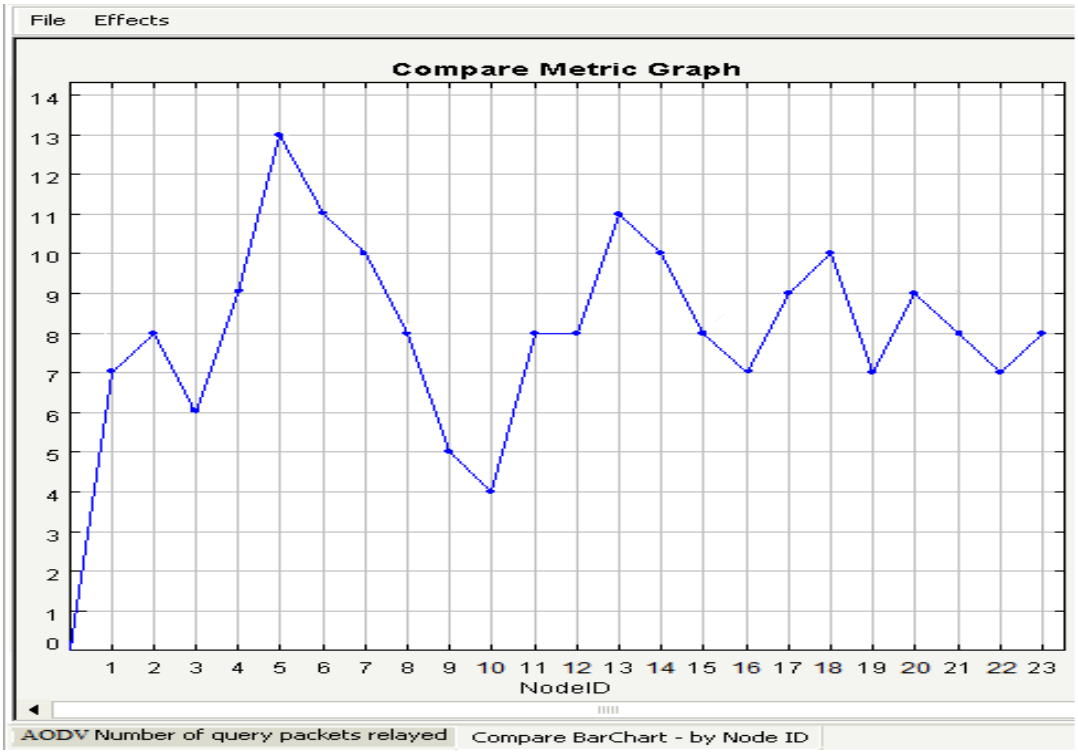

Figure4.4: MANET with No Wormhole Node – Number of Data Packets Relayed (Compare Metric Graph)

Description- This figure4.4 is a Compare Metric graph of the figure4.3.

4.5.2 In-Band Scenario: Network Performance using AODV with Wormhole Attack

In the second experiment, 25 nodes are taken in a network. All nodes are assumed to be legal nodes except no. 9 and 19 nodes. Node 9 and 19 are creating wormhole tunnel. Routing protocol AODV is taken. In the AODV, AODV max message buffer size = 100 are taken. This scenario is taken to see the performance of AODV before enhancement and under wormhole attack. This simulation executed 165761 events in real time 13.5323 seconds with 0.7247 sec spent paused.

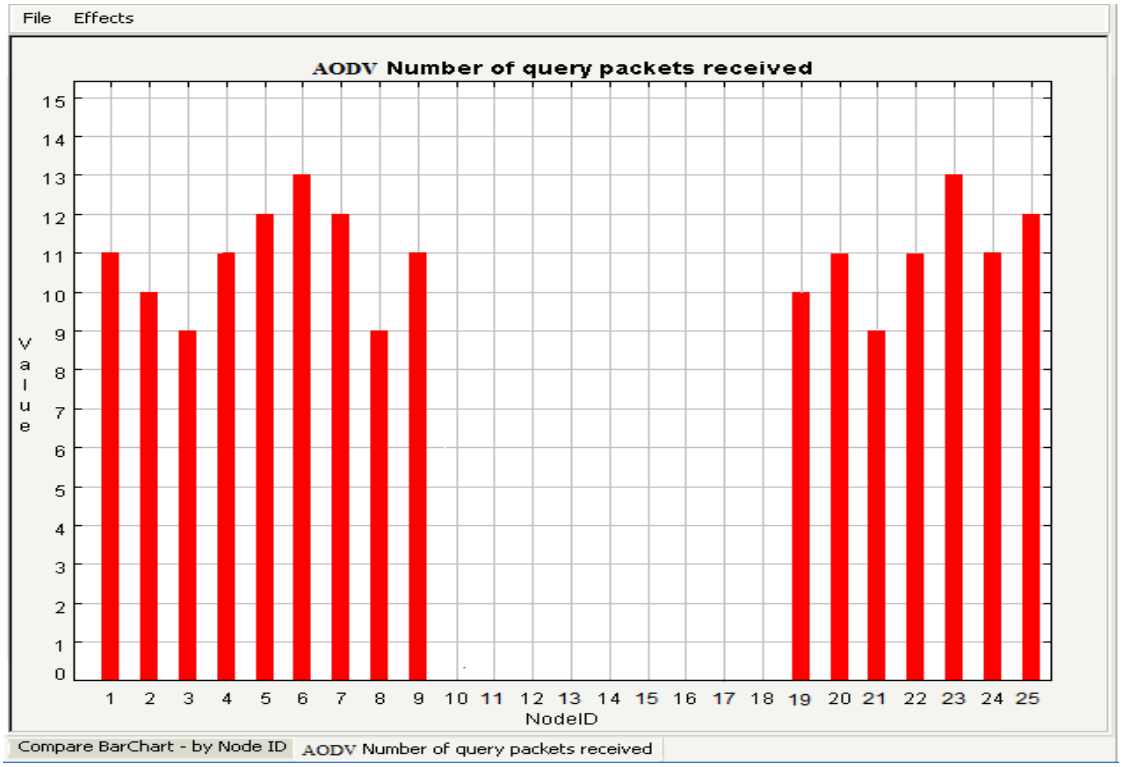

Figure4.5: MANET with Node 9 and 19 as wormhole nodes – Number of Data packets received

Description- In this figure4.5, there are 25 mobile nodes in a network. In experiment, nodes 9 and 19 are involved in creating wormhole attack and restricting nodes 10, 11, 12, 13, 14, 15, 16, 17 and 18 to receive data traffic. The figure shows no. of query packets received by each node.

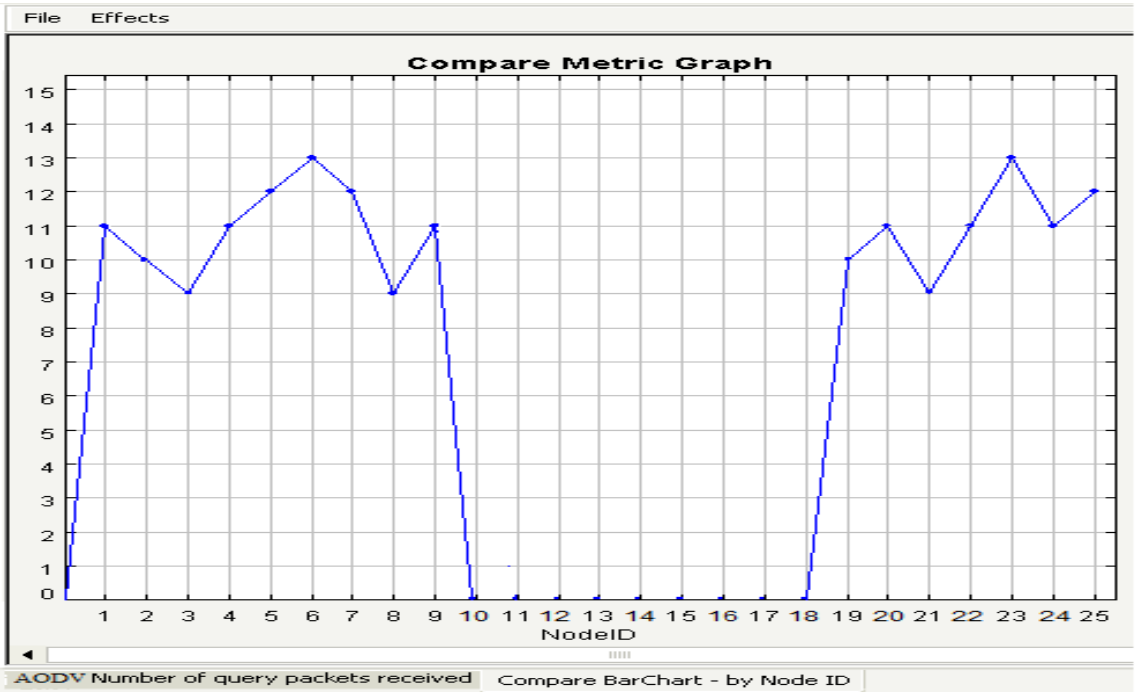

Figure4.6: MANET with Node 9 and 19 as wormhole nodes – Number of Data packets received (Compare Metric Graph)

Description- This figure4.6 is a Compare Metric graph of the figure4.5.

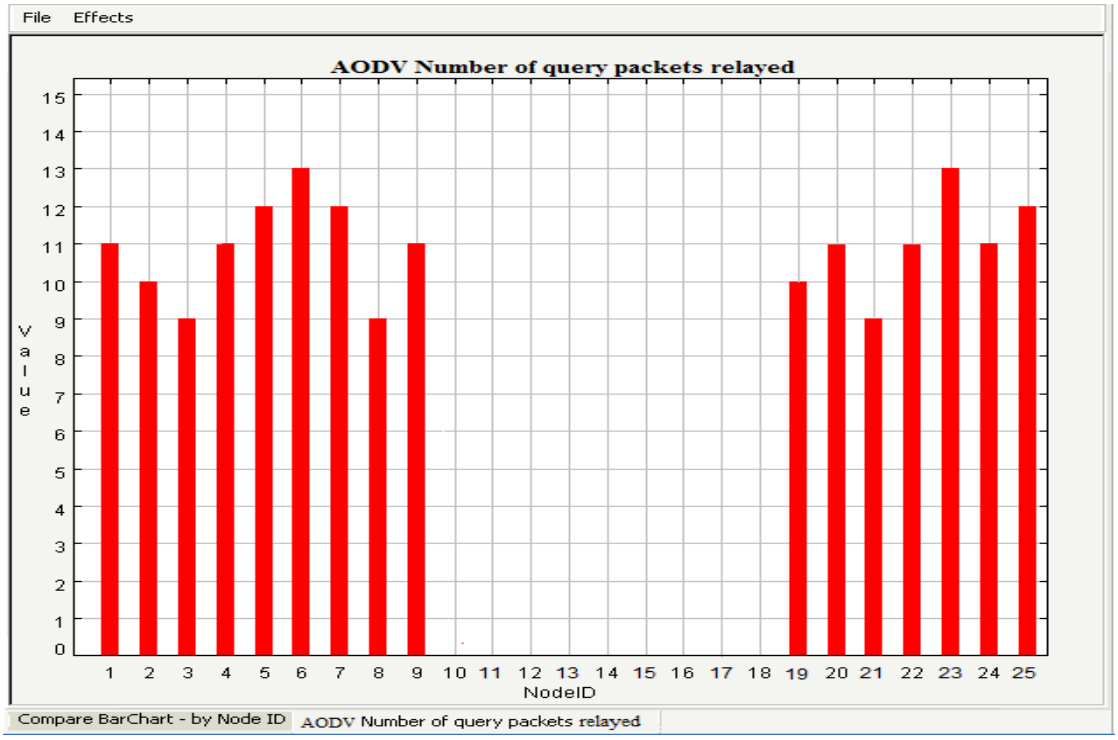

Figure4.7: MANET with Node 9 and 19 as wormhole nodes – Number of Data packets relayed

Description- In this figure4.7, there are 25 mobile nodes in a network. Node 9 and 19 are creating wormhole attack. The figure shows no. of query packets relayed by each node.

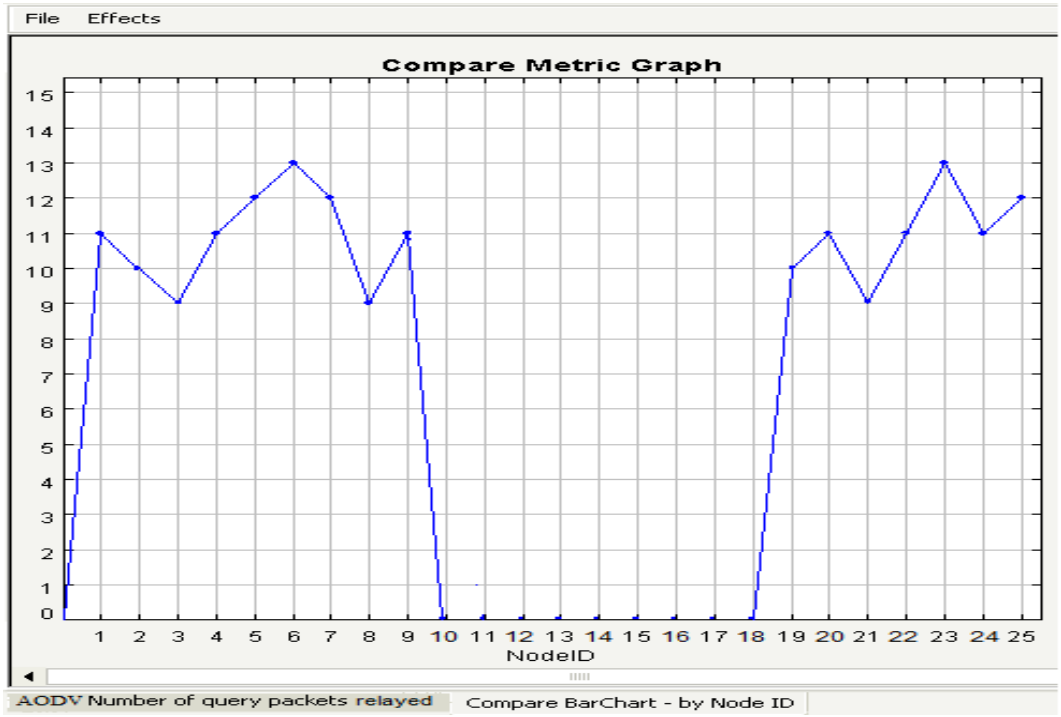

Figure4.8: MANET with Node 9 and 19 as wormhole nodes – Number of Data packets relayed (Compare Metric Graph)

Description- This figure4.8 is a Compare Metric graph of the figure4.7.

4.5.3 In-Band Scenario: Network Performance using SAODV with Wormhole Attack

This experiment investigates the effectiveness of the protocol design under wormhole attack. In this experiment, validity of SAODV protocol is checked and ensured that it is the sufficient and efficient approach for finding wormhole nodes within the network. It is considered that the node with hop count (HC) =1 will be direct neighbour node for each node. In this experiment, it is analyzed that how the network is protected from the wormhole attack. In this simulation scenario is created with in-band wormhole attack in the network. Now, SAODV is applied to see the effect of protocol when wormhole attack is present in the network. This scenario contains 25 nodes. In the scenario, nodes are chosen randomly. Mobility model was random way point. Routing protocol is SAODV. SAODV max message buffer size = 100. In this simulation IP forwarding is enabled. This simulation executed 255663 events in real time 19.4215 seconds with 2 sec spent paused. Simulation time is kept 30 sec. Results of this experiment is shown in following figures-

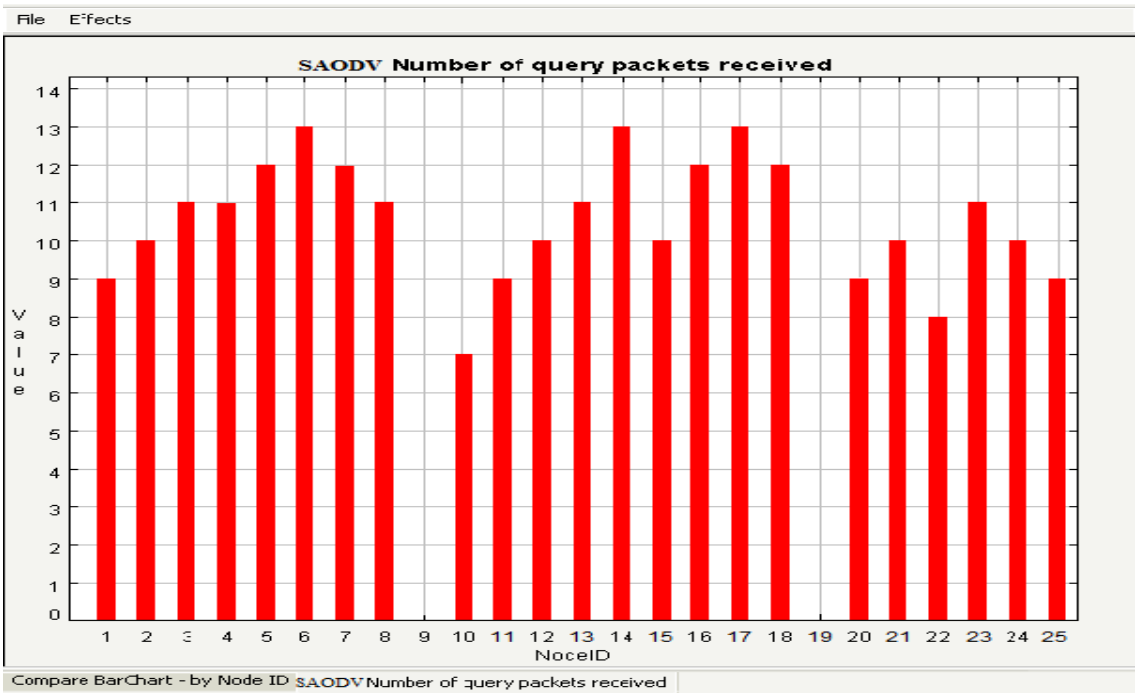

Figure4.9: MANET with SAODV– Number of Data packets received

Description- In this figure4.9, there are 25 mobile nodes in a network. Nodes 9 and 19 are involved in creating wormhole node. The figure shows no. of query packets received by each node except nodes 9 and 19.

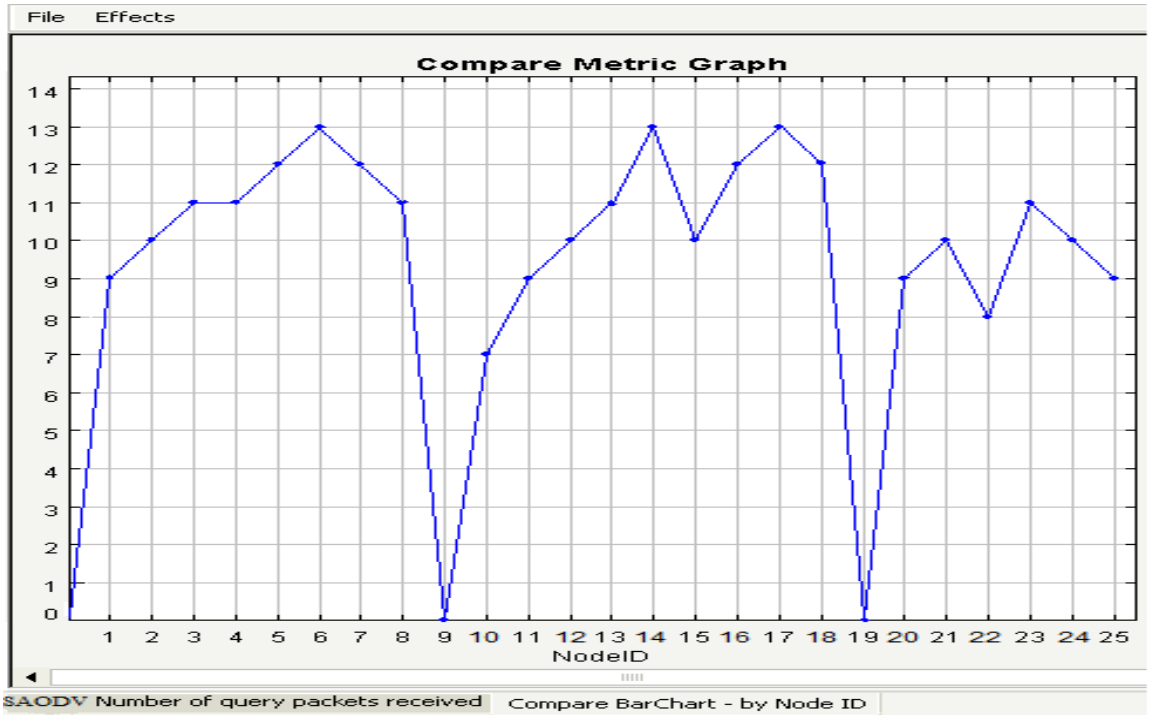

Figure4.10: MANET with SAODV– Number of Data packets received

(Compare Metric Graph)

Description- This figure4.10 is a Compare Metric graph of the figure4.9.

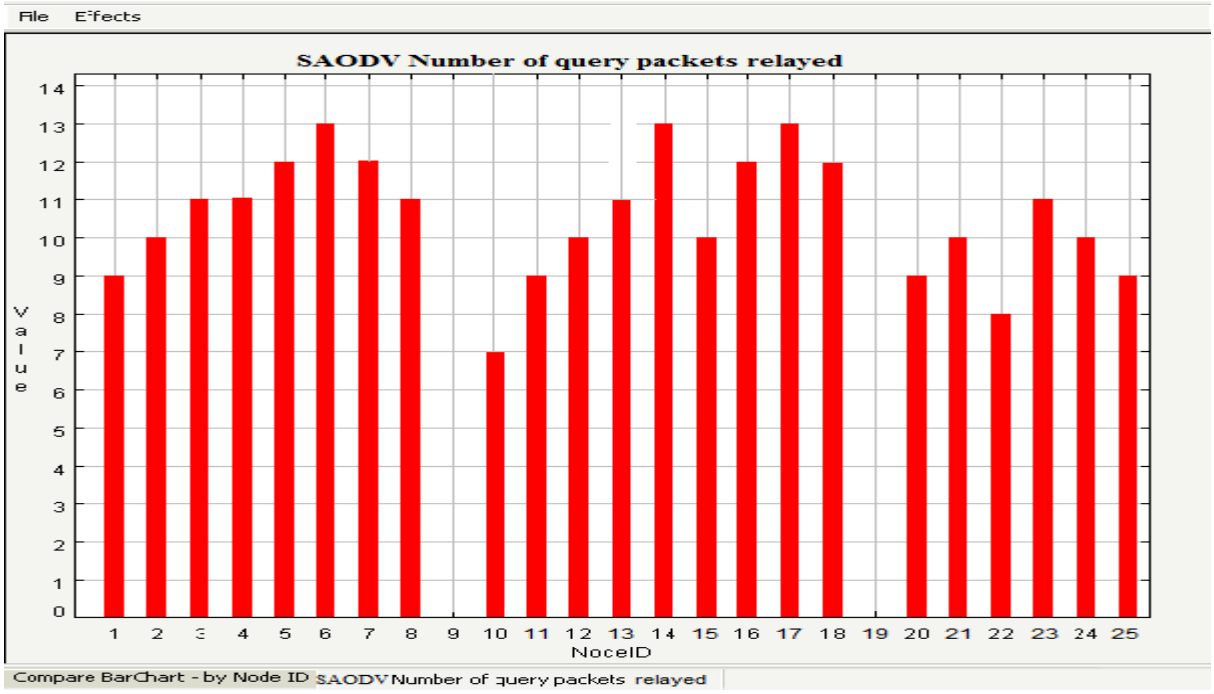

Figure4.11: MANET with SAODV– Number of Data packets Relayed

Description- In this figure4.11, there are 25 mobile nodes in a network. Nodes 9 and 19 are creating wormhole attack. The figure shows no. of query packets relayed by each node except nodes 9 and 19.

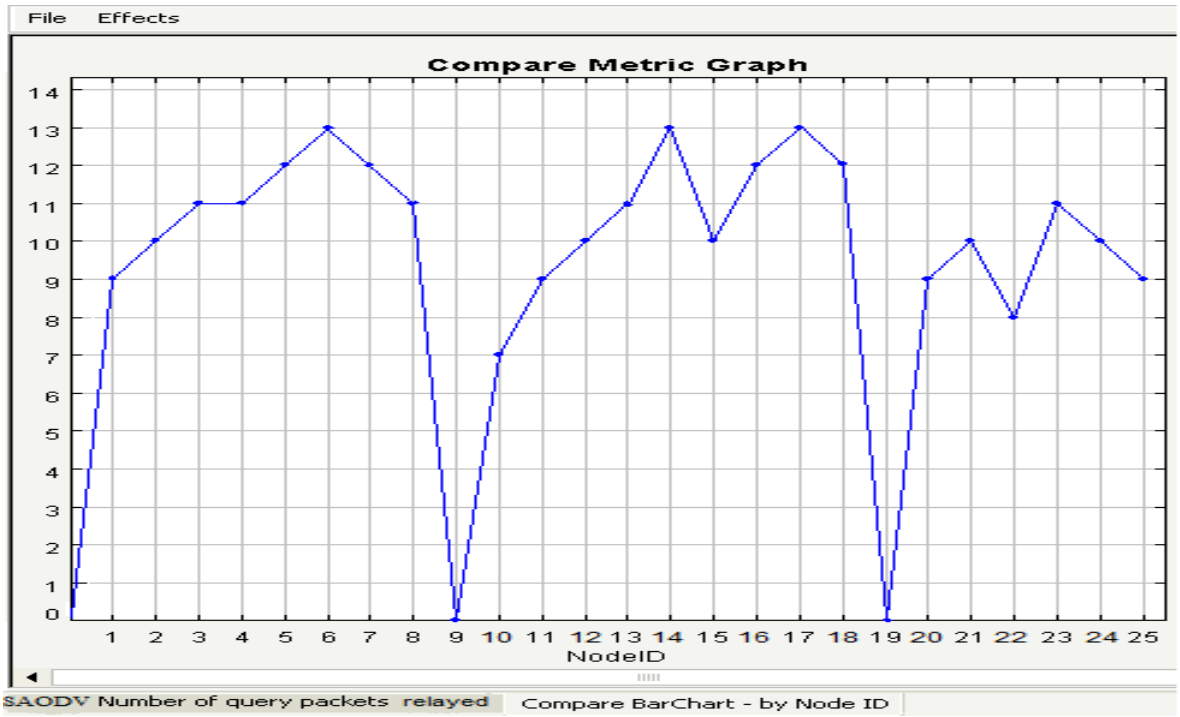

Figure4.12: MANET with SAODV– Number of Data packets Relayed

(Compare Metric Graph)

Description- This figure4.12 is a Compare Metric graph of the figure4.11.

4.5.4 Out-of-Band Scenario: Network Performance using AODV without Wormhole Attack

First three experiments are to see the performance of the proposed protocol in the presence of in-band wormhole attack. Now, the performance of the SAODV protocol will be analyzed under out-of-band wormhole. In this experiment, varying numbers of nodes (only valid nodes are considered) are taken to check the validity of SAODV protocol and ensure that it is the sufficient and efficient approach for finding wormhole nodes within the network or outside the network. It is considered that the node with hop count (HC) =1 will be direct neighbour node for each node. In this experiment, it is analyzed that how the network is protected from the wormhole attack. Now the inter network communication is considered. In this simulation two networks are taken to show inter network communication. First network consists of 18 nodes while in the second network, there are 23 nodes available for communication. Both the networks have no malicious nodes. In the scenario, nodes are chosen randomly. Mobility model was random way point. Routing protocol is AODV. AODV max message buffer size = 100 are taken. In this simulation IP forwarding is enabled. This simulation executed 357852 events in real time 30.5632 seconds with 3.4653 sec spent paused. Simulation time is kept 30 sec. Results of this experiment is shown in following figures-

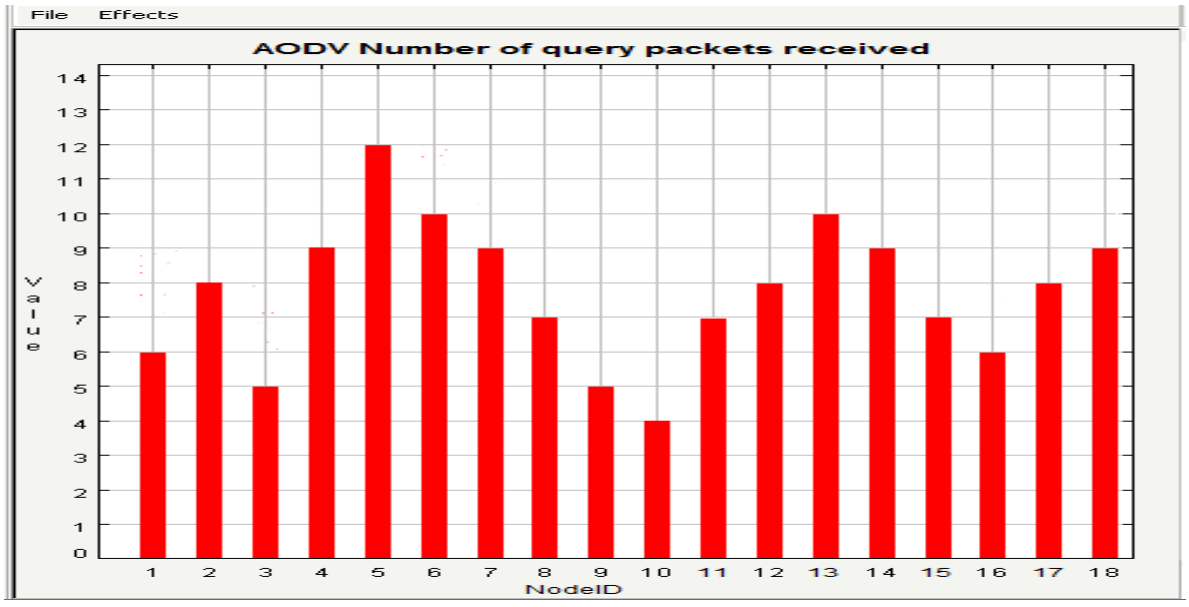

Figure4.13: Network1 with No Wormhole Node – Number of Data Packets Received

Description- In this figure4.13, there are 18 mobile nodes in a network 1. There is no wormhole node in the network. The figure shows no. of query packets received by each node.

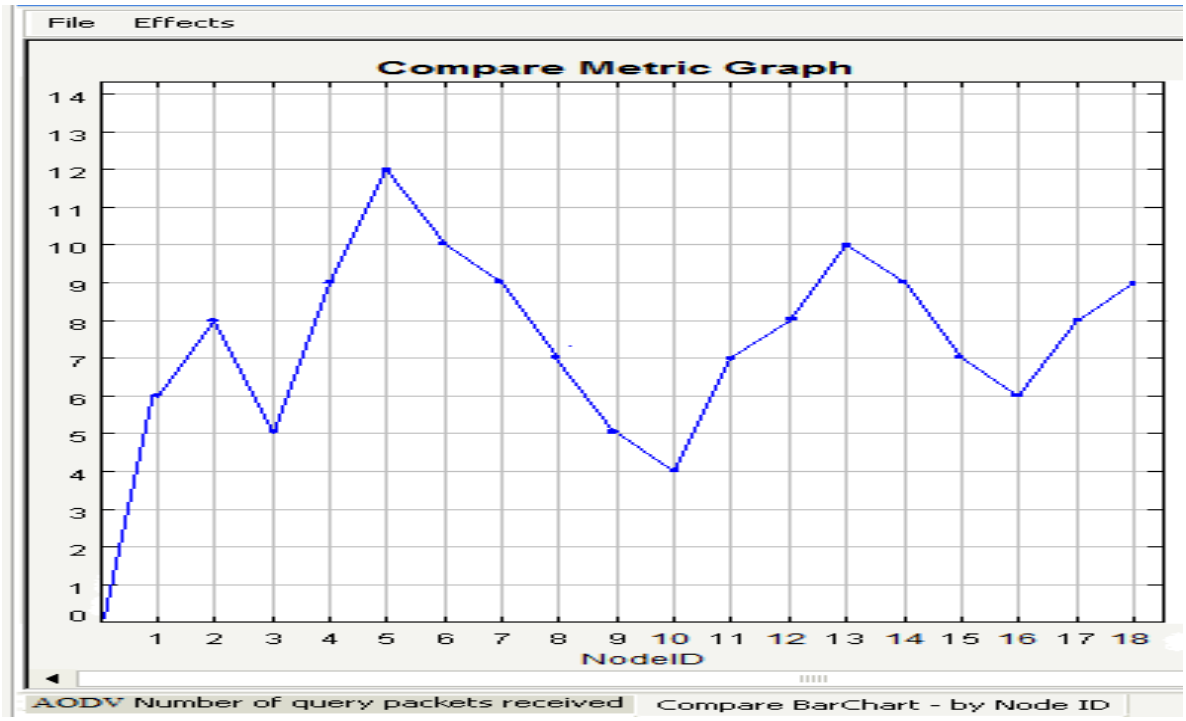

Figure4.14: Network1 with No Wormhole Node – Number of Data Packets Received (Compare Metric Graph)

Description- This figure4.14 is a Compare Metric graph of the figure4.13.

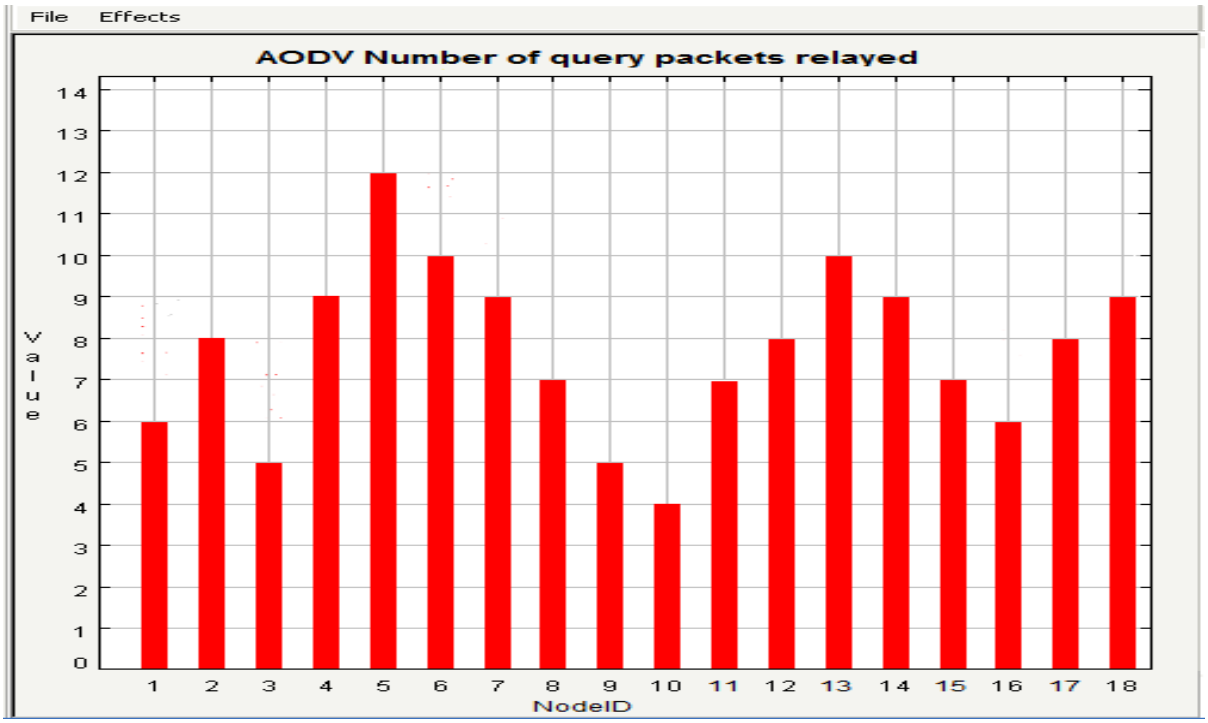

Figure4.15: Network1 with No Wormhole Node – Number of Data Packets Relayed

Description- In this figure4.15, there are 18 mobile nodes in a network. The figure shows no. of query packets relayed by each node.

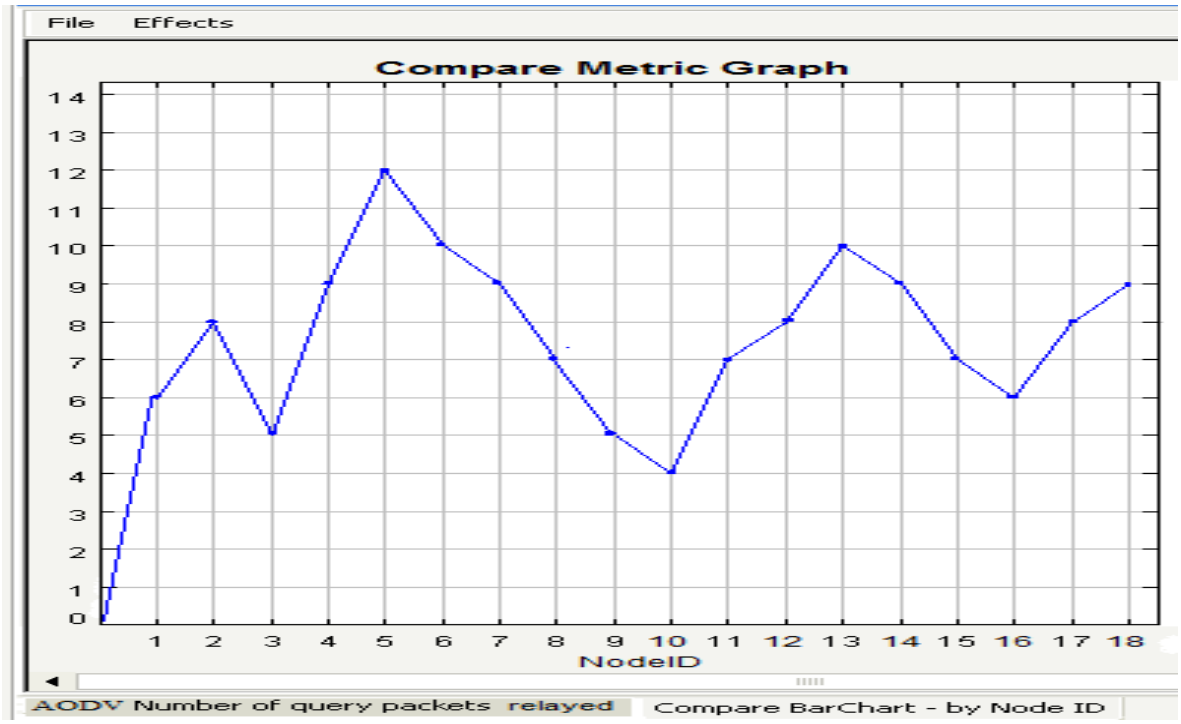

Figure4.16: Network1 with No Wormhole Node – Number of Data Packets Relayed (Compare Metric Graph)

Description- This figure4.16 is a Compare Metric graph of the figure4.15.

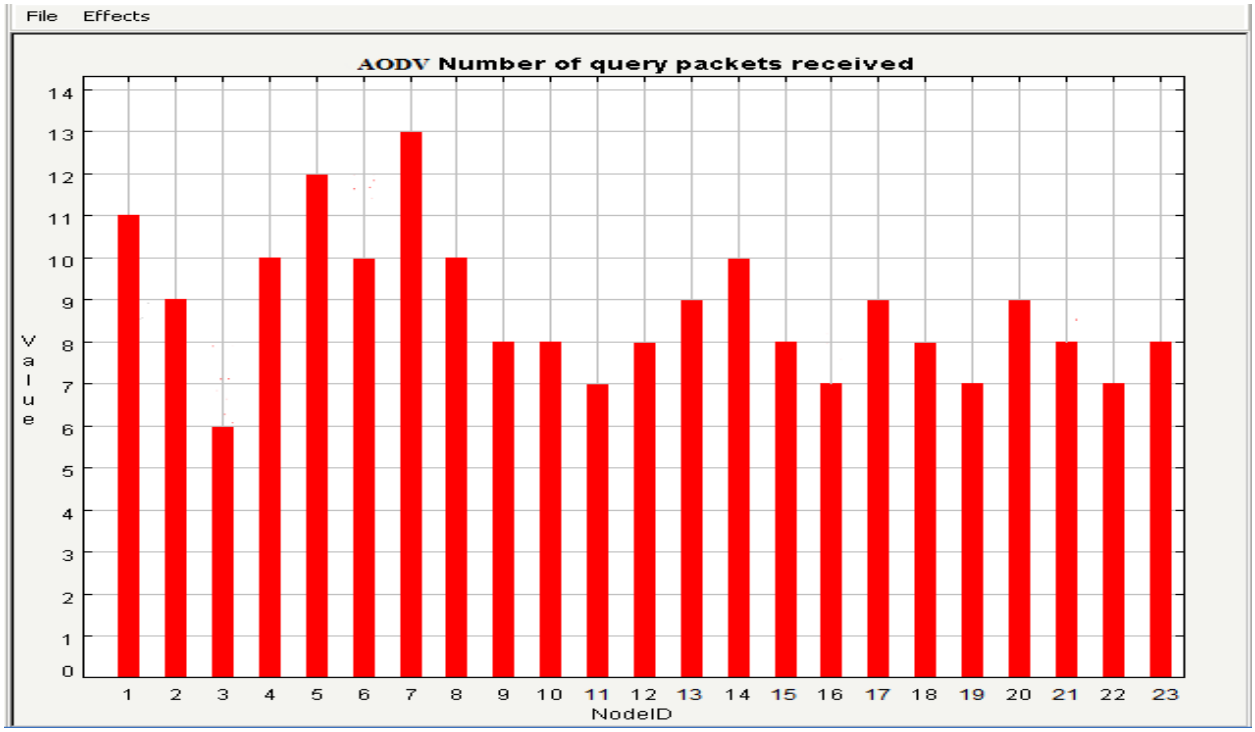

Figure4.17: Network2 with No Wormhole Node – Number of Data Packets Received

Description- In this figure4.17, there are 23 mobile nodes in network 2. There is no wormhole node in the network. The figure shows no. of query packets received by each node.

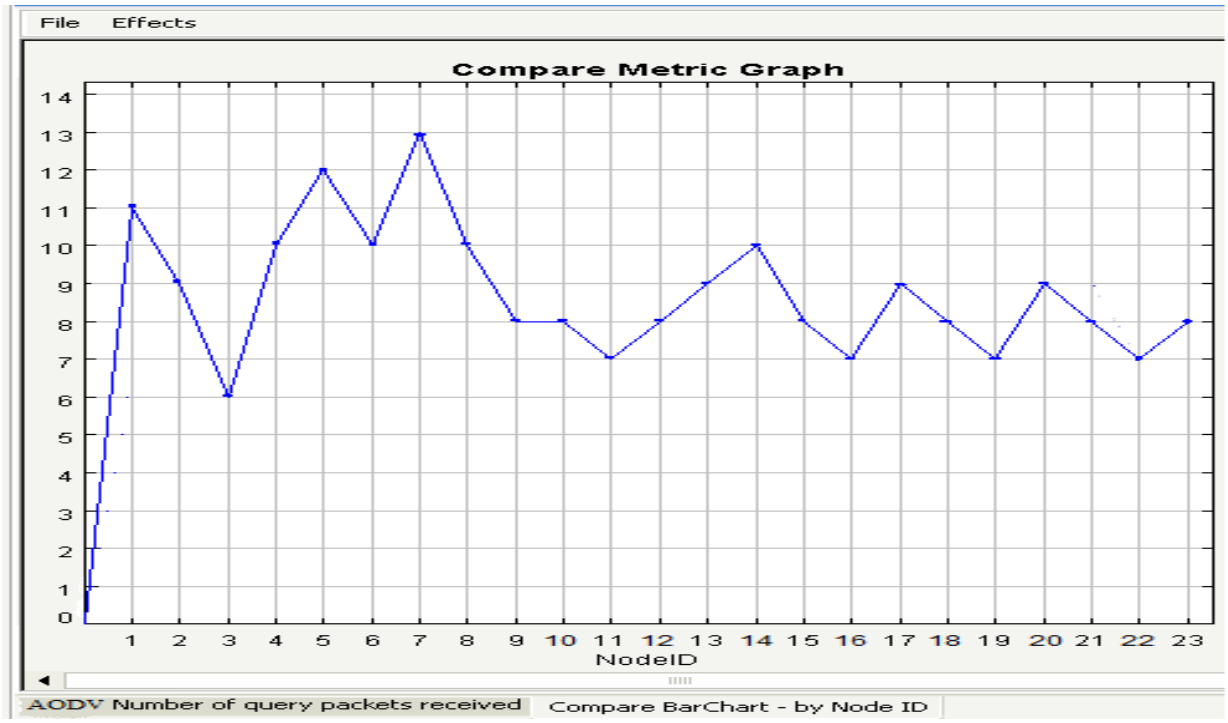

Figure4.18: Network2 with No Wormhole Node – Number of Data Packets Received (Compare Metric Graph)

Description- This figure4.18 is a Compare Metric graph of the figure4.17.

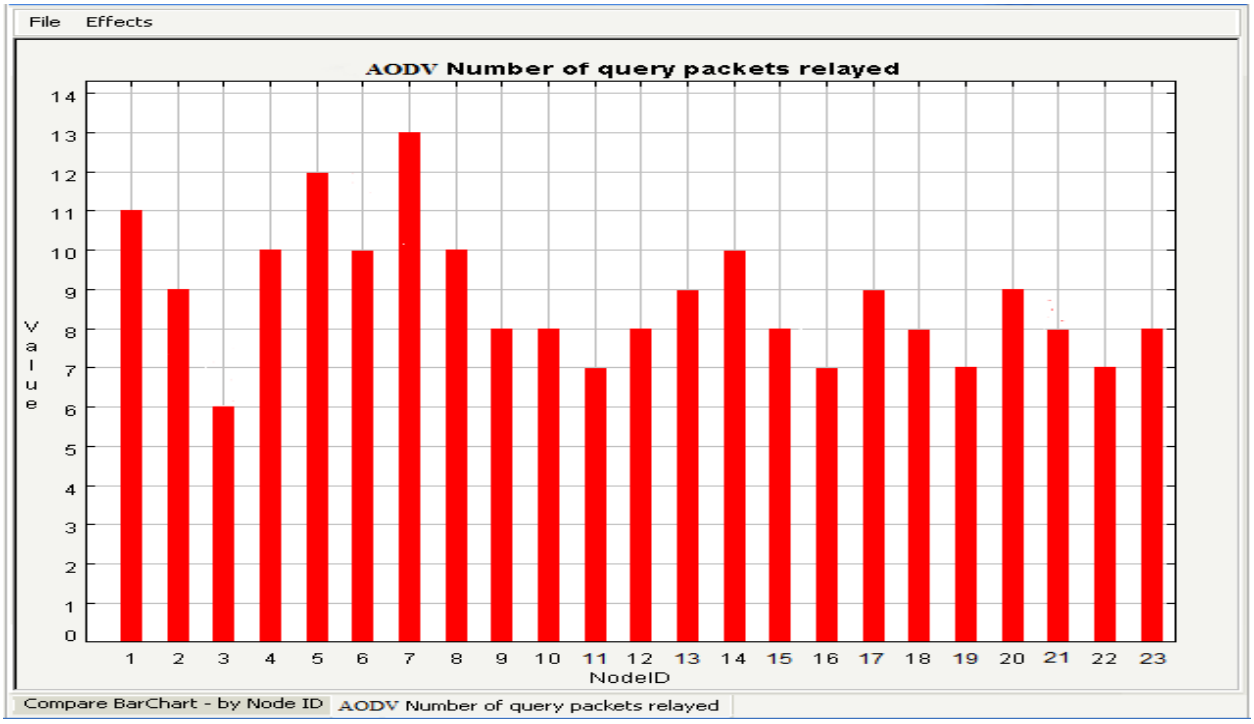

Figure4.19: Network2 with No Wormhole Node – Number of Data Packets Relayed

Description- in this figure4.19, there are 23 mobile nodes in the network. The figure shows no. of query packets relayed by each node.

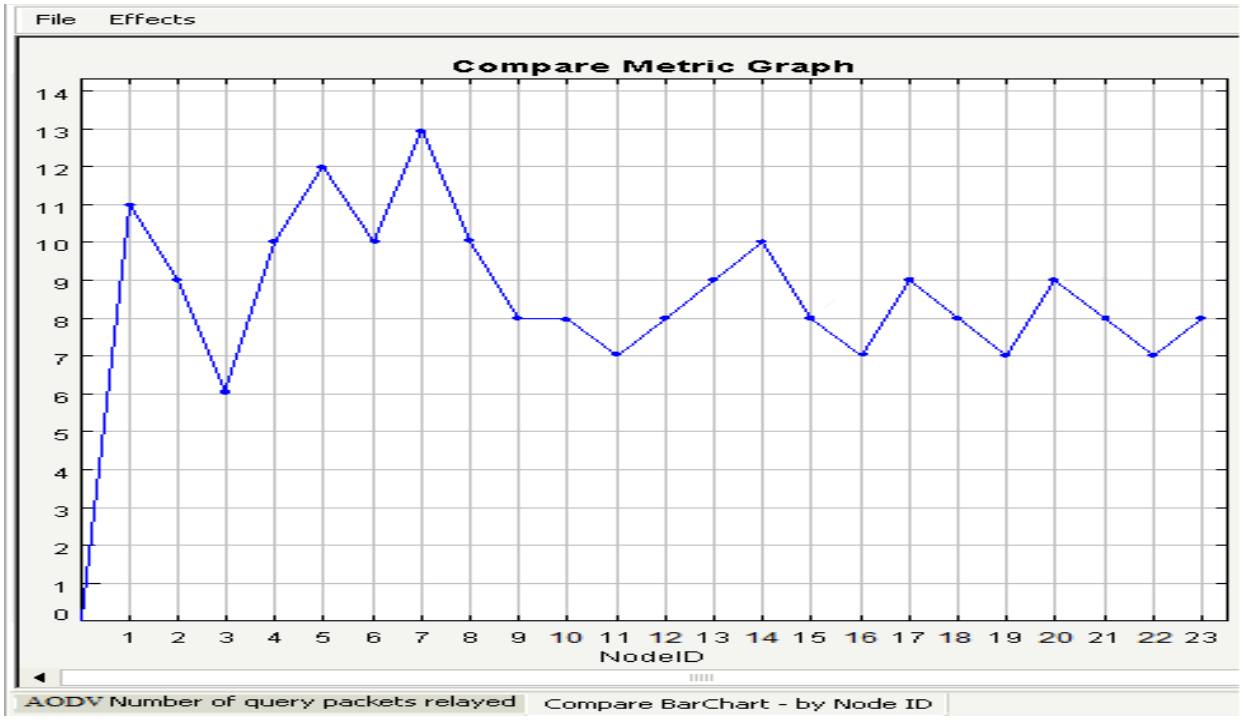

Figure4.20: Network2 with No Wormhole Node – Number of Data Packets Relayed (Compare Metric Graph)

Description- This figure4.20 is a Compare Metric graph of the figure4.19.

4.5.5 Out-of-Band Scenario: Network Performance using AODV with Wormhole Attack

In this experiment, two networks are taken. First network consist of 18 nodes while the second network consist of 25 nodes. All nodes are assumed to be legal node except two nodes, one wormhole node in each network. Node 12 in network 1 and node 11 in network 2 are creating wormhole attack. Routing protocol AODV is taken. AODV max message buffer size = 100 are taken. This scenario is taken to see the performance of AODV before enhancement. This simulation executed 296741 events in real time 25.4526 seconds with 3.4653 sec spent paused. Simulation time is kept 30 sec.

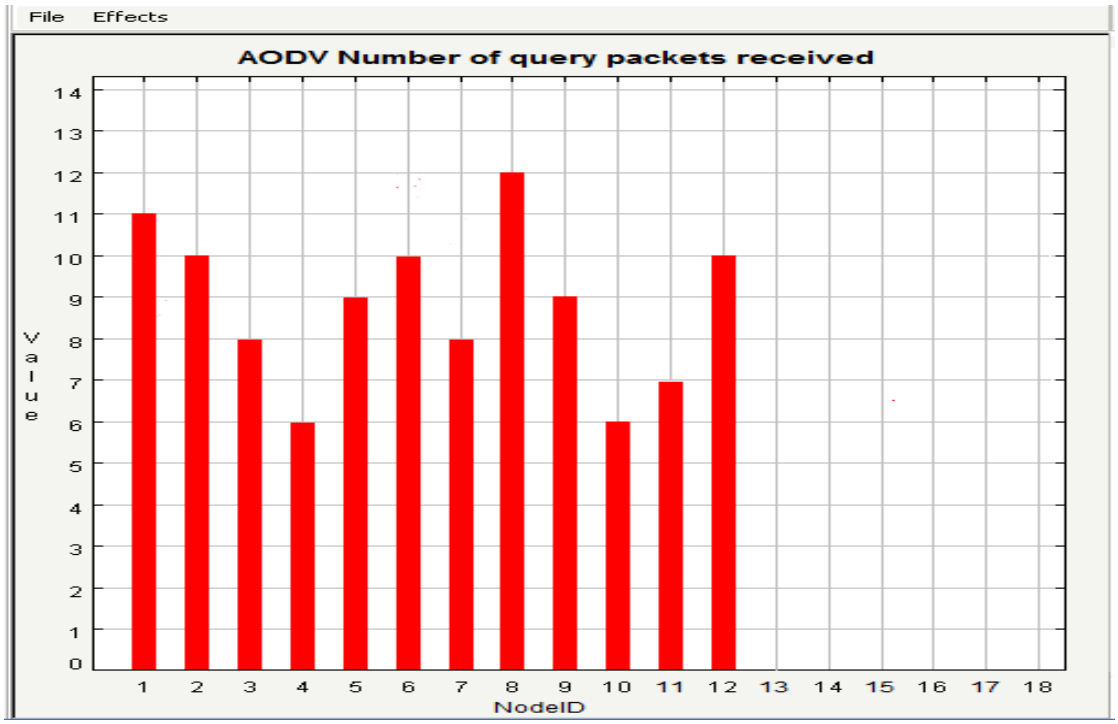

Figure4.21: Network1 with Node 12 as Wormhole Node – Number of Data Packets Received

Description- In this figure4.21, there are 18 mobile nodes in a network. There is one wormhole node in the network. Node 12 is wormhole node. The figure shows no. of query packets received by each node.

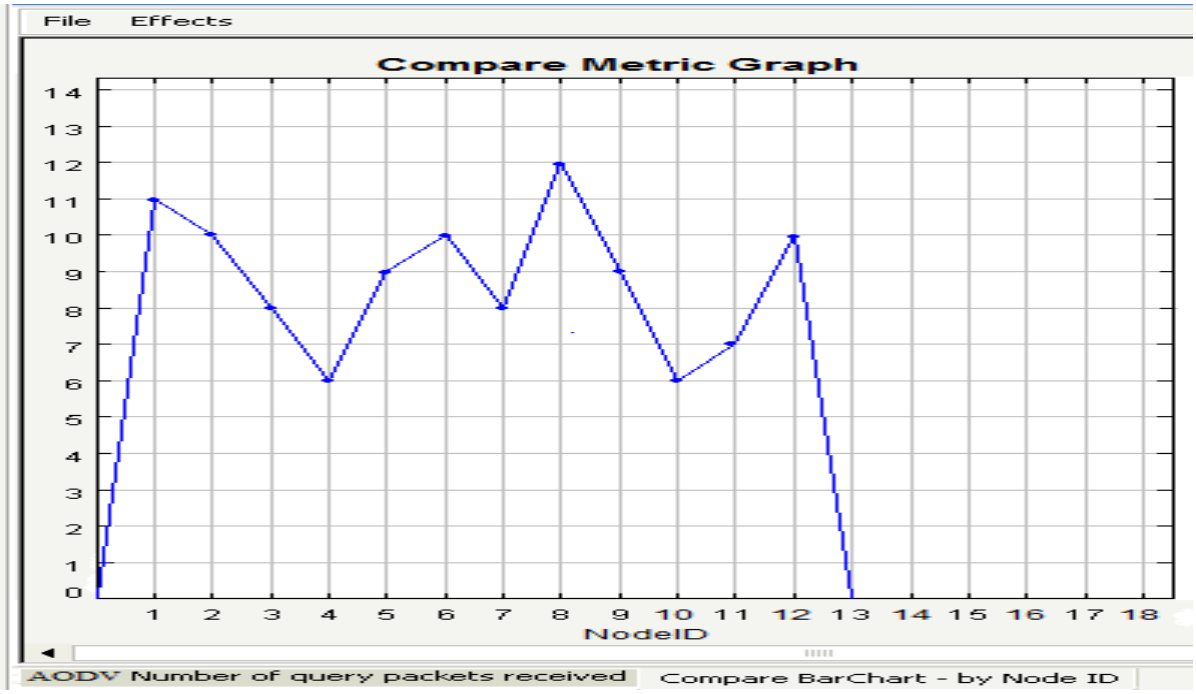

Figure4.22: Network1 with Node 12 as Wormhole Node – Number of Data Packets Received (Compare Metric Graph)

Description- This figure4.22 is a Compare Metric graph of the figure4.21.

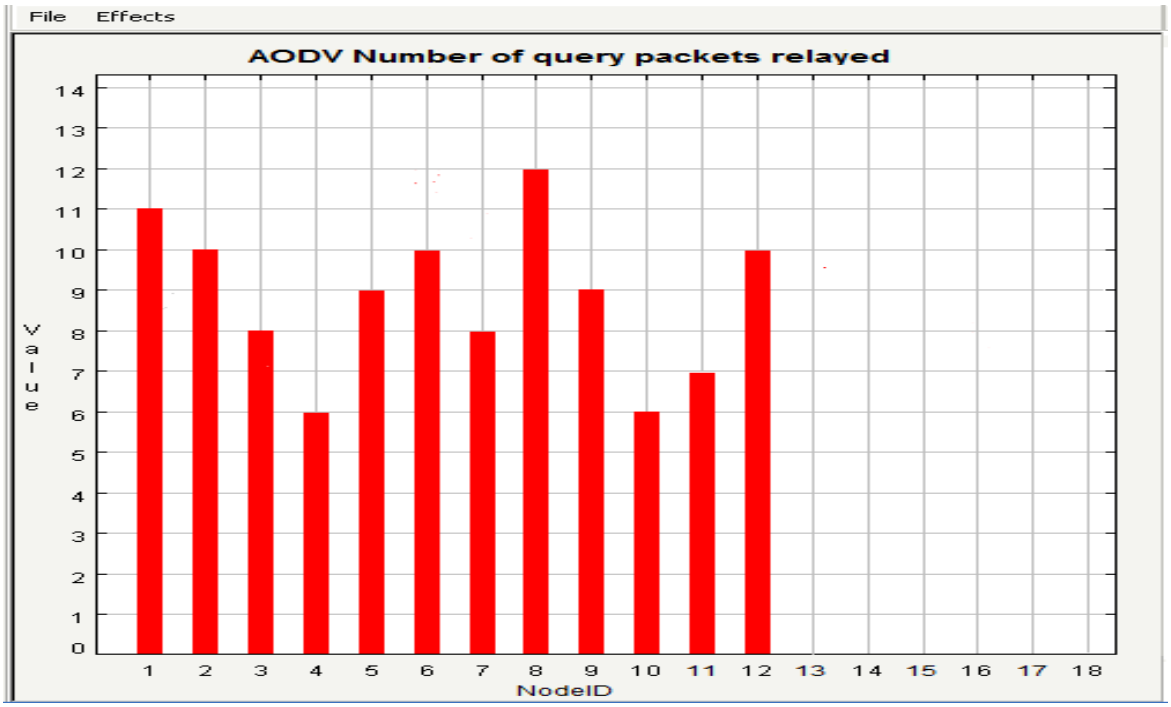

Figure4.23: Network1 with Node 12 as Wormhole Node – Number of Data Packets Relayed

Description- In this figure4.23, there are 18 mobile nodes in a network. There is one wormhole node in the network. Node 12 is wormhole node. The figure shows no. of query packets relayed by each node.

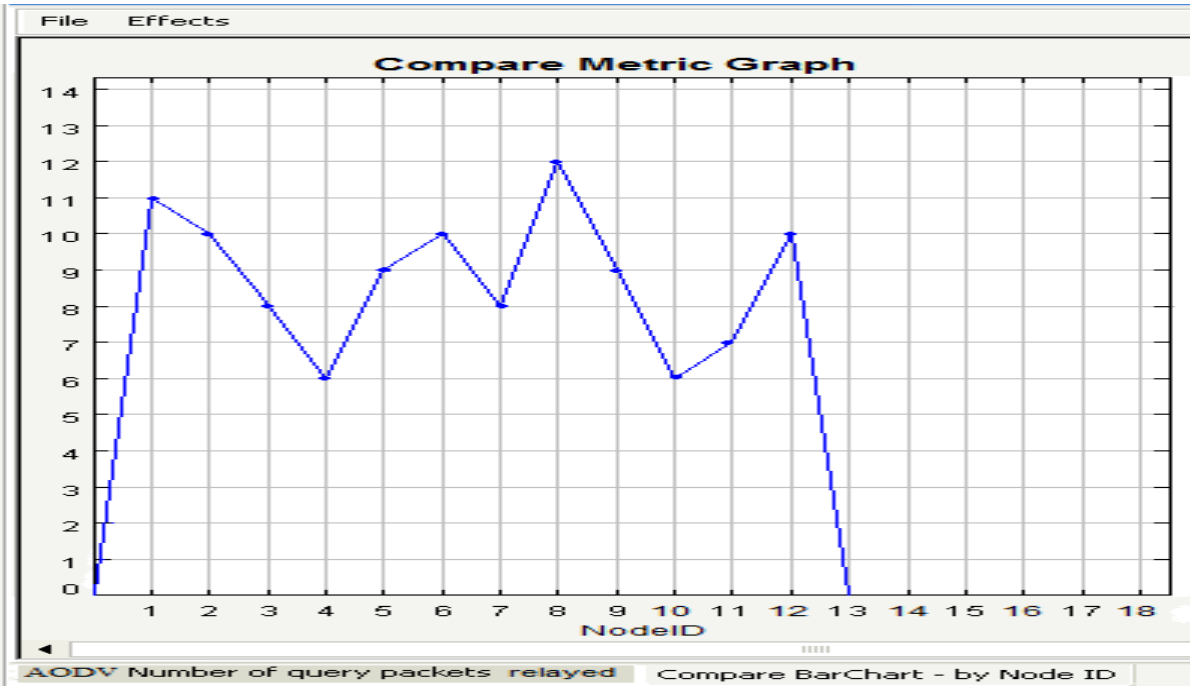

Figure4.24: Network1 with Node 12 as Wormhole Node – Number of Data Packets Relayed (Compare Metric Graph)

Description- This figure4.24 is a Compare Metric graph of the figure4.23.

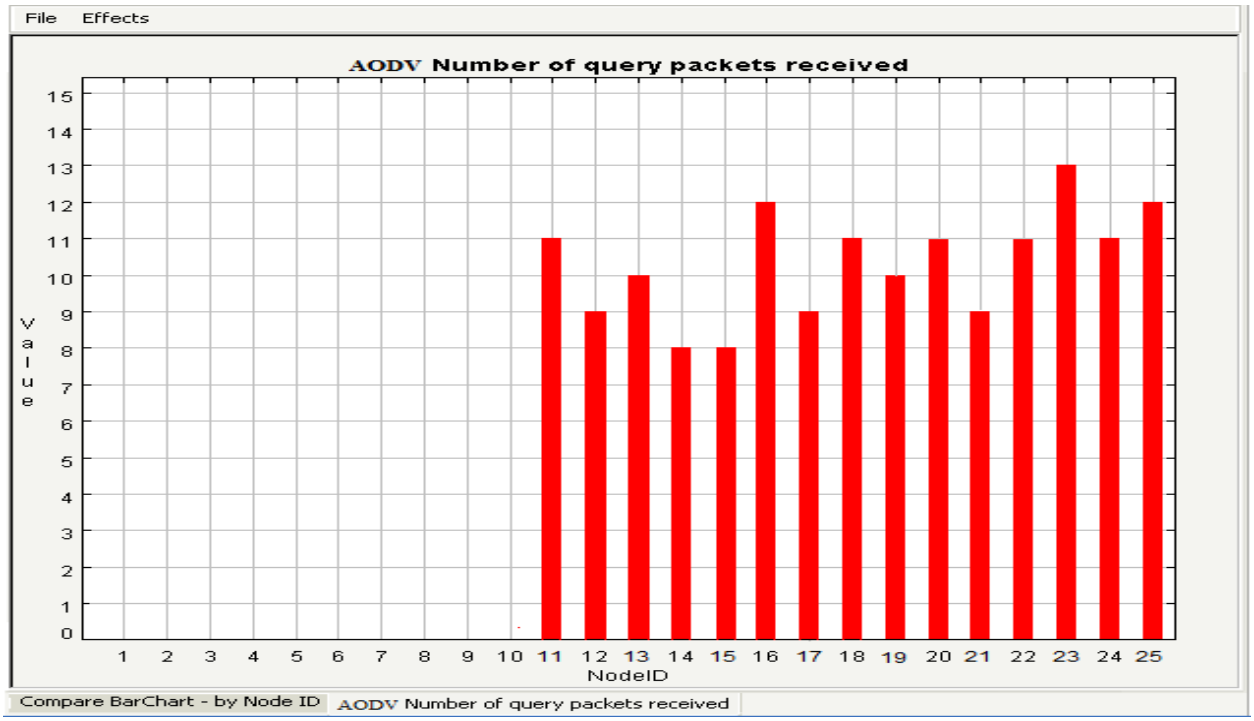

Figure4.25: Network2 with Node 11 as Wormhole Node – Number of Data Packets Received

Description- In this figure4.25, there are 25 mobile nodes in a network. There is one wormhole node in the network. Node 11 is wormhole node. The figure shows no. of query packets received by each node.

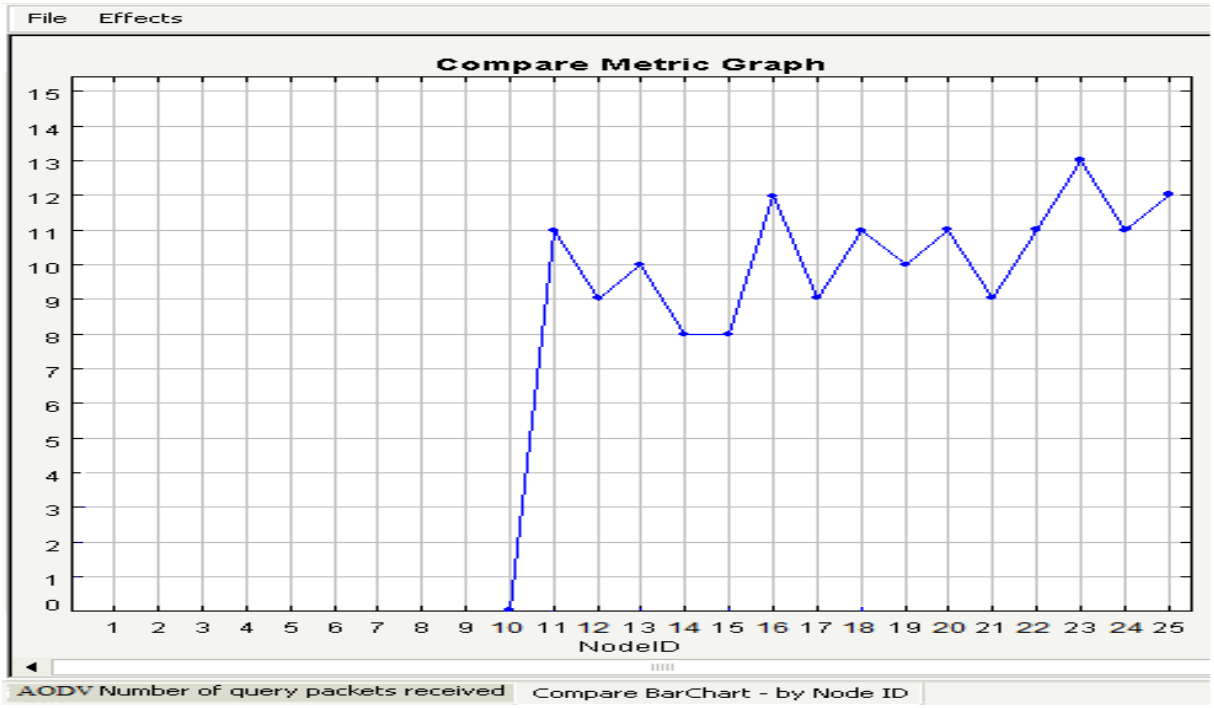

Figure4.26: Network2 with Node 11 as Wormhole Node – Number of Data Packets Received (Compare Metric Graph)

Description- This figure4.26 is a Compare Metric graph of the figure4.25.

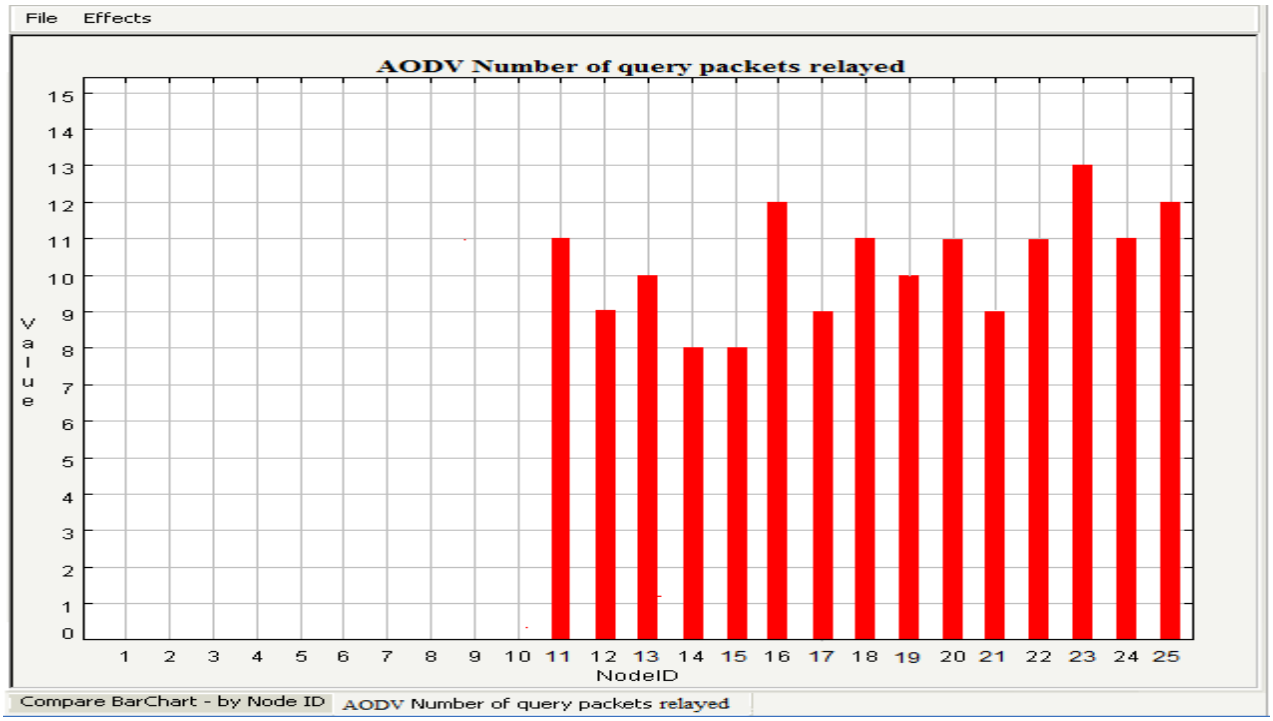

Figure4.27: Network2 with Node 11 as Wormhole Node – Number of Data Packets Relayed

Description- In this figure4.27, there are 25 mobile nodes in a network. There is one wormhole node in the network. Node 11 is wormhole node. The figure shows no. of query packets relayed by each node.

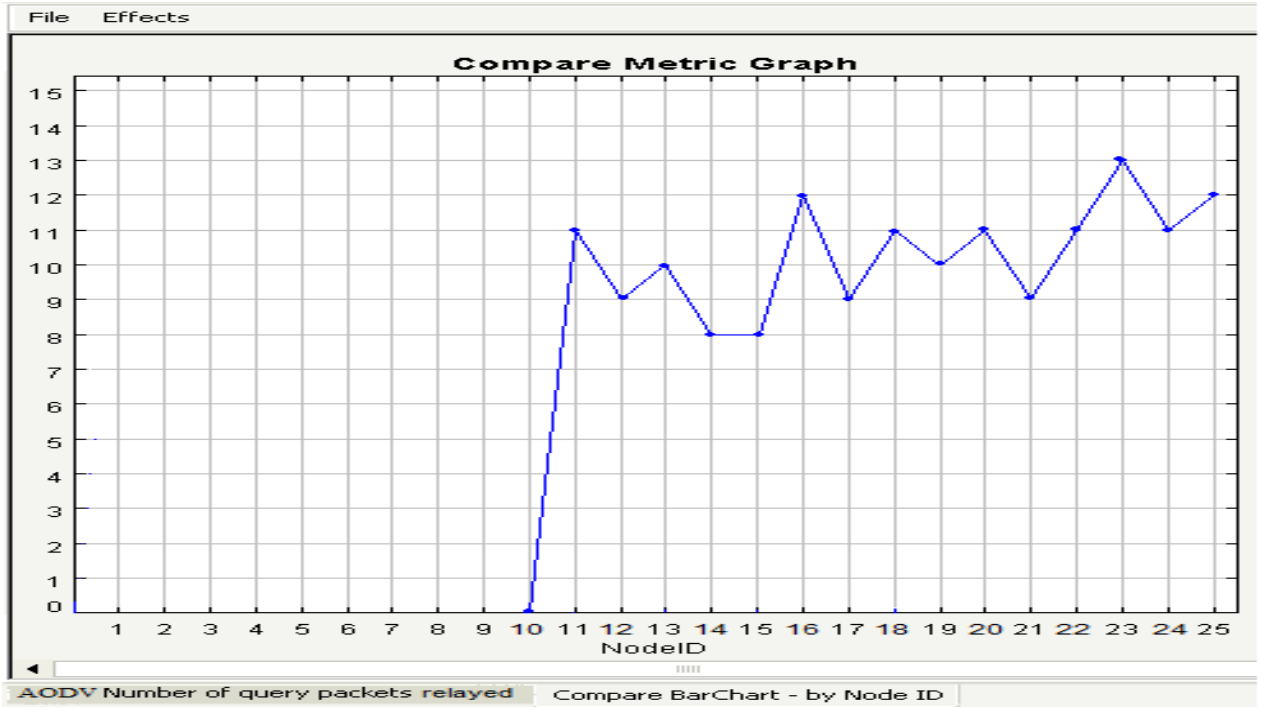

Figure4.28: Network2 with Node 11 as Wormhole Node – Number of Data Packets Relayed (Compare Metric Graph)

Description- This figure4.28 is a Compare Metric graph of the figure4.27.

4.5.6 Out-of-Band Scenario: Network Performance using SAODV with Wormhole Attack

The experiment analyzes the effectiveness of the protocol design under wormhole attack. In this experiment, varying numbers of nodes (only valid nodes are considered) are taken to check the validity of SAODV protocol and ensure that it is the sufficient and efficient approach for finding wormhole node during inter network communication. It is considered that the node with hop count (HC) =1 will be direct neighbour node for each node. In this experiment, it is analyzed that how the networks are protected from the wormhole attack if wormhole attack is taking place during wormhole attack. In this simulation, two networks are taken and each network has one wormhole node. Now, SAODV is applied to see the effect of protocol when wormhole attack is present in the network. In network 1, there are 18 nodes and node 12 is the part of wormhole attack. In network 2, there are 25 nodes and node 11 is the part of the wormhole attack. In the scenario, nodes are chosen randomly. Mobility model was random way point. Routing protocol is AODV. AODV max message buffer size = 100. In this simulation IP forwarding is enabled. This simulation executed 395632 events in real time 35.6451 seconds with 3.3743 sec spent paused. Simulation time is kept 30 sec. Results of this experiment is shown in following figures-

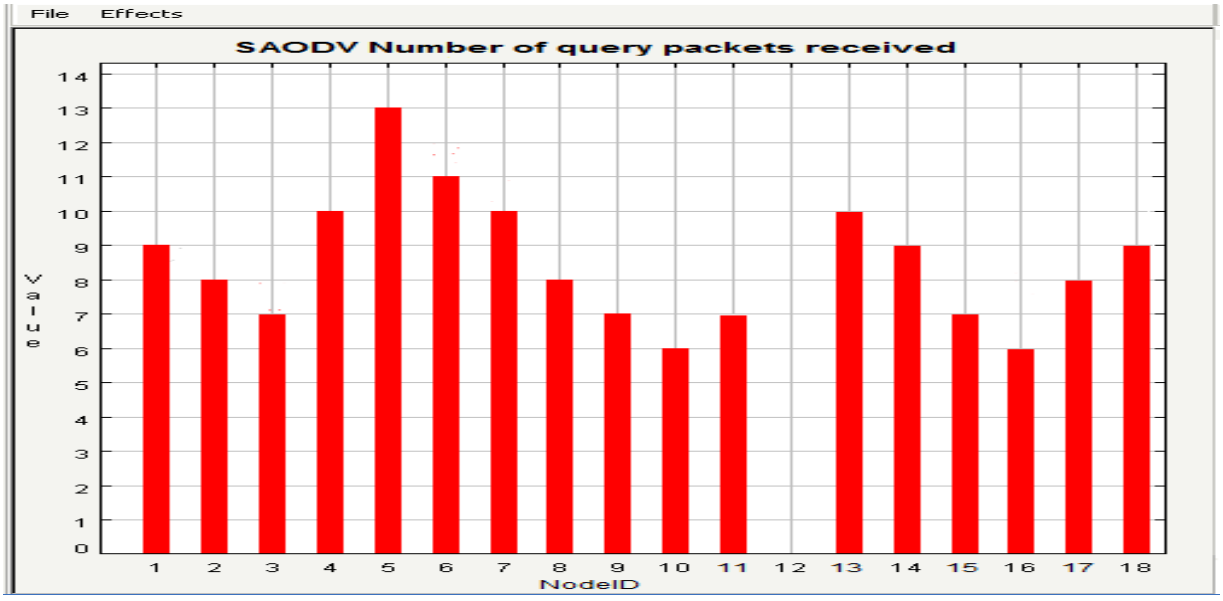

Figure4.29: Network1 with SAODV – Number of Data Packets Received

Description- In this figure4.29, there are 18 mobile nodes in a network. Node 12 is a part of wormhole attack. The figure shows no. of query packets received by each node except node 12. Node 12 is a wormhole node therefore it cannot receive any packet.

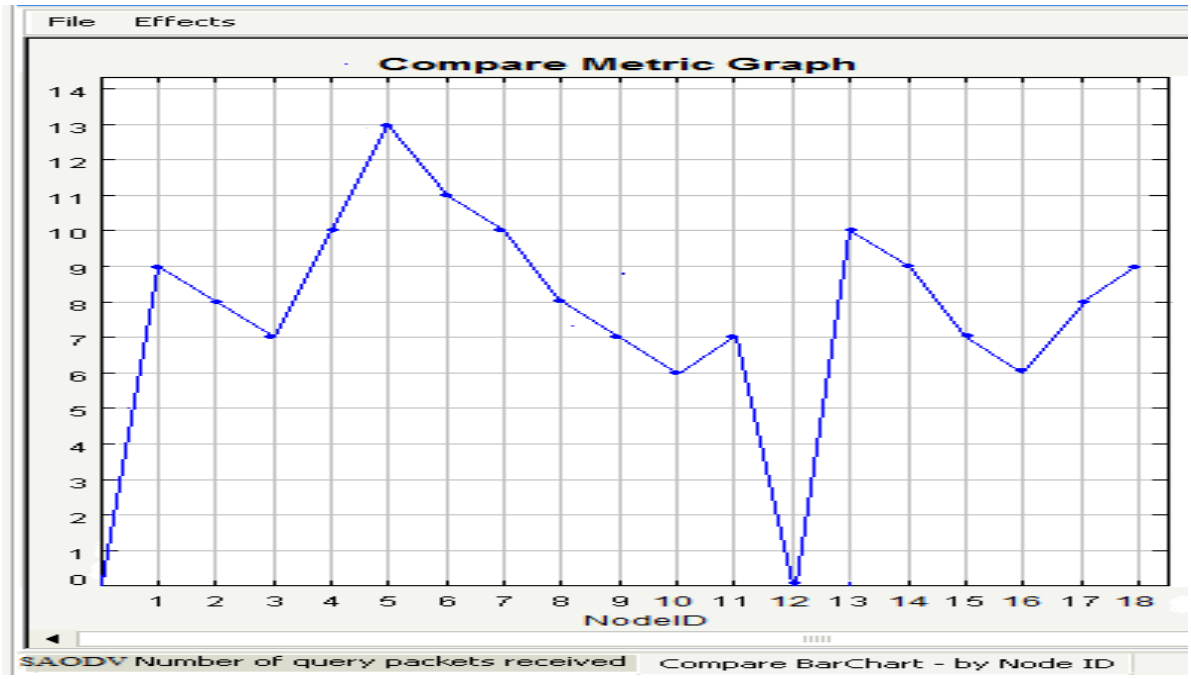

Figure4.30: Network1 with SAODV – Number of Data Packets Received (Compare Metric Graph)

Description- This figure4.30 is a Compare Metric graph of the figure4.29.

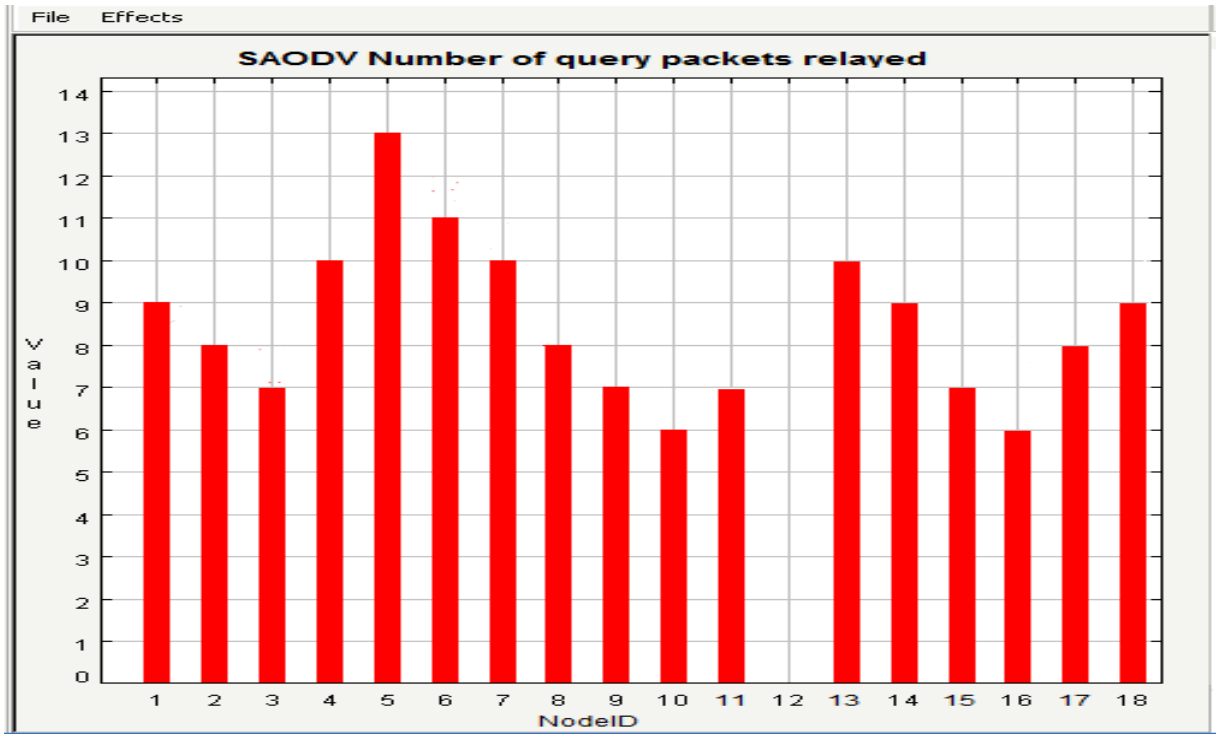

Figure4.31: Network1 with SAODV – Number of Data Packets Relayed

Description- In this figure4.31, there are 18 mobile nodes in a network 1. Node 12 is a part of wormhole node. The figure shows no. of query packets relayed by each node except node 12. Node 12 is a wormhole node therefore it cannot receive any packet and also relayed.

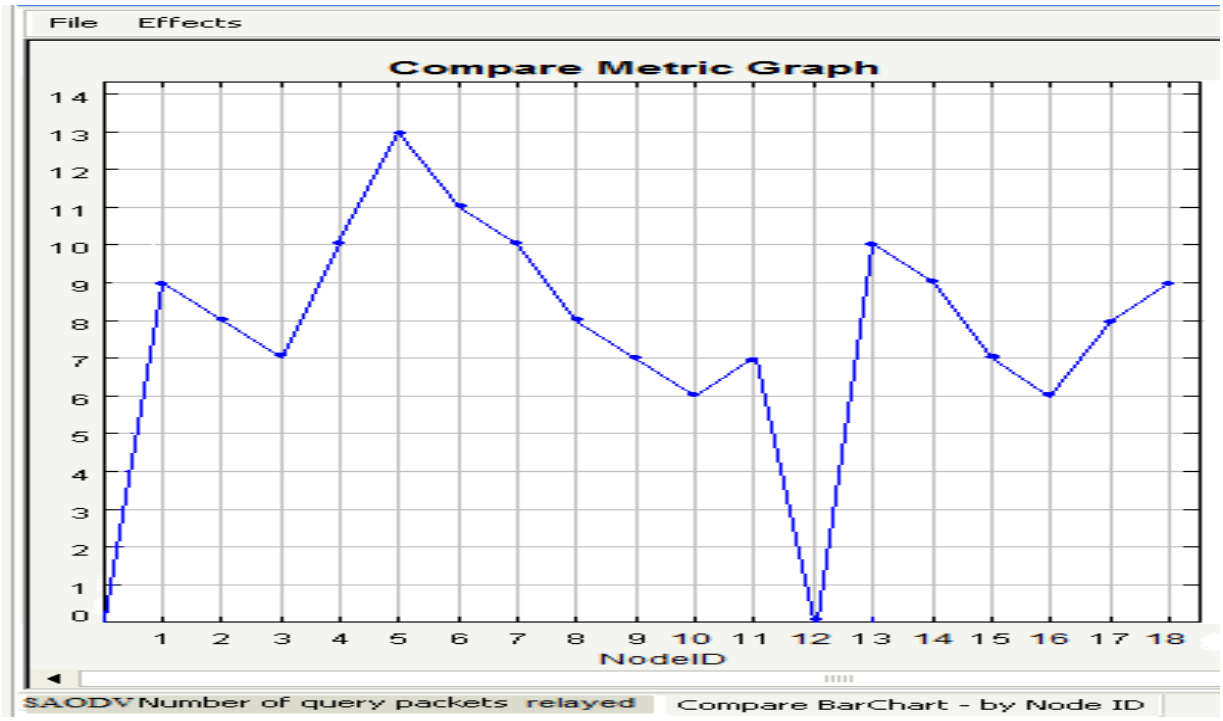

Figure4.32: Network1 with SAODV – Number of Data Packets Relayed (Compare Metric Graph)

Description- This figure4.32 is a Compare Metric graph of the figure4.31.

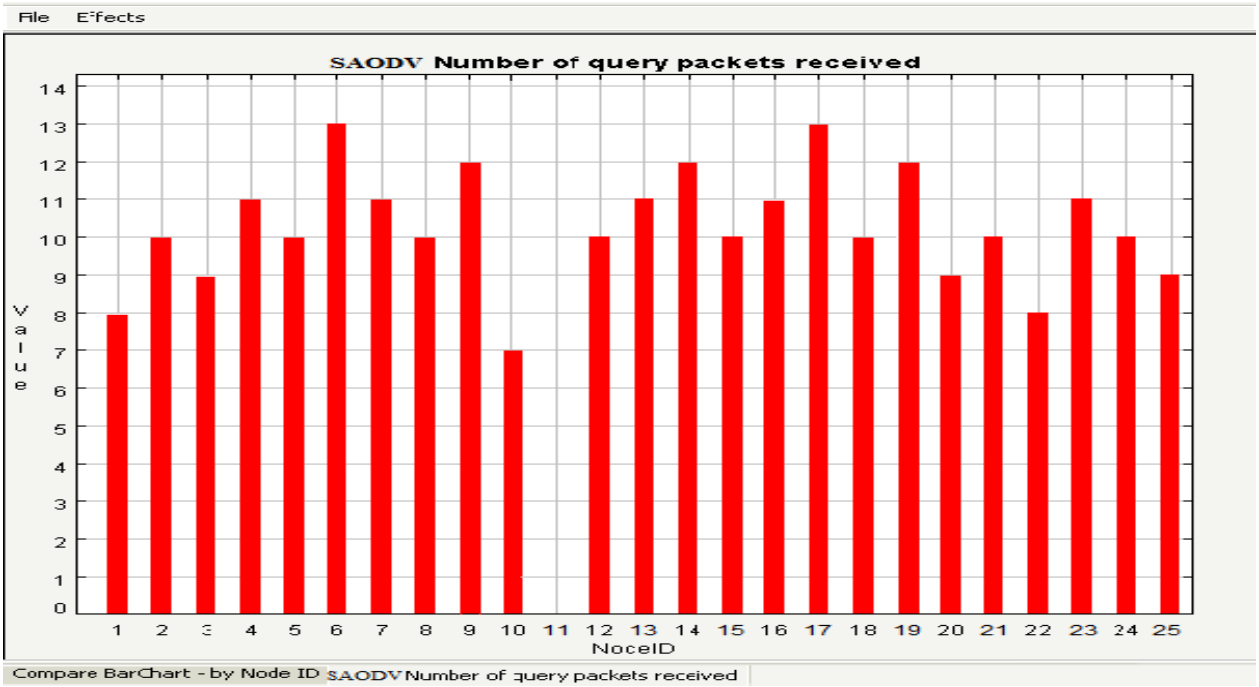

Figure4.33: Network2 with SAODV – Number of Data Packets Received

Description- In this figure4.33, there are 25 mobile nodes in network 2. Node 11 is a part of wormhole attack. The figure shows no. of query packets received by each node except node 11. Node 11 is a wormhole node therefore it cannot receive any packet.

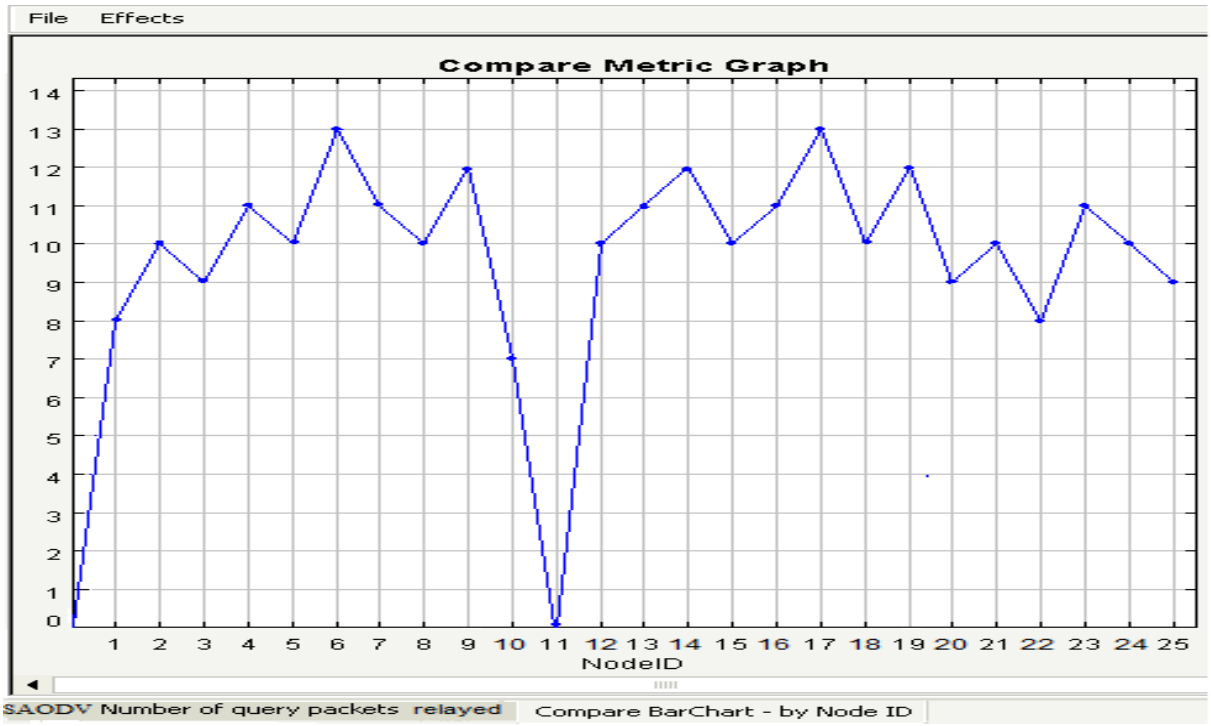

Figure4.34: Network2 with SAODV – Number of Data Packets Received (Compare Metric Graph)

Description- This figure4.34 is a Compare Metric graph of the figure4.33.

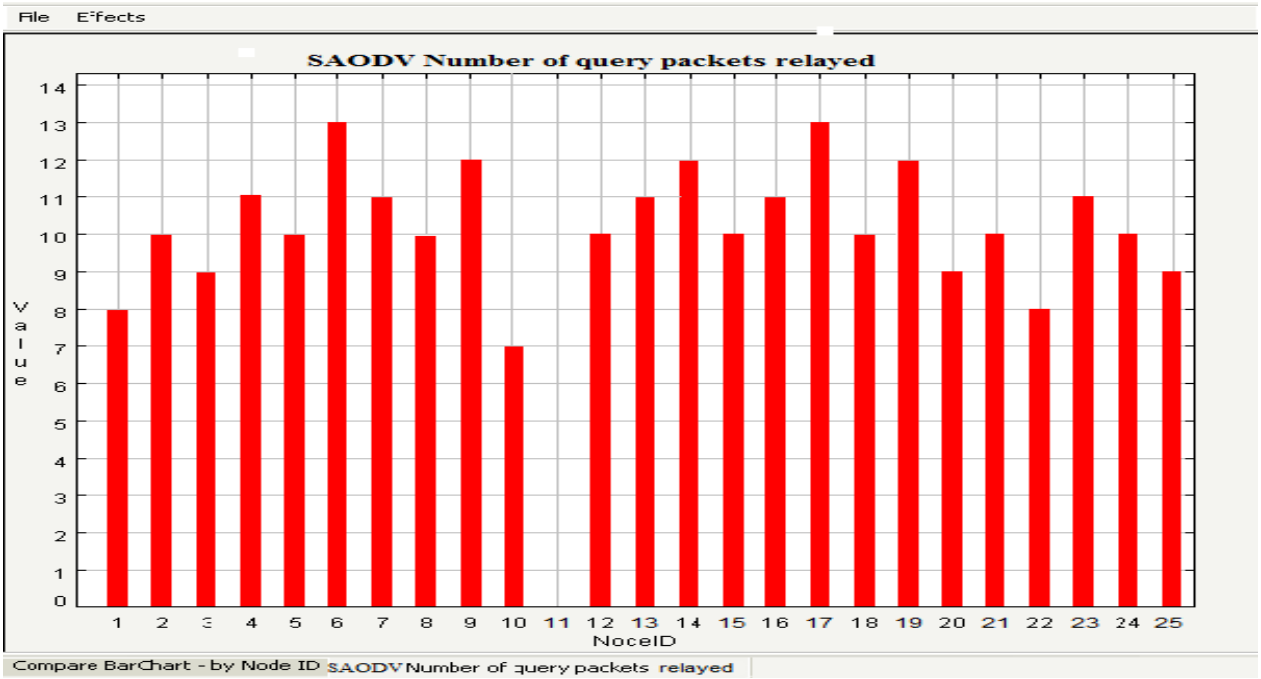

Figure4.35: Network2 with SAODV – Number of Data Packets Relayed

Description- In this figure4.35, there are 25 mobile nodes in a network. Node 11 is a part of wormhole attack. The figure shows no. of query packets relayed by each node except node 11. Node 11 is a wormhole node therefore it cannot receive any packet and relayed.

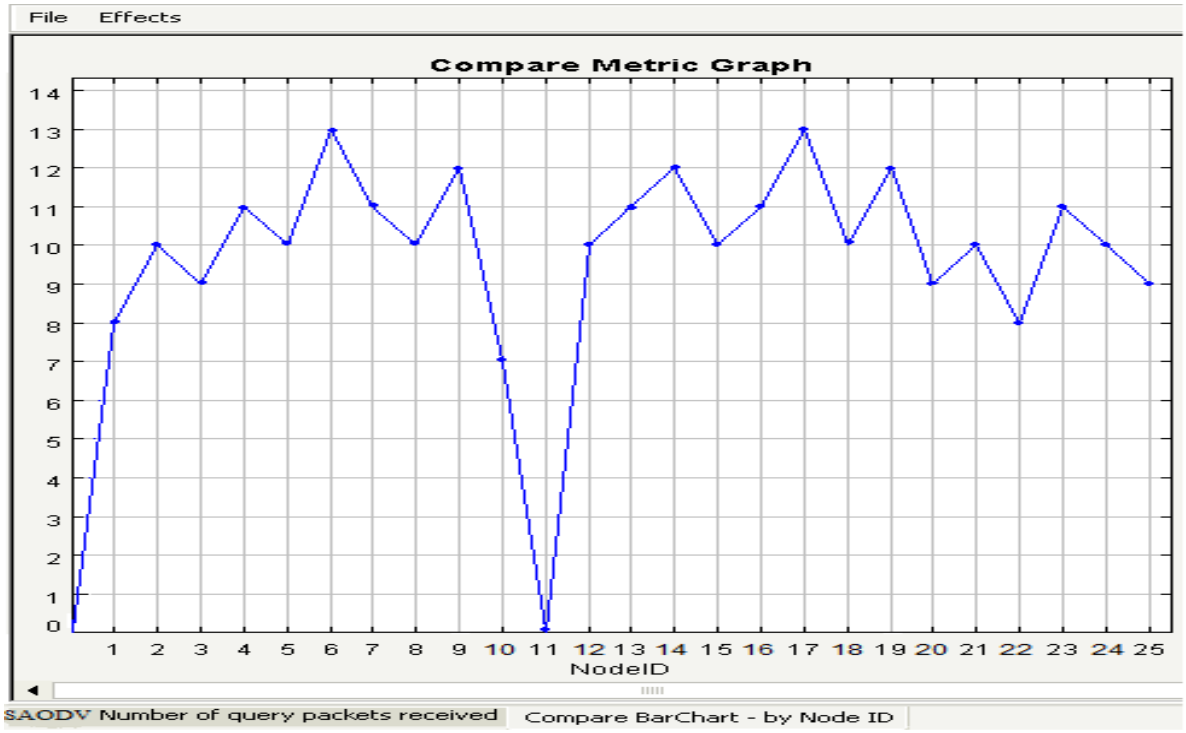

Figure4.36: Network2 with SAODV – Number of Data Packets Relayed (Compare Metric Graph)

Description- This figure4.36 is a Compare Metric graph of the figure.4.35.

4.6 Analysis

In the analysis of the results, researcher has taken two parameters. First is Packet Delivery Ratio and second is Average End-to-End Delay.

4.6.1 Packet Delivery Ratio (PDR)

In the experiment, the total number of packets successfully received at each node was first calculated. Afterwards, to compute the packet delivery ratio, the total number of packets successfully received at each node is divided by the total number of packets sent for each node and the resultant is multiplied by 100. The formula is shown below:-

$$\text{Packet Delivery Ratio (in \%)} = \frac{\text{Total No. of packets successfully received at each node}}{\text{Total No. of packets sent for each node}} * 100$$

Higher value of packet delivery ratio shows the effectiveness of the protocol in congestion. It also shows that user is experiencing better in receiving data packet. The packet delivery ratio is computed in In-Band wormhole and Out-of-Band wormhole attack, shown in figure4.37 and figure4.38:-

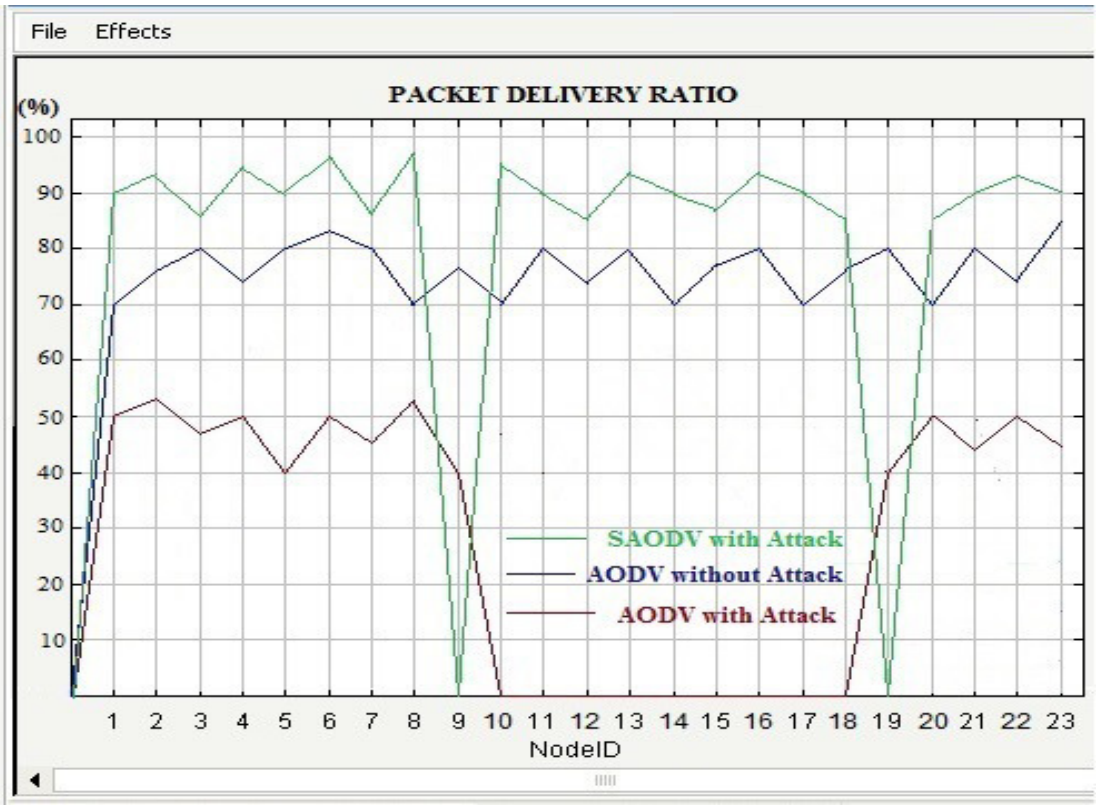

Figure4.37: Packet Delivery Ratio–In-Band Wormhole Attack

Description- In this figure4.37, there are 23 mobile nodes in a network. Packet delivery ratio is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol (shown with blue colour), second, packet delivery ratio with attack and using AODV routing protocol (shown with brown colour), and packet delivery ratio with attack and using SAODV routing protocol (shown with green colour). From the figure, it is clear that in presence of wormhole attack, the packet delivery ratio is between '40%' to '55%'. At this time, AODV routing protocol is used. Whereas, in normal condition that means no attack and using of AODV routing protocol, this ratio is between '70%' to '85%'. This ratio has increased i.e. '80%' to '95%', if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if In-Band wormhole attack is present.

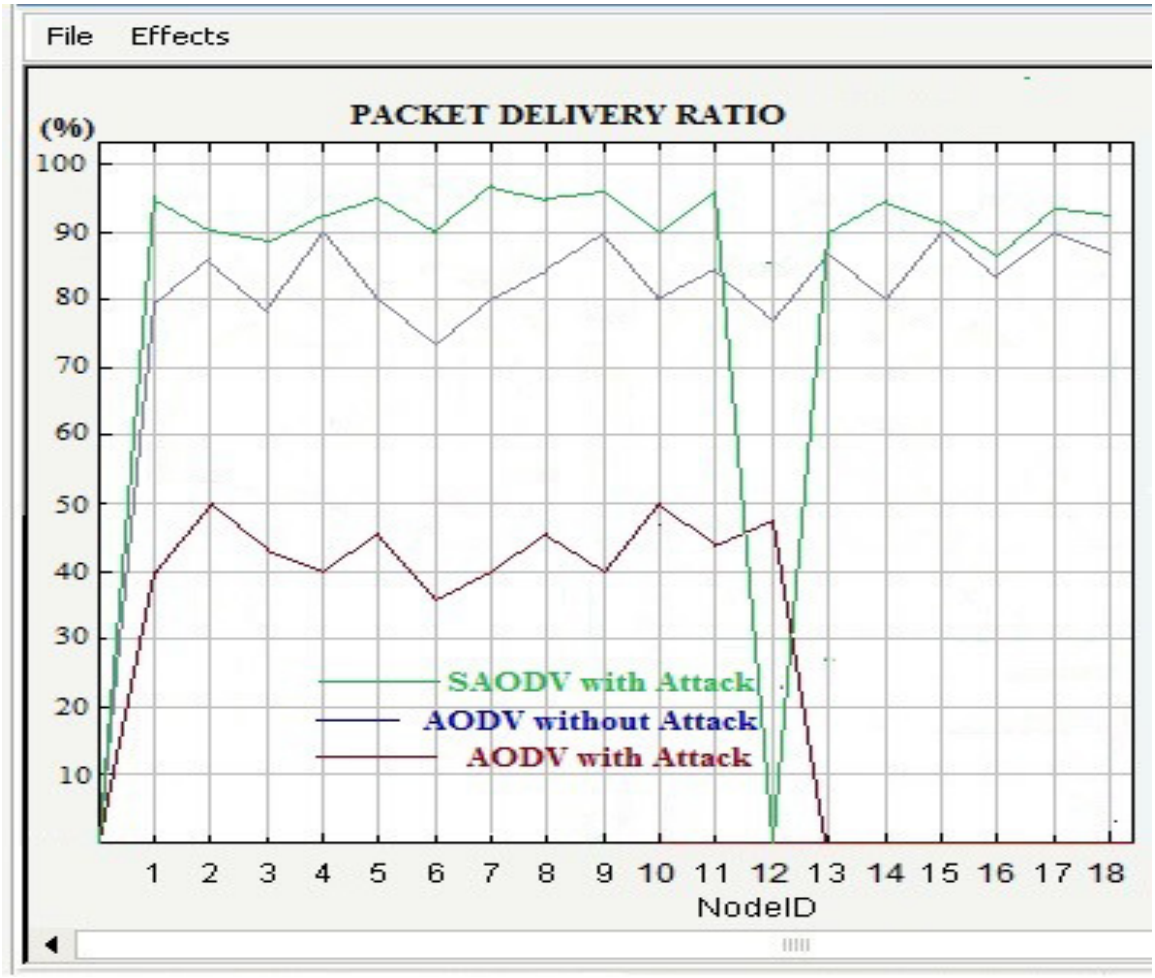

Figure4.38: Packet Delivery Ratio (Network1)–Out-of-Band Wormhole Attack

Description- This figure4.38 and next figure4.39 show the collaborative function of Network 1 and Network 2. In this figure, there are 18 mobile nodes in Network1. Packet delivery ratio is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol (shown with blue colour), second, packet delivery ratio with attack and using AODV routing protocol (shown with brown colour), and packet delivery ratio with attack and using SAODV routing protocol (shown with green colour). From the figure, it is clear that in presence of wormhole attack, the packet delivery ratio is between '35%' to '50%'. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this ratio is between '75%' to '90%'. This ratio has increased i.e. '85%' to '95%', if SAODV is used in presence of Out-of-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if Out-of-Band wormhole attack is present.

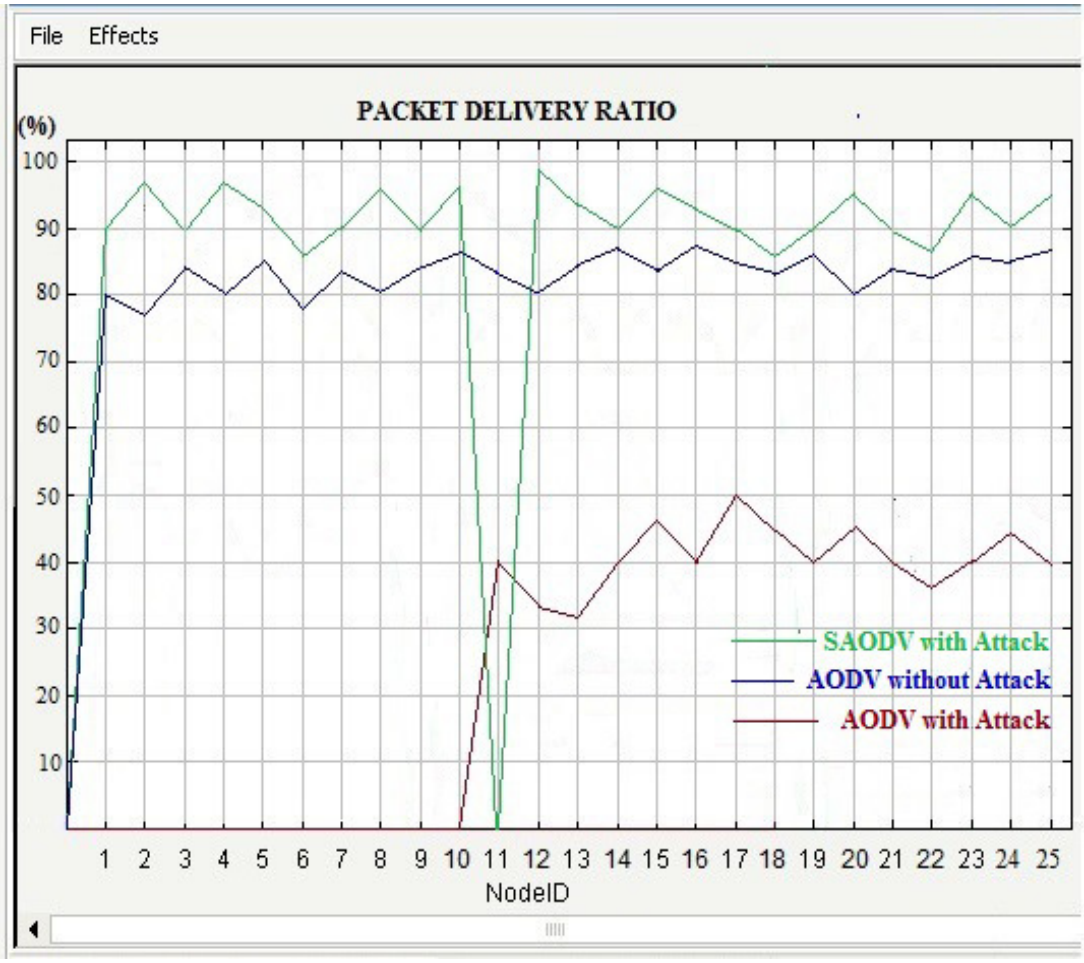

Figure4.39: Packet Delivery Ratio (Network2)–Out-of-Band Wormhole Attack

Description- In this figure4.39, there are 25 mobile nodes in Network2. Packet delivery ratio is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol (shown with blue colour), second, packet delivery ratio with attack and using AODV routing protocol (shown with brown colour), and packet delivery ratio with attack and using SAODV routing protocol (shown with green colour). From the figure, it is clear that in presence of wormhole attack, the packet delivery ratio is between '30%' to '50%'. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this ratio is between '75%' to '85%'. This ratio has increased i.e. '85%' to '98%', if SAODV is used in presence of Out-of-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if Out-of-Band wormhole attack is present.

4.6.2 Average End-to-End Delay

The average time that a packet takes to traverse the network is called End-to-End delay. In other words, the average time taken by a data packet to reach from source node to destination node is an average end-to-end delay. It is measured in seconds. Average end-to-end delay includes all the delays in the network such as transmission time, buffer queues, MAC control exchanges and delays induced by routing activities. It can be vary according to the use of applications. If there is a requirement of sending voice data than average delay should be low in the network. Node mobility, packet retransmissions due to weak signal strengths between nodes, and connection tearing and making are the prime characteristics of MANETs. Due to all these characteristics, delay in the network mostly is increased. The End-to-End delay therefore represents the reliability of the routing protocol.

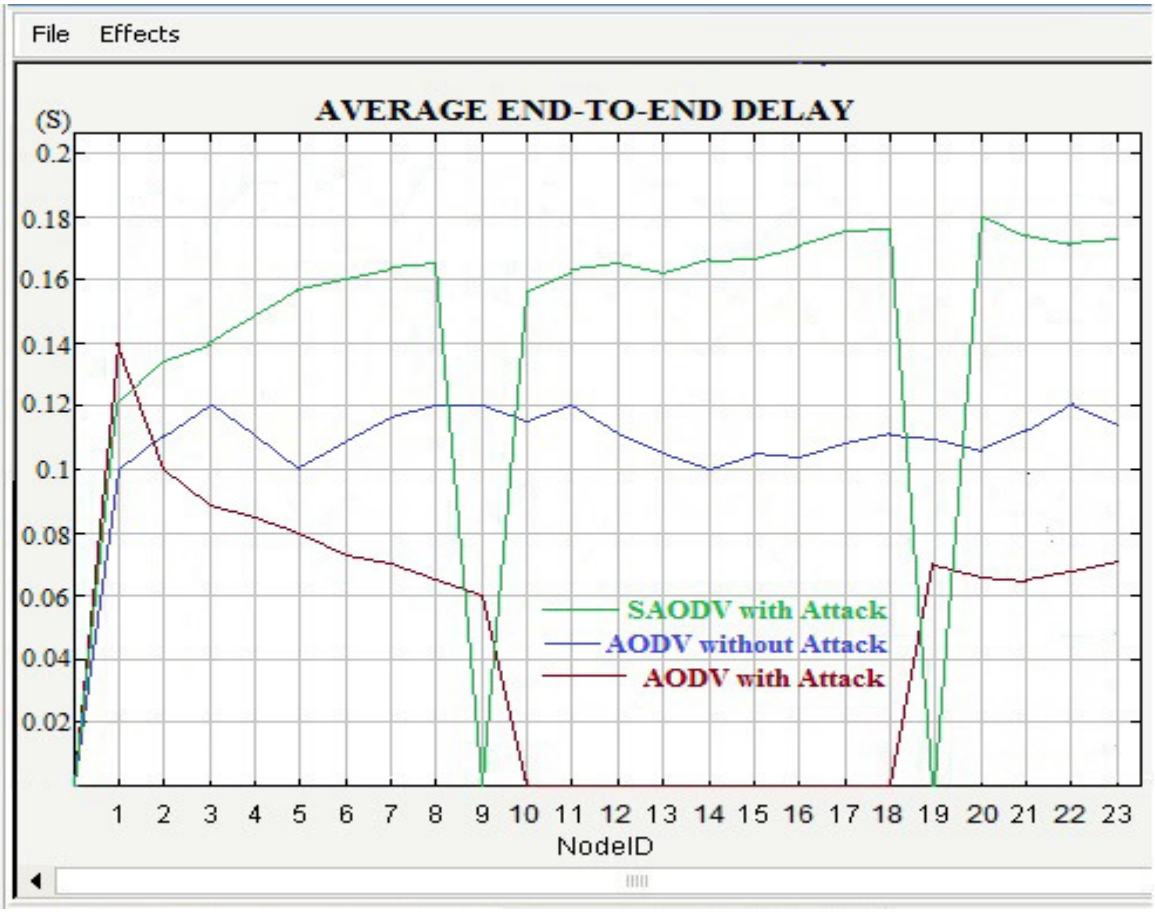

Figure4.40: Average End-to-End Delay–In-Band Wormhole Attack

Description- In this figure4.40, there are 23 mobile nodes in a network. Average End-to-End Delay is shown with three conditions, first, packet delivery ratio without attack and using

AODV routing protocol (shown with blue colour), second, packet delivery ratio with attack and using AODV routing protocol (shown with brown colour), and packet delivery ratio with attack and using SAODV routing protocol (shown with green colour). From the figure, it is clear that in presence of wormhole attack, the Average End-to-End Delay is between '0.06' sec to '0.12' sec. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this delay is between '0.1' sec to '0.12' sec. This delay has increased i.e. '0.12' sec to '0.18' sec, if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if In-Band wormhole attack is present.

Figure4.41: Average End-to-End Delay (Network 1)–Out-of-Band Wormhole Attack

Description- This figure4.41 and next figure4.42 show the collaborative function of Network 1 and Network 2. In this figure, there are 18 mobile nodes in Network1. Average End-to-End Delay is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol (shown with blue colour), second, packet delivery ratio with attack

and using AODV routing protocol (shown with brown colour), and packet delivery ratio with attack and using SAODV routing protocol (shown with green colour). From the figure, it is clear that in presence of wormhole attack, the Average End-to-End Delay is between '0.08' sec to '0.1' sec. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this delay is between '0.12' sec to '0.16' sec. This delay has increased i.e. '0.12' sec to '0.18' sec, if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if Out-of-Band wormhole attack is present.

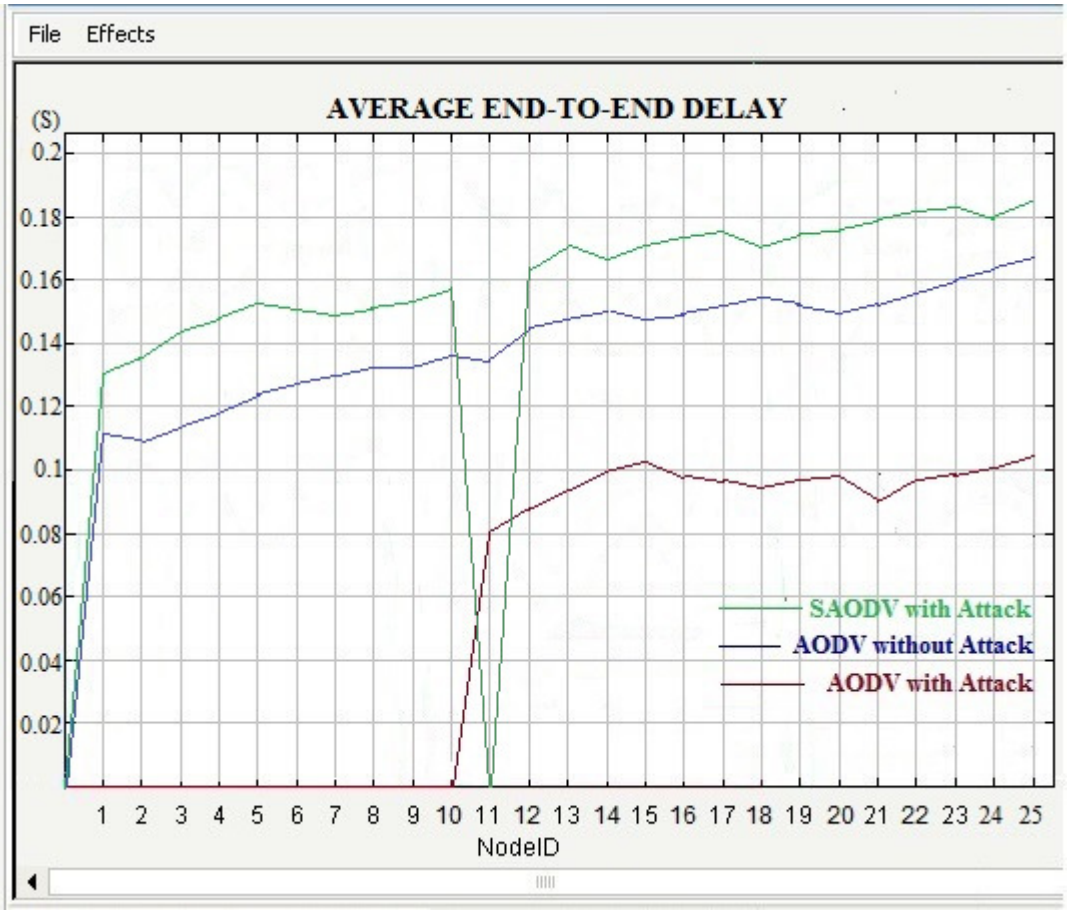

Figure4.42: Average End-to-End Delay (Network 2)–Out-of-Band Wormhole Attack

Description- In this figure4.42, there are 25 mobile nodes in Network2. Average End-to-End Delay is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol (shown with blue colour), second, packet delivery ratio with attack and using AODV routing protocol (shown with brown colour), and packet delivery ratio with attack and using SAODV routing protocol (shown with green colour). From the figure, it is

clear that in presence of wormhole attack, the Average End-to-End Delay is between ‘0.08’ sec to ‘0.1’ sec. At this time, AODV routing protocol is used. Whereas in normal condition, that means no attack and using of AODV routing protocol, this delay is between ‘0.1’ sec to ‘0.16’ sec. This delay has increased i.e. ‘0.12’ sec to ‘0.2’ sec, if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if out-of-Band wormhole attack is present.

4.7 Comparative Analysis

To assess whether the proposed approach is able to improve the network performance with added security feature, there is a requirement of comparative analysis on different scenarios. As previous scenario set up, three conditions have been taken. These are 1) Ad hoc Network with no Attack, 2) Ad hoc Network with Attack using AODV and 3) Ad hoc Network with Attack using SAODV. All the three conditions are implemented to compare the performance of the AODV and SAODV under wormhole attack. The results of collected data for security are tabulated in the next section with respect to in-band wormhole attack and out-of-band attack.

4.7.1 Comparative Analysis of In-Band Wormhole Attack: Packets Received & Relayed

To see whether the proposed approach is able to stop wormhole nodes in receiving or relaying data packets, a comparative analysis has been done. The results of collected data for security are tabulated in Table4.2

Node ID	Number of Packets Received & Relayed					
	In-Band Scenarios					
	With No Attack & Using AODV (Scenario 1)		With Attack & Using AODV (Scenario 2)		With Attack & Using SAODV (Scenario 3)	
	Received	Relayed	Received	Relayed	Received	Relayed
1	70	70	110	110	90	90
2	80	80	100	100	100	100
3	60	60	90	90	110	110
4	90	90	110	110	110	110
5	130	130	120	120	120	120

6	110	110	130	130	130	130
7	100	100	120	120	120	120
8	80	80	90	90	110	110
9	50	50	110	110	0	0
10	40	40	0	0	70	70
11	80	80	0	0	90	90
12	80	80	0	0	100	100
13	110	110	0	0	110	110
14	100	100	0	0	130	130
15	80	80	0	0	100	100
16	70	70	0	0	120	120
17	90	90	0	0	130	130
18	100	100	0	0	120	120
19	70	70	100	100	0	0
20	90	90	110	110	90	90
21	80	80	90	90	100	100
22	70	70	110	110	80	80
23	80	80	130	130	110	110
24	NIL	NIL	110	110	100	100
25	NIL	NIL	120	120	90	90
Total	**1910**	**1910**	**1750**	**1750**	**2430**	**2430**

Table4.2: Comparative Analysis of In-Band Scenarios: Packets Received & Relayed

From the table 4.2, it is clear that in normal situation (scenario 1) when no attack is present and used routing protocol is AODV, all the available nodes in the network are receiving and relaying data packet without any interruption. In the scenario 2, there is wormhole attack available and routing protocol is AODV. From the data present in the table, it is clear that in scenario 2, nodes 10, 11, 12, 13, 14, 15, 16, 17, 18 are not receiving any data packet that means they are not taking part in the routing process. This is due to wormhole nodes 9 and 19, present in the network. In the scenario 3, SAODV is used in presence of wormhole attack in the network. From the data record available in the table, it is clear that all nodes in the network are smoothly receiving and relaying data packets.

4.7.2 Comparative Analysis of Out-of-Band Wormhole Attack for Network1: Packets Received & Relayed

To see whether the proposed approach is able to stop wormhole nodes in receiving or relaying data packets, a comparative analysis has been done. The results of collected data for security are tabulated in Table4.3.

Node ID	Number of Packets Received & Relayed					
	Out-of-Band Scenarios (Network1)					
	With No Attack & Using AODV (Scenario 1)		With Attack & Using AODV (Scenario 2)		With Attack & Using SAODV (Scenario 3)	
	Received	Relayed	Received	Relayed	Received	Relayed
1	60	60	110	110	90	90
2	80	80	100	100	80	80
3	50	50	80	80	70	70
4	90	90	60	60	100	100
5	120	120	90	90	130	130
6	100	100	100	100	110	110
7	90	90	80	80	100	100
8	70	70	120	120	80	80
9	50	50	90	90	70	70
10	40	40	60	60	60	60
11	70	70	70	70	70	70
12	80	80	100	100	0	0
13	100	100	0	0	100	100
14	90	90	0	0	90	90
15	70	70	0	0	70	70
16	60	60	0	0	60	60
17	80	80	0	0	80	80
18	90	90	0	0	90	90
Total	**1390**	**1390**	**1060**	**1060**	**1450**	**1450**

Table4.3: Comparative Analysis of Out-of-Band Scenarios for Network1: Packets Received & Relayed

From the table 4.3, it is clear that in normal situation (scenario 1) when no attack is present and used routing protocol is AODV, all the available nodes in the network are receiving and relaying data packet without any interruption. In the scenario 2, there is wormhole attack available and routing protocol is AODV. From the data present in the table, it is clear that in scenario 2, nodes 13, 14, 15, 16, 17, 18 are not receiving any data packet that means they are not taking part in the routing process. This is due to wormhole node 12,

present in the network. In the scenario 3, SAODV is used in presence of wormhole attack in the network. From the data record available in the table, it is clear that all nodes in the network are smoothly receiving and relaying data packets.

4.7.3 Comparative Analysis of Out-of-Band Wormhole Attack for Network2: Packets Received & Relayed

To see whether the proposed approach is able to stop wormhole nodes in receiving or relaying data packets, a comparative analysis has been done. The results of collected data for security are tabulated in Table4.4

Node ID	Number of Packets Received & Relayed					
	Out-of-Band Scenarios (Network 2)					
	With No Attack & Using AODV (Scenario 1)		With Attack & Using AODV (Scenario 2)		With Attack & Using SAODV (Scenario 3)	
	Received	Relayed	Received	Relayed	Received	Relayed
1	110	110	0	0	80	80
2	90	90	0	0	100	100
3	60	60	0	0	90	90
4	100	100	0	0	110	110
5	120	120	0	0	100	100
6	100	100	0	0	130	130
7	130	130	0	0	110	110
8	100	100	0	0	100	100
9	80	80	0	0	120	120
10	80	80	0	0	70	70
11	70	70	110	110	0	0
12	80	80	90	90	100	100
13	90	90	100	100	110	110
14	100	100	80	80	120	120
15	80	80	80	80	100	100
16	70	70	120	120	110	110
17	90	90	90	90	130	130
18	80	80	110	110	100	100
19	70	70	100	100	120	120
20	90	90	110	110	90	90
21	80	80	90	90	100	100
22	70	70	110	110	80	80
23	80	80	130	130	110	110
24	NIL	NIL	110	110	100	100
25	NIL	NIL	120	120	90	90

Total	**2020**	**2020**	**1550**	**1550**	**2470**	**2470**

Table4.4: Comparative Analysis of Out-of-Band Scenarios for Network2: Packets Received & Relayed

From the table 4.4, it is clear that in normal situation (scenario 1) when no attack is present and used routing protocol is AODV, all the available nodes in the network are receiving and relaying data packet without any interruption. In the scenario 2, there is wormhole attack available and routing protocol is AODV. From the data present in the table, it is clear that in scenario 2, nodes 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 are not receiving any data packet that means they are not taking part in the routing process. This is due to wormhole node 11, present in the network. In the scenario 3, SAODV is used in presence of wormhole attack in the network. From the data record available in the table, it is clear that all nodes in the network are smoothly receiving and relaying data packets.

4.7.4 Comparative Analysis of In-Band Wormhole Attack: Packet Delivery Ratio

To see whether the proposed approach is able to stop wormhole nodes in receiving or relaying data packets, a comparative analysis has been done. The results of collected data for security are tabulated in Table4.5.

Node ID	Packet Delivery Ratio (%)		
	In-Band Scenarios		
	With No Attack & Using AODV (Scenario 1)	With Attack & Using AODV (Scenario 2)	With Attack & Using SAODV (Scenario 3)
1	70	50	90
2	77	52	93
3	80	48	88
4	72	50	94
5	80	40	90
6	81	50	97
7	80	47	89
8	70	52	97
9	77	40	0
10	70	0	96
11	80	0	90
12	75	0	88
13	80	0	93

14	70	0	90
15	78	0	88
16	80	0	92
17	70	0	90
18	78	0	86
19	80	40	0
20	70	50	87
21	80	45	90
22	76	50	92
23	82	45	90

Table4.5: Comparative Analysis of In-Band Scenarios: Packet Delivery Ratio

From the table 4.5, it is clear that in presence of wormhole attack, the packet delivery ratio is between '40%' to '55%'. At this time, AODV routing protocol is used. Whereas, in normal condition that means no attack and using of AODV routing protocol, this ratio is between '70%' to '85%'. This ratio has increased i.e. '80%' to '95%', if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if In-Band wormhole attack is present.

4.7.5 Comparative Analysis of Out-of-Band Wormhole Attack for Network1: Packet Delivery Ratio

To see whether the proposed approach is able to stop wormhole nodes in receiving or relaying data packets, a comparative analysis has been done. The results of collected data for security are tabulated in Table4.6.

Node ID	Packet Delivery Ratio (%)		
	Out-of-Band Scenarios (Network1)		
	With No Attack & Using AODV (Scenario 1)	With Attack & Using AODV (Scenario 2)	With Attack & Using SAODV (Scenario 3)
1	80	40	94
2	88	50	90
3	79	43	89
4	90	40	92
5	80	46	94
6	72	38	90
7	80	40	96
8	84	45	95

9	90	40	96
10	80	50	90
11	83	43	94
12	78	48	0
13	88	0	90
14	80	0	92
15	90	0	91
16	83	0	88
17	90	0	92
18	88	0	91

Table4.6: Comparative Analysis of Out-of-Band Scenarios for Network1: Packet Delivery Ratio

From the table 4.6, it is clear that in presence of wormhole attack, the packet delivery ratio is between '35%' to '50%'. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this ratio is between '75%' to '90%'. This ratio has increased i.e. '85%' to '95%', if SAODV is used in presence of Out-of-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if Out-of-Band wormhole attack is present.

4.7.6 Comparative Analysis of Out-of-Band Wormhole Attack for Network2: Packet Delivery Ratio

To see whether the proposed approach is able to stop wormhole nodes in receiving or relaying data packets, a comparative analysis has been done. The results of collected data for security are tabulated in Table4.7.

Node ID	Packet Delivery Ratio (%)		
	Out-of-Band Scenarios (Network2)		
	With No Attack & Using AODV (Scenario 1)	With Attack & Using AODV (Scenario 2)	With Attack & Using SAODV (Scenario 3)
1	80	0	90
2	78	0	95
3	82	0	90
4	80	0	95
5	83	0	93
6	78	0	87
7	82	0	90
8	80	0	95

9	83	0	90
10	88	0	95
11	82	40	0
12	80	33	98
13	84	31	92
14	88	40	90
15	85	46	95
16	88	40	92
17	84	50	90
18	82	45	88
19	86	40	90
20	80	45	93
21	82	40	90
22	81	37	88
23	86	40	94
24	85	44	90
25	87	40	94

Table4.7: Comparative Analysis of Out-of-Band Scenario for Network2: Packet Delivery Ratio

From the table 4.7, it is clear that in presence of wormhole attack, the packet delivery ratio is between '30%' to '50%'. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this ratio is between '75%' to '85%'. This ratio has increased i.e. '85%' to '98%', if SAODV is used in presence of Out-of-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if Out-of-Band wormhole attack is present.

4.7.7 Comparative Analysis of In-Band Wormhole Attack: Average End-to-End Delay

To see whether the proposed approach is able to stop wormhole nodes in receiving or relaying data packets, a comparative analysis has been done. The results of collected data for security are tabulated in Table4.8.

Node ID	Average End-to-End Delay (s)		
	In-Band Scenarios		
	With No Attack & Using AODV (Scenario 1)	With Attack & Using AODV (Scenario 2)	With Attack & Using SAODV (Scenario 3)
1	0.1	0.14	0.12
2	0.11	0.1	0.136

3	0.12	0.09	0.14
4	0.11	0.088	0.15
5	0.1	0.08	0.158
6	0.11	0.076	0.16
7	0.118	0.07	0.164
8	0.12	0.066	0.164
9	0.12	0.06	0
10	0.118	0	0.158
11	0.12	0	0.164
12	0.11	0	0.166
13	0.108	0	0.162
14	0.1	0	0.168
15	0.108	0	0.168
16	0.106	0	0.17
17	0.11	0	0.178
18	0.114	0	0.178
19	0.11	0.07	0
20	0.108	0.068	0.18
21	0.11	0.066	0.174
22	0.12	0.07	0.17
23	0.114	0.072	0.172

Table4.8: Comparative Analysis of In-Band Scenarios: Average End-to-End Delay

From the table 4.8, it is clear that in presence of wormhole attack, the Average End-to-End Delay is between '0.06' sec to '0.12' sec. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this delay is between '0.1' sec to '0.12' sec. This delay has increased i.e. '0.12' sec to '0.18' sec, if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if In-Band wormhole attack is present.

4.7.8 Comparative Analysis of Out-of-Band Wormhole Attack for Network1: Average End-to-End Delay

To see whether the proposed approach is able to stop wormhole nodes in receiving or relaying data packets, a comparative analysis has been done. The results of collected data for security are tabulated in Table4.9.

Node ID	Average End-to-End Delay (s)		
	Out-of-Band Scenarios (Network1)		
	With No Attack & Using AODV (Scenario 1)	With Attack & Using AODV (Scenario 2)	With Attack & Using SAODV (Scenario 3)
1	.1	.08	.12
2	.116	.088	.14
3	.12	.084	.15
4	.13	.09	.158
5	.14	.094	.16
6	.148	.096	.164
7	.144	.094	.17
8	.148	.09	.17
9	.15	.09	.17
10	.152	.1	.174
11	.16	.098	.176
12	.156	.096	0
13	.148	0	.18
14	.146	0	.182
15	.15	0	.182
16	.16	0	.182
17	.166	0	.19
18	.17	0	.19

Table4.9: Comparative Analysis of Out-of-Band Scenarios for Network1: Average End-to-End Delay

From the table 4.9, it is clear that in presence of wormhole attack, the Average End-to-End Delay is between '0.08' sec to '0.1' sec. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this delay is between '0.12' sec to '0.16' sec. This delay has increased i.e. '0.12' sec to '0.18' sec, if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if Out-of-Band wormhole attack is present.

4.7.9 Comparative Analysis of Out-of-Band Wormhole Attack for Network2: Average End-to-End Delay

To see whether the proposed approach is able to stop wormhole nodes in receiving or relaying data packets, a comparative analysis has been done. The results of collected data for security are tabulated in Table4.10.

Node ID	Average End-to-End Delay (s)		
	Out-of-Band Scenarios (Network2)		
	With No Attack & Using AODV (Scenario 1)	With Attack & Using AODV (Scenario 2)	With Attack & Using SAODV (Scenario 3)
1	.11	0	.132
2	.11	0	.136
3	.116	0	.144
4	.118	0	.15
5	.124	0	.154
6	.126	0	.15
7	.13	0	.15
8	.132	0	.152
9	.132	0	.156
10	.138	0	.158
11	.136	.08	0
12	.144	.09	.162
13	.15	.096	.17
14	.15	.1	.178
15	.148	.102	.17
16	.15	.1	.172
17	.152	.098	.176
18	.156	.096	.17
19	.154	.098	.176
20	.15	.1	.178
21	.152	.09	.18
22	.158	.098	.182
23	.16	.1	.182
24	.164	.1	.18
25	.168	.104	.184

Table4.10: Comparative Analysis of Out-of-Band Scenario for Network2: Average End-to-End Delay

From the table 4.10, it is clear that in presence of wormhole attack, the Average End-to-End Delay is between '0.08' sec to '0.1' sec. At this time, AODV routing protocol is used. Whereas in normal condition, that means no attack and using of AODV routing protocol, this delay is between '0.1' sec to '0.16' sec. This delay has increased i.e. '0.12' sec to '0.2' sec, if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if out-of-Band wormhole attack is present.

4.8 Validation

Validation techniques involves in judging that the proposed approaches meet the expectations of the researchers. To examine the performance and efficacy of the proposed approach, validation techniques play an important role. The statistical data collected from the implementation part can be the basis for the validation process of approaches or frameworks. Validation process is required to find out faults and gaps that can lead to incomplete development of frameworks or approaches. It is a route of creating indication that offers a high degree of declaration that a framework achieves its projected requirements.

Therefore, it can be said that validation involves acceptance of fitness for proposed frameworks by various researchers. There are various techniques available in the literature to validate the systems or frameworks. Hypothesis testing is one of the techniques involve in validating different types of approaches. It is also possible that an approach passes when verified but not succeed when validated. This situation can take place when, say, a framework is developed as per the set objectives but the objectives themselves not succeed to address the researcher's requirements.

For validation of the proposed framework, hypothesis testing is used. In the hypothesis testing, corollary 1 [145] and paired t-test [146] are used to check the significance of the proposed approach. Paired't-test' is based on t-distribution and is considered an appropriate test for judging the significance of the mean of difference between the two related data sets. The relevant test statistic, t, is calculated from the sample data and then compared with its probable value based on t-distribution at a specified level of significance for concerning degrees of freedom for accepting or rejecting null hypothesis [146].

As per the corollary1 [145], the wormhole nodes can be identified and eliminated by performing an exclusive OR (XOR) operation between the connectivity value, evaluated against geometric graph and value against communication graph with respect to the nodes that are expected as wormhole nodes. After performing exclusive OR, if any bit value comes 1 then a wormhole link will present during communication.

Therefore, researcher has to consider two types of graphs, first, Geometric Graph and second, Communication Graph for indentifying wormhole nodes. Geometric Graph is the

graph that is to be considered before the transmission while communication graph is the graph that may be considered after the transmission. It is assumed that every node has its own geometry graph. But the communication graph will be considered for the node that will announce shortest route to destination node during transmission process. Here, it is assumed that geometry graph for node N will be denoted as G_N and communication graph for node N will be denoted as $C_{N.}$ It is also assumed that if node n1 is one hop away from node n2 then the connectivity value between them will be one. If node n2 is more than one hop away from node n3, the connectivity value will be zero. This can be understood with the help of example. Consider the network, given below:-

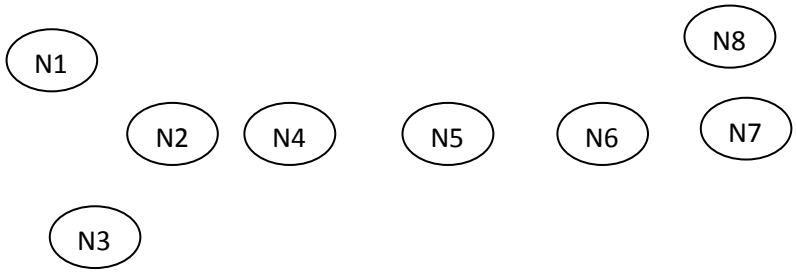

Figure4.43: A Wireless Ad hoc Network

From the figure4.43, it is clear that total number of nodes in the network is eight. These are N1, N2, N3, N4, N5, N6, N7 and N8. Node N2 is one hop away from N1, N3 and N4. Therefore, the connectivity value of N2 for N1, N3 and N4 is one, while other nodes, N5, N6, N7 and N8 are more than one hop away from N2, so the connectivity value of N2 for N5, N6, N7 and N8 will be zero. Finally, connectivity value of N2 geometry graph for whole network can be evaluated and the value will be 10110000. Likewise, the connectivity values of N1, N3, N4, N5, N6, N7 and N8 geometry graphs will be 01100000, 11000000, 01001000, 00001011, 00000101 and 00000110 respectively.

Now have another look. If suppose a wormhole link is present in a network.

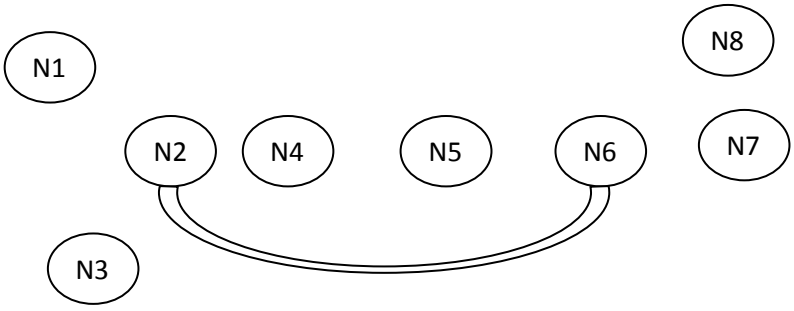

Figure4.44: A Wireless Ad hoc Network with Wormhole Link

From the figure4.44, network has total number of eight nodes N1, N2, N3, N4, N5, N6, N7 and N8. Nodes N2 and N6 are creating wormhole link. Suppose node N1 wants to communicate with node N8. Node N1 will send the RREQ data packet to N2 and N3. In normal environment, the RREQ packets will be forwarded till any node announces the route to the destination node N8. Once the node declare route to the destination, RREP will be generated in backward direction towards the source node. As in the above figure, N2 is initiating the wormhole link, the node N2 will advertise the shortest route to the destination node and all traffic will be diverted from N2 to N6. Due to presence of wormhole link, Node N4 and node N5 will not take part in communication process.

Therefore, to identify the wormhole link there is requirement to evaluate the geometry graph as well as communication graph. In the example, node N2 is announcing route to the destination. So to identify the wormhole link, there is a requirement of evaluating connectivity value of geometry graph and communication graph for node N2. For N2, the connectivity value of geometry graph is 10110000 and connectivity value of communication graph is 10110100. To identify the wormhole link, do the XOR between the connectivity value of geometry graph and connectivity value of communication graph as:-

$$G_{N2} = 10110000$$
$$C_{N2} = 10110100$$
$$\oplus = 00000100$$

In ideal case that means no presence of wormhole nodes, all bit values should be zero after doing XOR. But in this case one bit is zero in result value. That means there is presence of wormhole node in the network. To find which node is acting as wormhole, see the position of bit value with 1. In this case, the bit value is 1 at position 6. That means node N6 is creating wormhole link with the collaborating with node N2.

4.8.1 Hypothesis Testing for In-Band Wormhole Attack

It is mandatory to check the validity of the proposed framework for acceptance. The corollary 1 has been introduced to test the significance of the framework.

H0: (Null Hypothesis): Wormhole Nodes identified using corollary 1 and SAODV are not same.

Suppose, wormhole nodes identified using corollary 1 is denoted by $\mu 0$ and wormhole nodes identified using SAODV is denoted by $\mu 1$. Therefore, according to H0:-

$$H0: \mu 0 \neq \mu 1$$

H1: (Alternate Hypothesis): Wormhole Nodes identified using corollary 1 and SAODV are same.

Therefore,

$$H1: \mu 0 = \mu 1$$

From the scenario in section 4.5.3, it is clear that there are 25 nodes in the network. In that scenario, it is assumed that all nodes are legal nodes and they are not involved in creating wormhole link in the network. Now, to find out wormhole link during transmission, connectivity values of geometry graph and communication graph should be evaluated. The scenario is given below:-

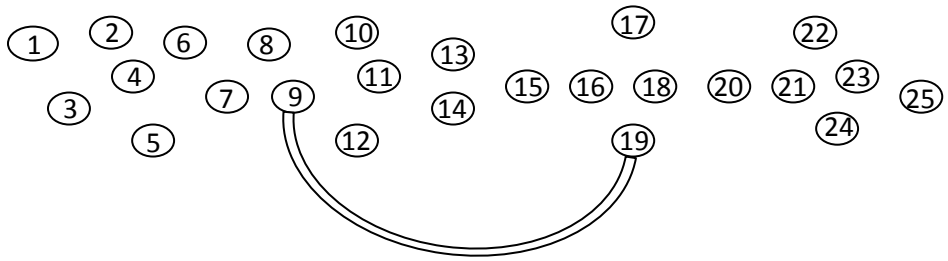

Figure4.45: A Wireless Ad hoc Network with In-Band Wormhole Attack

From figure4.45, suppose node 1 wants to communicate with node 22. Node 1 will send RREQ packet to its neighbours the process will continue till any node advertise shortest route to the destination. In this case, node 9 will announce route to the destination. Therefore, the RREP packet will be generated in backward direction towards source. After receiving RREP packet, source node will start the communication. Now, to identify the wormhole node it is the time to evaluate connectivity value of geometry graph and communication

graph for node 9 and after getting the values of C_9 and G_9, XOR operation should be performed. The values of C_9 and G_9 and XOR result are given below:-

$$G_9 = 00000011011100000000000000$$
$$C_9 = 00000011011100000001000000$$
$$\oplus = 00000000000000000001000000$$

From the result, it is clear that one bit value at position 19 is one. It can be said that, there is presence of wormhole link in the network. And node 9 and node 19 are involved in creating wormhole link.

Therefore, the value of $\mu 0$ = 9, 19……..(1)

From the table 4.2, it is clear that using SAODV routing protocol in scenario 3 all nodes in the network are able to receive and relay data packets except node 9 and 19.

Therefore, the value of $\mu 1$ = 9, 19…….(2)

From the equations 1 and 2, it is shown that the value of $\mu 0$ and the value of $\mu 1$ are same. These same values are 9 & 19.

That means the value of $\mu 0$ = the value of $\mu 1$

Because of same value of $\mu 0$ and $\mu 1$, therefore the null hypothesis is rejected and alternate hypothesis H1: $\mu 0 = \mu 1$ is accepted.

4.8.2 Hypothesis Testing for Out-of-Band Wormhole Attack

It is mandatory to check the validity of the proposed framework for acceptance. The corollary 1 has been introduced to test the significance of the framework.

H0: (Null Hypothesis): Wormhole Nodes identified using corollary 1 and SAODV are not same.

Suppose, Wormhole nodes identified using corollary 1 is denoted by $\mu 0$ and Wormhole nodes identified using SAODV is denoted by $\mu 1$. Therefore, according to H0:-

$$H0: \mu 0 \neq \mu 1$$

H1: (Alternate Hypothesis): Wormhole Nodes identified using corollary 1 and SAODV are same.

Therefore,

$$H1: \mu 0 = \mu 1$$

From the scenario in section 4.5.6, it is clear that there are 18 nodes in network1 and 25 nodes in the network2. In that scenario, it is assumed that all nodes are legal nodes and they are not involved in creating wormhole link in the network. Now, to find out wormhole link during transmission, connectivity values of geometry graph and communication graph should be evaluated. The scenario is given below:-

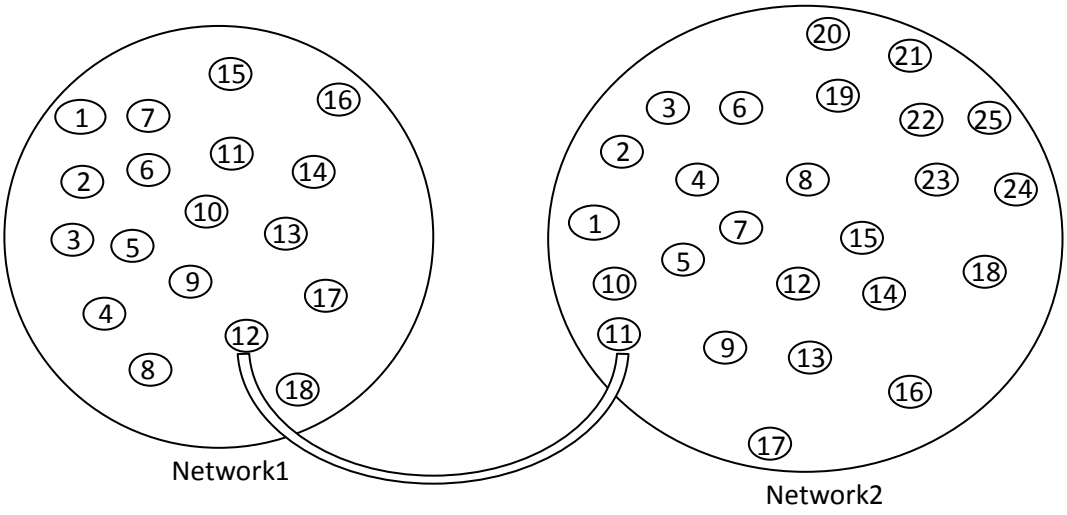

Figure4.46: A Wireless Ad hoc Network with Out-of-Band Wormhole Attack

From figure4.46, suppose node 1 of network1 wants to communicate with node 15 of network2. Node 1 will send RREQ packet to its neighbours and the process will continue till any node advertise shortest route to the destination. In this case, node 12 of network1 will announce route to the destination node 15 of network2. Therefore, the RREP packet will be generated in backward direction towards source node 1 of network1. After receiving RREP packet, source node will start the communication. Now, to identify the wormhole node it is the time to evaluate connectivity value of geometry graph and communication graph for node 12 of network1 and after getting the values of C_9 and G_9, XOR operation should be performed. The values of C_{12} and G_{12} of network1 and XOR result are as followed:-

G_{12} = 000000011000000011	00000000000000000000000000
C_{12} = 000000011000000011	00000000001000000000000000
⊕ = 000000000000000000	00000000001000000000000000

From the result, it is clear that one bit value at position 11 of network2 is one. Therefore, there is presence of wormhole link in the scenario. And node 12 and node 11 are involved in creating wormhole link.

Therefore, the value of μ0 = 12, 11……..(3)

From the table 4.3 and 4.4, it is clear that using SAODV routing protocol in scenario 3 all nodes in the network are able to receive and relay data packets except node 12 from network1 and node 11 from network 12.

Therefore, the value of μ1 = 12, 11…….(4)

From the equations 3 and 4, it is shown that the value of μ0 and the value of μ1 are same. These same values are 12 & 11.

That means the value of μ0 = the value of μ1

Because of same value of μ0 and μ1, therefore the null hypothesis is rejected and alternate hypothesis H1: μ0 = μ1 is accepted.

4.8.3 Hypothesis Testing for In-Band Wormhole Attack: Packet Delivery Ratio

It is mandatory to check the validity of the proposed framework for acceptance. A paired t-test has been introduced to test the significance of the framework [146]. The two data sets are obtained using AODV and SAODV in presence of in-band wormhole attack. A hypothesis test based on paired t-test is being performed and confidence interval is being observed by the difference of two standard mean. For this, the null hypothesis and alternative hypothesis are presented below:-

H0: (Null Hypothesis): The impact values derived from SAODV cannot significantly reflect the threat element with existing approach in packet delivery ratio under in-band wormhole attack.

H1: (Alternate Hypothesis): The impact values derived from SAODV can significantly reflect the threat element with existing approach in packet delivery ratio under in-band wormhole attack.

To perform t-test for validating the results, data sets are taken from Table4.5. The t-test history for in-band wormhole attack of packet delivery ratio is given in Table4.11.

t-Test for In-Band Wormhole Attack : Packet Delivery Ratio							
	Mean	Std. Deviation	Std. Error	No. of Sample	Two-tailed P-Value	Degree of Freedom	t-Value
With Attack & Using AODV	28.65	23.73	4.95	23	< .0001	22	6.7252
With Attack & Using SAODV	82.73	26.95	5.75				

.

Table4.11: t-Test for In-Band Wormhole Attack: Packet Delivery Ratio

To find out the significance of the difference between the means of 'With Attack & Using AODV' values and 'With Attack & Using AODV' values, the means for both AODV and SAODV is calculated. The P-value is less than 0.0001. This value shows that the values with AODV and SAODV are highly correlated and extremely statistically significant. The degree of freedom for both AODV and SAODV is 22. This test provides the ground for applicability of t-test. The t-test value comes out to be 6.7252. As the value exceeds the t critical value of 2.074 for two tailed test at the 0.05 level for 22 degree of freedom, thus the null hypothesis H0 is strongly rejected and the alternate hypothesis H1 is accepted. The impact values derived from SAODV can significantly reflect the threat element with existing approach in packet delivery ratio under in-band wormhole attack.

4.8.4 Hypothesis Testing for Out-of-Band Wormhole Attack: Packet Delivery Ratio

It is mandatory to check the validity of the proposed framework for acceptance. A paired t-test has been introduced to test the significance of the framework [146]. The two data sets are obtained using AODV and SAODV in presence of out-of-band wormhole attack. A hypothesis test based on paired t-test is being performed and confidence interval is being observed by the difference of two standard mean. For this, the null hypothesis and alternative hypothesis are presented below:-

H0: (Null Hypothesis): The impact values derived from SAODV cannot significantly reflect the threat element with existing approach in packet delivery ratio under out-of-band wormhole attack.

H1: (Alternate Hypothesis): The impact values derived from SAODV can significantly reflect the threat element with existing approach in packet delivery ratio under out-of-band wormhole attack.

To perform t-test for validating the results, data sets are taken from Table4.6 & Table4.7.The t-test history for out-of-band wormhole attack of packet delivery ratio is given in Table4.12.

t-Test for out-of-Band Wormhole Attack : Packet Delivery Ratio							
	Mean	Std. Deviation	Std. Error	No. of Sample	Two-tailed P-Value	Degree of Freedom	t-Value
With Attack & Using AODV	26.37	20.87	3.18	43	< .0001	42	12.5783
With Attack & Using SAODV	87.57	19.99	3.08				

.

Table4.12: t-Test for Out-of-Band Wormhole Attack: Packet Delivery Ratio

To find out the significance of the difference between the means of 'With Attack & Using AODV' values and 'With Attack & Using AODV' values, the means for both AODV and SAODV is calculated. The P-value is less than 0.0001. This value shows that the values with AODV and SAODV are highly correlated and extremely statistically significant. The degree of freedom for both AODV and SAODV is 42. This test provides the ground for applicability of t-test. The t-test value comes out to be 12.5783. As the value exceeds the t critical value of 2.021 for two tailed test at the 0.05 level for 42 degree of freedom, thus the null hypothesis H0 is strongly rejected and the alternate hypothesis H1 is accepted. The impact values derived from SAODV can significantly reflect the threat element with existing approach in packet delivery ratio under out-of-band wormhole attack.

4.8.5 Hypothesis Testing for In-Band Wormhole Attack: Average End-to-End Delay

It is mandatory to check the validity of the proposed framework for acceptance. A paired t-test has been introduced to test the significance of the framework [146]. The two data sets are obtained using AODV and SAODV in presence of in-band wormhole attack. A hypothesis test based on paired t-test is being performed and confidence interval is being observed by the difference of two standard mean. For this, the null hypothesis and alternative hypothesis are presented below:-

H0: (Null Hypothesis): The impact values derived from SAODV cannot significantly reflect the threat element with existing approach in end-to-end delay under in-band wormhole attack.

H1: (Alternate Hypothesis): The impact values derived from SAODV can significantly reflect the threat element with existing approach in end-to-end delay under in-band wormhole attack.

To perform t-test for validating the results, data sets are taken from Table4.8. The t-test history for in-band wormhole attack of end-to-end delay is given in Table4.13.

t-Test for In-Band Wormhole Attack : Average End-to-End Delay							
	Mean	Std. Deviation	Std. Error	No. of Sample	Two-tailed P-Value	Degree of Freedom	t-Value
With Attack & Using AODV	0.04852	0.04279	0.00892	23	< .0001	22	6.1625
With Attack & Using SAODV	0.14673	0.04960	0.01058				

.

Table4.13: t-Test for In-Band Wormhole Attack: Average End-to-End Delay

To find out the significance of the difference between the means of 'With Attack & Using AODV' values and 'With Attack & Using AODV' values, the means for both AODV and SAODV is calculated. The P-value is less than 0.0001. This value shows that the values with AODV and SAODV are highly correlated and extremely statistically significant. The degree of freedom for both AODV and SAODV is 22. This test provides the ground for applicability of t-test. The t-test value comes out to be 6.1625. As the value exceeds the t critical value of 2.074 for two tailed test at the 0.05 level for 22 degree of freedom, thus the null hypothesis H0 is strongly rejected and the alternate hypothesis H1 is accepted. The impact values derived from SAODV can significantly reflect the threat element with existing approach in end-to-end delay under in-band wormhole attack.

4.8.6 Hypothesis Testing for Out-of-Band Wormhole Attack: Average End-to-End Delay

It is mandatory to check the validity of the proposed framework for acceptance. A paired t-test has been introduced to test the significance of the framework [146]. The two data sets are obtained using AODV and SAODV in presence of out-of-band wormhole attack. A

hypothesis test based on paired t-test is being performed and confidence interval is being observed by the difference of two standard mean. For this, the null hypothesis and alternative hypothesis are presented below:-

H0: (Null Hypothesis): The impact values derived from SAODV cannot significantly reflect the threat element with existing approach in End-to-End Delay under out-of-band wormhole attack.

H1: (Alternate Hypothesis): The impact values derived from SAODV can significantly reflect the threat element with existing approach in End-to-End Delay under out-of-band wormhole attack.

To perform t-test for validating the results, data sets are taken from Table4.9 & Table4.10. The t-test history for out-of-band wormhole attack of End-to-End Delay is given in Table4.14.

t-Test for out-of-Band Wormhole Attack : Average End-to-End Delay							
	Mean	Std. Deviation	Std. Error	No. of Sample	Two-tailed P-Value	Degree of Freedom	t-Value
With Attack & Using AODV	0.5935	0.15752	0.00709	43	< .0001	42	10.3865
With Attack & Using SAODV	0.04650	0.3916	0.00604				

.

Table4.14: t-Test for Out-of-Band Wormhole Attack: Average End-to-End Delay

To find out the significance of the difference between the means of 'With Attack & Using AODV' values and 'With Attack & Using AODV' values, the means for both AODV and SAODV is calculated. The P-value is less than 0.0001. This value shows that the values with AODV and SAODV are highly correlated and extremely statistically significant. The

degree of freedom for both AODV and SAODV is 42. This test provides the ground for applicability of t-test. The t-test value comes out to be 10.3865. As the value exceeds the t critical value of 2.021 for two tailed test at the 0.05 level for 42 degree of freedom, thus the null hypothesis H0 is strongly rejected and the alternate hypothesis H1 is accepted. The impact values derived from SAODV can significantly reflect the threat element with existing approach in End-to-End Delay under out-of-band wormhole attack.

4.9 Comparison of Existing Approaches with SAODV

In this research, SAODV (Secure Ad hoc on demand Distance Vector) is implemented to detect wormhole attack and prevent network by restricting wormholes to receive packets. This approach use QOS parameters to differentiate available solutions. This approach successfully detects the wormhole nodes without using the extra hardware. As per section 2.6, the available solutions regarding wormhole attack are divided into three categories: the first category of solutions is based on modifying the routing protocols such as AODV, DSR, and OLSR. The solutions given in [104, 105, 106, 107, 108] are the example of this category. The second category of solutions is based on modifying routing protocol without using extra hardware. The examples of this category are in [102, 109, 111, 88, 110].

The third and final category of methods is based on deployment of intrusion detection nodes or system with or without using extra hardware. The examples are in [89, 113, 114, 112]. Table4.15 shows differences of approaches and accomplishments between SAODV and other available related work with taking parameters such as extra hardware, clock synchronisation, wormhole node detection, out of band wormhole detection, in-band wormhole detection etc..Furthermore, approaches in [102, 109, 111, 88, 113, 89, 110, 112] are solutions that require extra hardware facilities. Whereas, Approaches like SAODV and [106] do not require extra hardware facilities. SAODV does not rely on loose time synchronisation mechanism while an approach in [106] requires loose time synchronisation mechanism.

There are two solutions that claimed to prevent wormhole attacks, but they are not capable of identifying wormhole. These approaches are in [111, 105] whereas SAODV successfully prevented wormhole nodes from receiving packets. There are several methods that can defend in band wormhole attack or out of band wormhole attack. SAODV is

compatible for detecting both the in band and out of band wormhole attacks. The approaches that can defend against in band wormhole attacks, but not out of band wormhole attack are in [111, 88, 107, 108, 114, 112]. The examples for out of band wormhole attacks are in [104, 105, 117, 110]. Apart from above mentioned approaches there are some other solutions available in literature.

These solutions are somehow different from SAODV. The proposed solution against wormhole attack enables quality of service (QOS) parameters as additional value. To differentiate SAODV from other available approaches researcher took help from [124]. Parameters, used to differentiate SAODV from available approaches, are platform, quality of surface parameters, extra hardware support, clock-synchronization, wormhole attack detection, out-of-band wormhole detection and in-band wormhole detection. The proposed solution is based on AODV protocol. This solution used QualNet simulator for implementing various scenarios and analysis of these scenarios. After implementation it was observed that there is no need of clock synchronization. The overall summary of all the available solutions with described parameters are given in Table4.15.

Protocol	**Based on**	**Implemented on**	**QOS Parameters**	**Extra H/W**	**Clock Synchronization**	**wormhole attack Detection**	**out of band wormhole detection**	**in-band wormhole detection**
DelPHI (Chiu and Lui, 2006) [105]	AODV	NS-2	No	No	No	No	Yes	Yes
WARP (Ming-Yang Su, 2010) [117]	AODV	NS-2	No	No	No	Yes	Yes	Yes
SAODV (Raj Shree et al., 2014)	AODV	QualNet Simulator	Yes	No	No	Yes	Yes	Yes
EDWA (Wang and Wong, 2007 [110]	AODV	NS-2	No	Yes	Yes	Yes	Yes	Yes
SAM (Song et al., 2005)[104]	DSR	NS-2	No	No	No	Yes	Yes	Yes
Lee et al. (2008) [106]	DSR	NS-2	No	No	Yes	Yes	Yes	Yes

LITEWORP (Khalil et al., 2005) [102]/ MOBIWORP (Khalil et al., 2006) [106]	DSR	NS-2	No	Yes	Yes	Yes	Yes	Yes
Secure DSR (Qazi et al. 2013 [51]	DSR	No Info	No	Yes	Yes	Yes	Yes	Yes
Naıt-Abdesselam et al. (2007)[108]	OLSR	NS-2	No	No	No	Yes	No	Yes
Su et al. (Su and Boppana, 2007) [107]	Ariadne	NS-2	No	No	No	Yes	No	Yes
TIK (Hu et al., 2006) [88]	None	NS-2	No	Yes	Yes	Yes	No	Yes
Lazos et al. (2005) [111]	None	NS-2	No	Yes	Yes	No	No	Yes
MSDN (Stoleru et al. 2012) [126]	None	purpose-built simulator	No	Yes	Yes	Yes	No	No
LDAC (Thanassis Giannetsos, Tassos Dimitriou, 2014) [125]	None	None	No	No	Yes	Yes	No	No
Gorlatova et al. (2006) [89]	OLSR	NS-2	No	Yes	No	Yes	Yes	Yes
Wang (2006) [113]	AODV	NS-2	No	Yes	N/A	Yes	Yes	Yes
TTM (Phuong et al., 2007) [114]	AODV	NS-2	No	No	No	No	No	Yes
Azer et al., 2008) [112]	AODV	NS-2	No	Yes	No	Yes	No	Yes

Table4.15: Comparison of Various Approaches of Wormhole Attacks with SAODV

4.10 Conclusion

The challenge of providing security is greater when wireless and mobile networks are considered for exchanging data. Mobility and Freedom are the main advantage provided by wireless and mobile devices and it is, sarcastically, the source of creating major problems. In particular, Mobile Ad–hoc Networks present the following challenges: dynamic topology, uneven structure, open network architecture, limited battery life, limited computational resources and shared wireless environment. Therefore, it is the need of time to provide secure environment that can exchange data over wireless and mobile networks. Here, from the attack detection and prevention module it is clear that to introduce SAODV, no significant changes are required on the AODV protocol. Thus SAODV operation mode remains practically unchanged. SAODV is capable of finding In-Band wormhole attack and Out-of-Band wormhole attacks. Even high quantity of false detections is not generated. From the simulation, it is clear that the percentage of packet delivery ratio has increased up to 10% after adding security module. And average packet delay is also increased.

Chapter 5: Conclusion & Future Work

5.1 Background

Keeping in view of the upcoming technological trends like IoT, SDR (software defined radios), dynamic self configuring which rely heavily on secure networking protocol. Its imperatives to make all networking and routing protocols secure, fault tolerant and robust. Making existing routing protocols full proof is very important for the phenomena of "ubiquitous computing". Exploring various attack vectors and developing solutions to mitigate them is a continuous process. The present study will pave path for more secure application and directing other researchers' efforts in mitigating other vulnerability. This will also open a noble way of mitigating similar vulnerabilities and loopholes.

Therefore, the next section will provide the major findings that are the results of implementing the SAODV followed by future work.

5.2 Major Findings

In this thesis, SAODV, a secure routing protocol has implemented to provide security in Mobile Ad hoc Network using the QualNet simulation environment. Six experiments are conducted to see the effectiveness of the SAODV protocol. Two types of wormhole attacks are taken in this research. First is In-Band wormhole attack and second is Out-of-Band wormhole attack.

- **For In-Band wormhole attack,** three scenarios are taken into account:-

1. **A Network is simulated that has no wormhole attack and using AODV routing protocol: -** In this scenario, 23 nodes are taken in a network. And AODV routing protocol is used. It is seen that all nodes are working properly and they are receiving and relaying data packets with normal behavior.

2. **A Network is simulated that has In-Band wormhole attack and using AODV routing protocol: -** In this scenario, 25 nodes are taken in a network. In-Band wormhole attack is present in the network and AODV routing protocol is used. It is seen that node 9 and 19 nodes are initiating wormhole attack. Due to them, nodes 10, 11, 12, 13, 14, 15, 16, 17, 18 are not able to receive data packets.

3. **A Network is simulated that has In-Band wormhole attack and using SAODV routing protocol: -** In this scenario, 25 nodes are in the network as above. Difference is that this scenario is using SAODV routing protocol. It is seen that SAODV has successfully stopped to node 9 and 19 in receiving and relaying data packets.

- **For Out-of-Band wormhole attack,** three scenarios are taken into account:-

1. **A Network is simulated that has no wormhole attack and using AODV routing protocol: -** In this scenario, there are two networks. No wormhole attack is present in the network and networks are using AODV routing protocol. Network1 has 18 nodes whereas Network2 has 23 nodes in the network. It is seen that all nodes in both the network are working properly and they are receiving and relaying data packets with normal behavior.

2. **A Network is simulated that has Out-of-Band wormhole attack and using AODV routing protocol: -** In this scenario, Network1 has 18 nodes and Network2 has 25 nodes in the network. It is seen that node 12 from Network1 and node 11 from Network2 are launching Out-of-Band wormhole

attack. Due to them, nodes 13, 14, 15, 16, 17, 18 from Network1 and nodes 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 from Network2 are not involve in exchanging data packets.

3. **A Network is simulated that has out-of-Band wormhole attack and using SAODV routing protocol: -** In this scenario, Network1 has 18 nodes and Network2 has 25 nodes in the network as above. Difference is that this scenario is using SAODV routing protocol. It is seen that SAODV has successfully stopped to node 12 from Network1 and node 11 from Network2 in receiving and relaying data packets.

Therefore, from the above discussion, it is clear that SAODV can work effectively in presence of both the wormhole attacks, In-Band wormhole attack and Out-of-Band wormhole attack.

5.3 Other Findings

The packet delivery ratio and average end-to-end delay is computed in In-Band wormhole and Out-of-Band wormhole attack, as discussed below:-

➢ Packet Delivery Ratio for In-Band wormhole attack

In this scenario, there are 23 mobile nodes in a network. Packet delivery ratio is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol, second, packet delivery ratio with attack and using AODV routing protocol, and packet delivery ratio with attack and using SAODV routing protocol. From the scenario, it is clear that in presence of wormhole attack, the packet delivery ratio is between '40%' to '55%'. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this ratio is between '70%' to '85%'. This ratio has increased i.e. '80%' to '95%', if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if In-Band wormhole attack is present.

➢ Packet Delivery Ratio for Out-of-Band wormhole attack in Network1

This scenario and next scenario show the collaborative function of two networks, Network1 and Network2. In this scenario, there are 18 mobile nodes in Network1. Packet delivery ratio is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol, second, packet delivery ratio with attack and using AODV routing protocol, and packet delivery ratio with attack and using SAODV routing protocol. From the scenario, it is clear that in presence of wormhole attack, the packet delivery ratio is between '35%' to '50%'. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this ratio is between '75%' to '90%'. This ratio has increased i.e. '85%' to '95%', if SAODV is used in presence of Out-of-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if Out-Band wormhole attack is present.

➢ Packet Delivery Ratio for Out-of-Band wormhole attack in Network2

In this scenario, there are 25 mobile nodes in Network2. Packet delivery ratio is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol, second, packet delivery ratio with attack and using AODV routing protocol, and packet delivery ratio with attack and using SAODV routing protocol. From the scenario, it is clear that in presence of wormhole attack, the packet delivery ratio is between '30%' to '50%'. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this ratio is between '75%' to '85%'. This ratio has increased i.e. '85%' to '98%', if SAODV is used in presence of Out-of-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if Out-of-Band wormhole attack is present.

➢ Average End-to-End Delay for In-Band wormhole attack

In this scenario, there are 23 mobile nodes in a network. Average End-to-End Delay is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol, second, packet delivery ratio with attack and using AODV routing protocol, and packet delivery ratio with attack and using SAODV routing protocol. From the scenario, it is clear that in presence of wormhole attack, the Average End-to-End Delay is between '0.06' sec to '0.12' sec. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this delay is between '0.1' sec to '0.12' sec. This delay has increased i.e. '0.12' sec to '0.18' sec, if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if In-Band wormhole attack is present.

➢ Average End-to-End Delay for Out-of-Band wormhole attack in Network1

This scenario and next scenario show the collaborative function of two networks, Network1 and Network2. In this scenario, there are 18 mobile nodes in Network1. Average End-to-End Delay is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol, second, packet delivery ratio with attack and using AODV routing protocol, and packet delivery ratio with attack and using SAODV routing protocol. From the scenario, it is clear that in presence of wormhole attack, the Average End-to-End Delay is between '0.08' sec to '0.1' sec. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this delay is between '0.12' sec to '0.16' sec. This delay has increased i.e. '0.12' sec to '0.18' sec, if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if Out-of-Band wormhole attack is present.

- **Average End-to-End Delay for Out-of-Band wormhole attack in Network2**

In this scenario, there are 25 mobile nodes in Network2. Average End-to-End Delay is shown with three conditions, first, packet delivery ratio without attack and using AODV routing protocol, second, packet delivery ratio with attack and using AODV routing protocol, and packet delivery ratio with attack and using SAODV routing protocol. From the scenario, it is clear that in presence of wormhole attack, the Average End-to-End Delay is between '0.08' sec to '0.1' sec. At this time, AODV routing protocol is used. Whereas in normal condition that means no attack and using of AODV routing protocol, this delay is between '0.1' sec to '0.16' sec. This delay has increased i.e. '0.12' sec to '0.2' sec, if SAODV is used in presence of In-Band wormhole attack. Therefore, it is clear that the SAODV routing protocol is working efficiently even if out-of-Band wormhole attack is present.

5.4 Future Work

There are different types of attacks available in Mobile Ad hoc Network. Most of the attacks against security in Mobile Ad hoc Network are related to routing information within the network. In this research work, the wormhole is simulated in the Ad-hoc Networks and applied SAODV protocol to detect and remove wormhole node from the network. A no. of techniques has been proposed by various researchers to detect wormhole node. So the next logical outcome is to compare these techniques and evaluate them. However, developing such a detection mechanism and making it efficient represents a great research challenge. Many of today's proposed security schemes are based on specific network models.

A combined effort to take a common model to ensure security for each layer is not present in literature, therefore in future there will be requirement of well established security mechanisms for each individual layer and all the mechanisms should be worked together in collaboration with each other that will also incur a hard research challenge. In this work, only wormhole node is found out and block them to send or receive packets. In the future work researchers can use this protocol with more parameters. The cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming

days. The mathematical modeling of different threats present in the MANET is another aspect of this work.

It is known that mobile devices use small portable batteries in many of the application. Therefore, to develop energy efficient routing protocol that can maximize the life of batteries is also a top importance.

5.5 Conclusion

There are a great number of various kinds of routing protocols available for mobile Ad hoc network. Many factors, like network load, network size, routing overhead mobility requirement and throughput, decide the application of a specific routing protocol in mobile Ad hoc network. In current situation, on-demand routing protocols have achieved more consideration in mobile Ad hoc networks as compared to other routing schemes due to their possible flexibility in deployment and competence in terms of throughput. They are capable of organizing themselves dynamically with lesser memory overhead and lesser bandwidth requirement than table driven protocols. There are many on-demand routing protocols present for mobile Ad hoc networks (MANETS). Most of the protocols are not security aware in sense of exchanging data packets. Therefore, there is a need of such protocol that can provide security in exchanging data packets.

In the present research SAODV is implemented and subsequently comprehensive analysis has been done using QualNet simulator. To achieve lower traffic congestion, higher packet delivery ratio, resilience to route failures where mobility is high, nodes are dense and traffic is more, simulation results reveals that SAODV is the best choice. The overall conclusion is that SAODV routing protocol is best choice to move towards a network with better Quality of Service (QoS).

References

[1] Debashis Saha, Amitava Mukherjee, Somprakash Bandyopadhyay, 'Networking Infrastructure for Pervasive Computing Enabling Technologies and Systems', ISBN: 978-1-4020-7249-9 (Print), 978-1-4615-1143-4 (Online), 2003, Springer.

[2] James A. Freebersyser, Barry Leiner, 'A DoD perspective on mobile ad hoc networks', Charles E. Perkins (Ed.), Ad Hoc Networking, Addison Wesley, Reading, MA, 2001, pp. 29–51.

[3] W. Fifer, F. Bruno, 'The low-cost packet radio', Proceedings of the IEEE volume 75, number 1, 1987, pp. 33–42.

[4] N. Shacham, J. Westcott, 'Future directions in packet radio architectures and protocols', Proceedings of the IEEE volume 75, number 1, 1987, pp. 83–99.

[5] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, 'Mobile ad hoc networking: imperatives and challenges', Ad Hoc Networks 1 (2003) 13–64.

[6] Sourangsu Banerji, Rahul Singha Chowdhury, 'On IEEE 802.11: Wireless LAN Technology', Original Publication: International Journal of Mobile Network Communications & Telematics, (IJMNCT), Vol.3, Issue 4, 2013. [DOI: 10.5121/ijmnct.2013.3405]

[7] B. Leiner, R. Ruth, A.R. Sastry, 'Goals and challenges of the DARPA GloMo program', IEEE Personal Communications, Vol.3, Issue 6, 1996, pp. 34–43.

[8] Chapter 4, Digitization Execution, Army Digitization Master Plan (ADMP), http://www.globalsecurity.org/military/library/report/1995/admp95-adoch4.htm.

[9] R. Ruppe , S. Griswald , P. Walsh, R. Martin, Near Term Digital Radio (NTDR) System', Proceedings MILCOM \'97, 1997, pp.1282 -1287

[10] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, Piet Demeester, 'an overview of mobile ad hoc networks: applications and challenges', Session 4. http://cwi.unik.no/images/Manet_Overview.pdf.

[11] C-F Huang, H-W Lee, and Y-C Tseng, 'A Two-Tier Heterogeneous Mobile Ad Hoc Network Architecture and Its Load-Balancing Routing Problem', ACM/Kluwer Journal of Mobile Networks and Applications, vol.9, no.4, 2004, pp.379-391.

[12] J. Strater, B. Wollman, 'OSPF Modeling and Test Results and Recommendations', Mitre Technical Report 96W0000017, Xerox Office Products Division, 1996.

[13] IEEE Std. 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1997.

[14] J. Khun-Jush, P. Schramm, U. Wachsmann, F. Wenger, 'Structure and Performance of the HIPERLAN/2 Physical Layer', Proc. IEEE Vehicular Technology Conf. (VTC ',99), vol. 5, pp. 2667-2671, 1999.

[15] W. Choi, M. Woo, 'A distributed weighted clustering algorithm for mobile ad hoc networks', International Conference on Internet and Web Applications and Telecommunications (AICT-ICIW), 2006, pp. 73.

[16] Mihail C. Roco, William Sims Bainbridge, 'Converging Technologies for Improving Human Performance', Nanotechnology, Biotechnology, Information Technology And Cognitive Science, NSF/DOC-sponsored report, June 2002, http://www.whitehouse.gov/sites/default/files/microsites/ostp/bioecon-%28%23%20023SUP P%29%20NSF-NBIC.pdf.

[17] Pereira, Vasco, Sousa, Tiago, 'Evolution of Mobile Communications: from 1G to 4G', Department of Informatics Engineering of the University of Coimbra, Portugal, 2004.

[18] Vasco Pereira, Tiago Sousa, Paulo Mendes, Edmundo Monteiro, 'Evaluation of Mobile Communications: From Voice Calls to Ubiquitous Multimedia Group Communications', 2nd International Working Conference on Performance Modelling and Evaluation of Heterogeneous Networks, HET-NETs'04, ilkey, West Yorkshire, U.K., 2004.

[19] Mohammed Jaloun, Zouhair Guennoun, ' Wireless Mobile Evolution to 4G Network', Wireless Sensor Network, 2010, 2, 309-317, doi:10.4236/wsn.2010.24042.

[20] M. Weiser, 'The Computer for the Twenty-First Century', Scientific American, 1991.

[21] J. Ahola, 'Ambient Intelligence', ERCIM (European Research Consortium for Information and Mathematics) NEWS, N. 47, 2001.

[22] Jennifer J.-N. Liu And Imrich Chlamtac, 'Mobile Ad-Hoc Networking With A View Of 4G Wireless: Imperatives And Challenges', Chapter 1, Mobile Ad Hoc Networking, IEEE Press, A John Wiley & Sons, Inc., Publication, ISBN 0-471-37313-3, 2004.

[23] Lin, Y. B., Haung, Y.R., Pang, A. C., Chlamtac, I., 'All-IP Approach for UMTS Third Generation Mobile Networks', IEEE Network, volume 16, number 5, 2002, pp. 8-19.

[24] Mohamed-Lamine Messai, 'Classification of Attacks in Wireless Sensor Networks', International Congress on Telecommunication and Application'14, University of A.MIRA Bejaia, Algeria, 2014.

[25] Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia, Nirali Mody, Sugata Sanyal, Ajith Abraham, 'A Distributed Security Scheme for Ad Hoc Networks', ACM Publications, Vol-11, Issue 1, 2004, pp. 5– 15.

[26] Cordeiro, C., Agrawal, D., 'Mobile ad hoc networking', Tutorial/Short Course in 20 th Brazilian Symposium on Computer Networks, 2002, pp. 125–186.

[27] Kai Chen, Samarth H. Shah, Klara Nahrstedt, 'Cross-Layer Design for Data Accessibility in Mobile Ad hoc Networks', Kluwer Academic Publishers, Printed in the Netherlands, 2001, pp. 1-34.

[28] Kees Jan Hermans, 'Secure Networking in the Field', https://www.fox-it.com/en/files/2012/03/fox_skytale__whitepaper.pdf.

[29] Vasco Pereira, Tiago Sousa, Paulo Mendes, Edmundo Monteiro, 'Evaluation of Mobile Communications: From Voice Calls to Ubiquitous Multimedia Group Communications', http://copelabs.ulusofona.pt/files/pmendes/2004-ieee-hetnets-voice-group.pdf.

[30] Chapter 3, 'The Cellular Engineering Fundamentals', http://www.iitg.ernet.in/scifac/qip/public_html/cd_cell/chapters/a_mitra_mobile_communication/chapter3.pdf.

[31] Clarke, R., 'Expanding mobile wireless capacity: The challenges presented by technology and economics', Available at SSRN 2197416.

[32] Yu Wang, 'Collision Avoidance Protocols In Ad Hoc Networks', Chapter 2, Ad Hoc Networks Technologies And Protocols, Ebook ISBN: 0-387-22690-7, Springer Science + Business Media, Inc. Boston, 2005, pp. 23-60.

[33] Subir Kumar Sarkar, T. G. Basavaraju, C. Puttamadappa., 'Ad hoc mobile wireless networks : principles, protocols, and applications', ISBN 978‑1‑4200‑6221‑2, Auerbach Publications, Taylor & Francis Group, New York, London, 2008.

[34] J. Sen, 'Security and Privacy Issues in Wireless Mesh Networks: A Survey', Wireless Networks and Security, Khan, S. (eds.), Springer-Verlag, Berlin, Heidelberg, February 2013, pp. 189-272.

[35] P. Papadimitratos, Z. Haas, 'Secure routing for mobile ad hoc networks', SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), 2002. http://www.csee.umbc.edu/courses/graduate/CMSC691A/Spring04/papers/secure_routi_adhoc.pdf

[36] C. Karlof, D. Wagner, 'Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures', Ad Hoc Networks, vol. 1, 2003, pp. 293 -315.

[37] D. Lough, 'A Taxonomy of Computer Attacks with Applications to Wireless Networks', Virginia Polytechnic Institute PhD Thesis, April 2001. http://vtechworks.lib.vt.edu/bitstream/handle/10919/27242/lough.dissertation.pdf?sequence=1.

[38] J. Luo, D. Ye, X. Liu, M. Fan, 'A survey of multicast routing protocols for mobile ad-hoc networks', IEEE Communications Surveys & Tutorials, vol. 11, no. 1, 2009, pp. 78 -91.

[39] M. Mauve, A. Widmer, H. Hartenstein, ‘A survey on position-based routing in mobile ad hoc networks’, IEEE Network: The Magazine of Global Internetworking, Vol.15, No.6, pp. 30-39, 2001. [doi>10.1109/65.967595]

[40] T. Lin, ‘Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications’, Doctoral dissertation in Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, 2004. http://scholar.lib.vt.edu/theses/available/etd-03262004-144048/unrestricted/Tao_PhD_Dissertation.pdf.

[41] D. Mahmood, N. Javaid, U. Qasim, Z. A. Khan, A. Khan, S. Qurashi, A. Memon, ‘Modeling and Evaluating Performance of Routing Operations in Proactive Routing Protocols’, Journal of Basic and Applied Scientific Research, Vol. 3, Issue 9, 2013(ISI-Index), pp. 585-602.

[42] Perkins, C. E., Bhagwat, P, ‘DSDV Routing over a Multihop Wireless Network of Mobile Computers’, In Perkins [20], 2001, chapter 3, pp. 53–74. http://arxiv.org/ftp/arxiv/papers/1309/1309.4389.pdf.

[43] C.E. Perkins, P. Bhagwat, ‘Highly Dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers’, SIGCOMM Computer Communication Rev. ISSN: 0146-4833-2-4, 1994, pp. 234–244, http://dx.doi.org/10.1145/190314.190336.

[44] K. Ur R. Khan, A V. Reddy, R. U Zaman, ‘An efficient DSDV routing protocol for wireless mobile ad hoc networks and its performance comparison’, Second UKSIM Symposium on Computer Modeling and Simulation, 2008, pp. 506–511.

[45] Jyu-Wei Wang, Hsing-Chung Chen, Yi-Ping Lin, ‘A Secure DSDV Routing Protocol for Ad Hoc Mobile Networks’, fifth International Joint Conference on INC, IMS and IDC, 2009, pp. 2079-2084.

[46] https://www.ietf.org/rfc/rfc3626.txt.

[47] Hiroshi Mineno, Kazuyoshi Soga, Tomoya Takenaka, Yoshiaki Terashima, Tadanori Mizuno, ‘Integrated protocol for optimized link state routing and localization: OLSR-L’, Simulation Modelling Practice and Theory, Volume 19, Issue 8, 2011, pp. 1711-1722.

[48] Jiazi Yi, Asmaa Adnane, Sylvain David, Benoît Parrein, 'Multipath optimized link state routing for mobile ad hoc networks', Ad Hoc Networks, Volume 9, Issue 1, 2011, pp. 28–47.

[49] Jan-Maarten Verbree, Maurits de Graaf, Johann Hurink, 'An analysis of the lifetime of OLSR networks', Ad Hoc Networks, Volume 8, Issue 4, 2010, pp. 391–399.

[50] Fenglien Lee, 'Routing in Mobile Adhoc Networks', Chapter 16, Mobile Adhoc Networks: Protocol Design, Edited by Xin Wang, www.intechopen.com, ISBN-978-953-307-402-3.

[51] Shams Qazi, Raad Raad, Yi Mu, Willy Susilo, ' Securing DSR against wormhole attacks in multirate ad hoc networks', Review Article, Journal of Network and Computer Applications, Volume 36, Issue 2, 2013, pp. 582-592.

[52] R. Kasirama, G. RajKumar, J. Asokan, Durairaj Parthiban, 'Performance Analysis of DSR and DSDV in Motion and Motionless State', Original Research Article, Procedia Engineering, Volume 38, 2012, pp. 1518-1523.

[53] V. Park, J. Macker and M. S. Corson "Applicability of the Temporally-Ordered Routing Algorithm for use in Mobile Tactical Networks", Proc. IEEE MILCOM \'98, 1998.

[54] http://www.ietf.org/proceedings/52/I-D/draft-ietf-manet-tora-spec-04.txt.

[55] Carlos De Morais Cordeiro, Dharma Prakash Agrawal, 'Adhoc & Sensor Networks, Chapter 2, Theory And Applications', Word Scientific Publishing Co. Pte. Ltd, ISBN: 981-256-682-1, 2006, pp. 19-75.

[56] Walter Goralski, 'The Illustrated Network', Chapter 5, 2009, pp. 143-164.

[57] Charles Perkins. Ad-Hoc On Demand Distance Vector Routing (AODV). Internet-Draft, November 1997. draft~ietf-manet-aodv-00.txt.

[58] http://nccur.lib.nccu.edu.tw/bitstream/140.119/32704/6/53003106.pdf

[59] Peng Ning, Kun Sun, 'How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols', Ad Hoc Networks, No.3, 2005, pp.795–819.

[60] Perkins C., Belding-Royer E., Das S., 'Ad hoc On-Demand Distance Vector (AODV) Routing', IETF, RFC 3561. MANET Working Group, 2004, Retrieved on 2010-06-18. https://www.ietf.org/rfc/rfc3561.txt.

[61] M.Saravana karthikeyan, K.Angayarkanni, Dr.S.Sujatha, 'Throughput Enhancement in Scalable MANETs using Proactive and Reactive Routing Protocols', International MultiConference of Engineers and Computer Scientists 2010, Vol II, IMECS 2010, March 17-19, 2010, Hong Kong.

[62] Jianhong Xia , Lixin Gao , Teng Fei, 'Flooding attacks by exploiting persistent forwarding loops', 5th ACM SIGCOMM conference on Internet Measurement, Berkeley, CA, October 19-21, 2005, pp. 36-36.

[63] Abderrahmane Baadache, Ali Belmehdi, 'Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks', Original Research Article, Computer Networks, Volume 73, 14 November 2014, pp. 173-184.

[64] Meenakshi Tripathi, M.S. Gaur, V. Laxmi , 'Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN', Original Research Article, Procedia Computer Science, Volume 19, 2013, pp. 1101-1107.

[65] Snehlata Handrale, Prof. S. K. Pathan, 'An Overview of Anonymous Routing ALERT Protocol ', International Journal of Computer Science and Information Technologies, Vol. 5 (2), ISSN: 0975-9646, 2014, pp. 1607-1609.

[66] Lidong Zhou , Z. J. Haas, 'Securing ad hoc networks', IEEE Network: The Magazine of Global Internetworking, Vol.13, No. 6, 1999, pp.24-30, doi>10.1109/65.806983.

[67] P. Argyroudis, D. O. Mahony, 'Secure routing for mobile ad hoc networks', IEEE Commun. Surveys & Tutorials, Vol. 7, No. 3, 2005, pp. 2-21.

[68] Y.-C. Hu, A. Perrig, D.B. Johnson, 'Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Networks', 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03), San Francisco, CA, April 2003.

[69] A. S. Al Shahrani, 'Rushing Attack in Mobile Ad Hoc Networks', 3rd International Conference on Intelligent Networking and Collaborative Systems, Fukuoka, 30 November-2 December 2011, pp. 752-758, doi:10.1109/INCoS.2011.145.

[70] J. Lundberg, 'Routing Security in Ad hoc Networks', http://citeseer.nj.nec.com/400961.html.

[71] J.-F. Raymond, 'Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems', Proc. Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, 2000, pp. 7-26.

[72] Chia- Chun Chang, Min-Kuan Chang, 'Distributed ad-hoc passive routing path selection algorithm with prioritized broadcasting order based on non-realtime and semi-global routing information', proceeding of the International Conference on Mobile Technology, Application, and Systems, Article No. 36, ISBN: 978-1-60558-089-0, 2008, doi>10.1145/1506270.1506317.

[73] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, E. Belding-Royer, 'Authenticated Routing for Ad Hoc Networks', IEEE J. Selected Areas Comm., Vol. 23, No. 3, Mar. 2005, pp. 598-610.

[74] Y.-C. Hu, D.B. Johnson, A. Perrig, 'SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks', 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), 2002, pp. 3–13.

[75] Seung Yi, Prasad Naldurg, Robin Kravets, 'Security-Aware Ad hoc Routing for Wireless Networks', University of Illinois at Urbana-Champaign, Champaign, IL, 2001.

[76] S. Sharma, Rajshree, R. P. Pandey, V. Shukla, 'Bluff-Probe Based Black Hole Node Detection and prevention', Advance Computing Conference, IACC 2009, IEEE International. 2009.

[77] Raj Shree, Ravi Prakash Pandey, 'Security Advancement in ZRP Based Wireless Networks', Lambert Academic Publishing, ISBN: 978-3-659-50041-1, 2014.

[78] Shree, R., Dwivedi, S.K., Pandey, R.P., 'Design Enhancements in ZRP for Detecting Multiple Blackhole Nodes in Mobile Ad Hoc Networks', International Journal of Computer Applications, Vol. 18(5), 2011, pp. 6–10.

[79] Kargl, F., Gei, A., Schlott, S., Weber, M., 'Secure dynamic source routing' 38th Hawaii International Conference on System Sciences (HICSS-38), Hilton Waikoloa Village, HA 2005.

[80] Hu YC, Perrig A, Davic B. Johnson, 'Ariadne: a secure on-demand routing protocol for ad hoc networks', ACM conference on mobile computing and networking (Mobicom), 2002, pp. 12–23.

[81] Rajshree, Ravi Prakash Pandey, Sanjeev Sharma, Vivek Shukla, 'A Secure Hybrid Routing Information Protocol for WSN', Chapter 6, Strategic Pervasive Computing Applications: Emerging Trends, 2010, DOI: 10.4018/978-1-61520-753-4.ch006.

[82] P. Papadimitratos, Z. Haas, 'Secure Link State Routing for Mobile Ad Hoc Networks', IEEE Wksp. Security and Assurance in Ad Hoc Networks, 2003.

[83] Dong Chen, Guiran Chang, 'A Survey on Security Issues of M2M Communications in Cyber-Physical Systems', KSII Transactions On Internet And Information Systems, Vol. 6, No. 1, Jan 2012, pp. 24-45, DOI: 10.3837/tiis.2012.01.002.

[84] C. Hsueh , Y. Li , C. Wen and Y. Ouyang, 'Secure adaptive topology control for wireless ad-hoc sensor networks', Sensors, Vol. 10, No. 2, 2010, pp.1251 -1278.

[85] T. Zia, A. Zomaya, 'Security issues in wireless sensor networks', International Conference on Systems and Networks Communication (ICSNC 2006), 2006.

[86] Obaidat, M.S., Woungang, I., Dhurandher, S.K., Koo, V., 'Preventing packet dropping and message tampering attacks on AODV-based Mobile Ad Hoc Networks', Computer, Information and Telecommunication Systems (CITS), 2012 IEEE International Conference on, ISBN: 978-1-4673-1549-4, 2012, pp. 1-5, DOI: 10.1109/CITS.2012.6220366.

[87] Wesam S. Bhaya, Suad A. Alasadi, 'Security against Spoofing Attack in Mobile Ad Hoc Networks', European Journal of Scientific Research, ISSN 1450-216X, Vol.64, No.4, 2011, pp. 634-643.

[88] Hu Yih-Chnu, Perrig Adrian, Jonhson David B., 'Wormhole attacks in wireless networks', IEEE Journal on Selected Areas in Communication Vol. 24(2), 2006, pp.370–80.

[89] Gorlatova MA, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, 'Detecting wormhole attacks in mobile ad hoc networks through protocol breaking and packet timing analysis', In the proceedings of the IEEE conference on military communications, 2006.

[90] Capkun, S., Buttyán, L. and Hubaux, J., 'SECTOR: secure tracking of node encounters in multi-hop wireless networks', Proceedings of ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 2003, pp.21–32.

[91] Jan vonMulert, IanWelch, WinstonK.G.Seah, 'Security threats and solutions in MANETs: A case study using AODV and SAODV', Journal of Network and Computer Applications, 35, 2012, pp. 1249–1259.

[92] B. Bellur, R.G. Ogier, 'A reliable, efficient topology broadcast protocol for dynamic networks', 18th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'99), March 1999, pp. 178-186.

[93] Adrian Perrig, Ran Canetti, Doug Tygar, Dawn Song, 'Efficient Authentication and Signature of Multicast Streams over Lossy Channels', IEEE Symposium on Research in Security and Privacy, May 2000, pp. 56–73.

[94] I. Khalil, S. Bagchi, N. B. Shroff, 'Liteworp:Detection and isolation of the wormhole attack in static multihop wireless networks', Computer Networks, Vol. 51, 2007, pp. 3750–3772.

[95] I. Krontiris, T. Giannetsos, T. Dimitriou, 'Launching a Sinkhole attack in wireless sensor networks; the intruder side', WIMOB '08, 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication,

IEEE Computer Society, Washington, DC, USA, ISBN 978-0-7695-3393-3, 2008, pp. 526–531.

[96] J. Eriksson, S. Krishnamurthy, M. Faloutsos, 'TrueLink: A practical countermeasure to the wormhole attack in wireless networks', Proceedings of the 2006 IEEE International Conference on Network Protocols, IEEE Computer Society, Washington, DC, USA, ISBN: 1-4244-0593-9, 2006, pp. 75–84, http://dl.acm.org/citation.cfm?id=1317535.1318358.

[97] Y.C. Hu, A. Perrig, D.B. Johnson, 'Packet leashes: a defense against wormhole attacks in wireless networks', Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, INFOCOM, IEEE Societies, Vol. 3, IEEE Computer Society, San Fransisco, California, USA, 2003, pp. 1976–1986.

[98] G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, J. Lees, 'Deploying a Wireless Sensor Network on an Active Volcano', IEEE Internet Computing, ISSN: 1089-7801-10, 2006, pp. 18–25, http://dx.doi.org/10.1109/MIC.2006.26.

[99] T. Schmid, H. Dubois-Ferrière, M. Vetterli, 'SensorScope: Experiences with a wireless building monitoring sensor network', Workshop on Real-World Wireless Sensor Networks, REALWSN'05, ACM, Stockholm, Sweden, 2005.

[100] D.B. Johnson, D.A. Maltz, Y.C. Hu, 'The dynamic source routing protocol for mobile ad hoc networks (DSR)', Tech. Rep. IETF MANET Working Group, 2007, http://tools.ietf.org/html/rfc4728.

[101] C.E. Perkins, E.M. Royer, 'Ad-hoc on-demand distance vector routing', Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA'99, IEEE Computer Society, New Orleans, Louisiana, USA, 1999, pp. 90–100.

[102] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, 'LITEWORP: a Lightweight countermeasure for the wormhole attack in multihop wireless networks', 2005 international conference on dependable systems and networks (DSN'05), 2005.

[103] Johnson DB, Maltz DA, Hu YC, 'The dynamic source routing protocol for mobile ad-hoc network (DSR)', IETF internet draft, July 2004.

[104] Ning Song, Lijun Qian, and Xiangfang Li, 'Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach', In the proceedings of the 19th IEEE international parallel and distributed processing symposium (IPDPS'05), 2005.

[105] Hon Sun Chiu, King-Shan Lui, 'DelPHI: wormhole detection mechanism for ad hoc wireless networks', In the proceedings of the 1st international symposium on wireless pervasive computing, 2006.

[106] Gunhee Lee, Dong-kyoo Kim, Jungtaek Seo, 'An approach to mitigate wormhole attack in wireless ad hoc networks' In the proceedings of the international conference on information security and assurance; 2008. pp. 220–5.

[107] Xu Su , Rajendra V. Boppana, 'On mitigating in-band wormhole attacks in mobile ad hoc networks', IEEE international conference on communications, 2007, pp.1136–41.

[108] Farid Naıt-Abdesselam, Brahim Bensaou, Jinkyu Yoo, 'Detecting and avoiding wormhole attacks in optimized link state routing protocol', IEEE conference on wireless communications and networking, 2007, pp.3117–22.

[109] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff, 'MOBIWORP: mitigation of the wormhole attack in mobile multihop wireless networks', In the IEEE securecomm and workshops, 2006, pp. 1–12.

[110] Xia Wang and Johnny Wong, 'An end-to-end detection of wormhole attack in wireless ad-hoc networks', 31st annual international computer software and applications conference (COMPSAC), 2007.

[111] Lazos L, Poovendran R, Meadows C, Syverson P, Chang LW, 'Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach', IEEE conference on wireless communications and networking, Vol. 2., 2005, pp. 1193–9.

[112] Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F, Magdy S. El-Soundani, 'Intrusion detection for wormhole attacks in ad hoc networks a survey and a proposed decentralized scheme', IEEE international conference on availability, reliability and security, 2008, pp.636–41.

[113] Xia Wang, 'Intrusion detection techniques in wireless ad hoc networks', IEEE international computer software and applications conference, 2006.

[114] Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, Heejo Lee, 'Transmission time-based mechanism to detect wormhole attacks', IEEE Asia-Pacific service computing conference, 2007, pp.172–8.

[115] Ralph C. Merkle, Protocols for Public Key Cryptosystems, IEEE Symposium on Security and Privacy, 1980.

[116] Khabbazian, M., Mercier, H., & Bhargava, V.K., 'Wormhole attack in wireless ad hoc networks: Analysis and countermeasure', Proceedings of Global Telecommunications Conference, GLOBE-COM'06, IEEE, 2006.

[117] Ming-Yang Su, 'WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks', computers & security, 29, 2010, pp. 208 – 224.

[118] Yu Yao, Lei Guo, Xingwei Wang, Cuixiang Liu, 'Routing security scheme based on reputation evaluation in hierarchical ad hoc networks', Computer Network, 54, 2010, pp. 1460–1469.

[119] Qian, L.J., Song, N., Li, X.F., 'Detection of wormhole attacks in multipath routed wireless ad hoc networks: a statistical analysis approach', J. Network Comput. Appl., Vol. 30(1), 2007, pp. 308-330, doi:10.1016/j.jnca.2005.07.003.

[120] L. F. Garcia, J. M. Robert, 'Preventing layer-3 wormhole attacks in ad-hoc networks with multipath DSR', IEEE Ad Hoc Networking Workshop (Med-Hoc-Net 2009), 2009, pp. 15-20.

[121] Prasannajit B, Anupama, Vindhykumari, Subhashini, Vinitha, 'An Approach Towards Detection Of Wormhole Attack in Sensor Networks', Integrated Intelligent Computing (ICIIC), 2010 First International Conference on, IEEE , E-ISBN 978-0-7695-4152-5, pp 283-289.

[122] Znaidi W, Minier M, Babau J-P. 'Detecting wormhole attacks in wireless networks using local neighborhood information', IEEE 19th international symposium on

personal, indoor and mobile radio communications, 2008, PIMRC 2008, 2008. pp. 1-5.

[123] D. Dong, M. Li, Y. Liu, X. Y. Li, X. Liao, 'Topological detection on wormholes in wireless ad hoc and sensor networks', 17th IEEE International Conference on Network Protocols (ICNP '09), October 2009, pp. 314–323.

[124] E. A. Panaousis, L. Nazaryan, C. Politis, 'Securing aodv against wormhole attacks in emergency manet multimedia communications', Mobimedia '09, 5th International ICST Mobile Multimedia Communications Conference. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, pp. 1-7.

[125] Thanassis Giannetsos, Tassos Dimitriou, 'LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks', Journal of Computer and System Sciences, Vol. 80, 2014, pp. 618–643.

[126] Radu Stoleru, Haijie Wu, Harsha Chenji, 'Secure neighbor discovery and wormhole localization in mobile ad hoc networks', Ad Hoc Networks, Vol.10, 2012, pp. 1179–1190.

[127] Clausen T, Jacquet P., 'Optimized link state routing protocol (OLSR)', 3626. IETF RFC; October 2003.

[128] Hu L, Evans D., 'Using directional antennas to prevent wormhole attacks', Proceedings of the network and distributed system security symposium, San Diego, CA, USA, 2004.

[129] Kimaya Sanzgiri, Bridget Dahill, Brain Neil Levine, Clay Shields, Elizabeth Belding-Royer, 'A Secure routing protocol for ad hoc networks', 10th IEEE international conference on network protocols (ICNP), November 2002.

[130] Zapata, MG, Asokan N., 'Securing ad-hoc routing protocols', ACM workshop on wireless Security (WiSe), Sept 2002.

[131] Mahesh K. Marina and Samir R. Das, 'On-demand multipath distance vector routing in ad hoc networks', IEEE international conference on network protocols (ICNP), 2001, pp.14–23.

[132] Elizabeth M. Belding-Royer, Charles E. Perkins, 'Evolution and future directions of the ad hoc on-demand distance-vector routing protocol', Ad Hoc Networks, Vol.1, 2003, pp. 125–150, doi:10.1016/S1570-8705(03)00016-7.

[133] Safdar Ali Soomro, Sajjad Ahmed Soomro, Abdul Ghafoor Memon, Abdul Baqi, 'Denial of Service Attacks in Wireless Ad hoc Networks', Journal of Information & Communication Technology, Vol. 4, No. 2, 2010, pp. 01-10.

[134] Wang W, Bhargava B, Linderman M, 'Defending against Collaborative Packet Drop Attacks on MANETs', the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009.

[135] Dhane, A., Sharma, S, 'Modeling and analysis of Sequence Number Attack and its detection in AODV', 16th IEEE International Conference on Networks, ICON 2008.

[136] P-W. Yau, S. Hu, C. J. Mitchell, 'Malicious attacks on ad hoc network routing protocols', International Journal of Computer Research, Vol. 15, No 1, 2007, pp. 73-100.

[137] Villanueva-Cruz J.A., Cahue-Díaz G., García-Hernández C.F., González-Serna J.G., Pérez-Díaz J.A., 'Security in AODV Protocol Routing for Mobile ad hoc Networks', Ingeniería Investigación y Tecnología. Vol. XII, Núm. 1, ISSN 1405-7743, FI-UNAM, 2011, pp.15-24,

[138] Shashi Gurung, Dr. Krishan Kumar Saluja, 'Mitigating Impact of Blackhole Attack in MANET', Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC, Association of Computer Electronics and Electrical Engineers, 2014, pp. 229-237, DOI: 02.ITC.2014.5.560.

[139] S.Santhi, Dr.G.Sudha Sadasivam, 'Power Aware Qos Multipath Routing Protocol For Disaster Recovery Networks', International Journal of Wireless & Mobile

Networks (IJWMN) Vol. 3, No. 6, December 2011, pp.47-57, DOI : 10.5121/ijwmn.2011.3604 47.

[140] http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf

[141] http://www1.i2r.a-star.edu.sg/~tanhx/research/Guide%20to%20GloMoSim.pdf

[142] http://www.robertoverdone.org/uploads/teaching/QualNet-5%201-UsersGuide.pdf

[143] http://www.sce.carleton.ca/faculty/lambadaris/courses/5001/opent_tutorial.pdf

[144] N. Sarkar and S. Halim, 'A Review of Simulation of Telecommunication Networks: Simulators, Classification, Comparison, Methodologies, and Recommendations', Journal of Selected Areas in Telecommunications (JSAT), March 2011.

[145] Radha Poovendran, Loukas Lazos, 'A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks', Wireless Networks, Volume 13, Issue 1, February 2007, pp. 27-59.

[146] C. R. Kothari, 'Research Methodology, Methods & Techniques', Chapter 9, Testing of Hypothesis 1 (Parametric or Standard Tests of Hypothesis), ISBN 81-224-1522-9, pp. 184-232.

Appendix-A

ABBREVIATIONS

4G	- Fourth Generation
ACK	- Acknowledgement
ADMR	- Adaptive Demand-Driven Multicast Routing protocol
AMD	- Advanced Micro Devices
AODV	- Ad hoc On-Demand Distance Vector
AODV-UU	- AODV by Uppsala University
ARAN	- Authenticated Routing for Ad hoc Networks
CMU	- Carnegie Mellon University
CS	- Specific Coefficient
CSMA	- Carrier sense multiple access
CSMA/CA	- Carrier Sense Multiple Access/Collision Avoidance
DARPA	-Defense Advanced Research Projects Agency
DelPHI	- Delay Per Hop Indication
DN	- Destination Node
DoD	-Department of Defense
DOS	- Denial of Service
DSDV	- Destination Sequenced Distance Vector Protocol
DSR	- Dynamic Source Routing
EDWA	- End-To-End Detection of Wormhole Attack
ELB ACTD	- Expanding the Littoral Battle-Space Advanced Concept Technology Demonstration
FDR BAA	- Future Digital Radio Broad Area Announcement
FN	- False Node
GloMo	- Global Mobile
GloMoSim	- Global Mobile Information Systems Simulator

GPS	- Global Positioning System
GUI	- Graphical User Interface
HC	- Hop Count
HNA Message	- Host Network Announcement Message
IDS	- Intrusion Detection System
IEEE	-Institute of Electrical and Electronics Engineers
IETF	- Internet Engineering Task Force
IMEP	- Internet MANETs Encapsulating Protocol
IN	- Intermediate Node
IoT	- Internet of Things
IP	- Internet Protocol
ISI	- Information Sciences Institute
IS-IS	- Intermediate System
LAN	- Local Area Network
LAR	- Location-Aided Routing
LDAC	- Localized-Decentralized Algorithm for Countering Wormholes
LOS	- Line of Sight
LPR	- Low-cost Packet Radio
MAC	- Medium Access Control
MACT	- Multicast Activation
MAD	- Mutual Authentication with Distance Bounding
MANET	- Mobile Ad hoc Network
MAODV	- multicast ad hoc on-demand distance vector
MDS	- Multidimensional Scaling
MEGACOP	- Media Gateway Control protocol
MGCP	- Media Gateway Control Protocol
MMWN	- Multimedia Mobile Wireless Network
MPRs	- Multipont Relays

MSDN - Mobile Secure Neighbour Discovery

NS2 - Network Simulator 2

NTDR - Near Term Digital Radio

ODMRP - On-Demand Multicast Routing Protocol

OLSR - Optimized Link State Routing Protocol

OLSRd - OLSR daemon

OPNET - Optimized Network Engineering Tools

OSPF -Open Shortest Path First

OTH - Over The Horizon

PCMCIA - Personal Computer Memory Card International Association Cards

PDR - Packet Delivery Ratio

PRNet - Packet Radio Network

QoS - Quality of Service

RERR - Route Error

RIP - Routing Information Protocol

RREP - Route Reply

RREQ - Route Request

RTT - Round Trip Time

SAM - Statistical Analysis of Multipath

SAODV - Secure Ad hoc On-Demand Distance Vector

SAR - Security-Aware Ad hoc Routing Protocol

SCTP - Stream Control Transmission Protocol

SDK - software development kit

SDR - Software Defined Radios

SDSR - Secure Dynamic Source Routing

SEAD - Secure Efficient Ad hoc Distance Vector Routing Protocol

SIP - Session Initiation Protocol

SLSP - Secure Link State Routing Protocol

SMR	- Split Multipath Routing
SN	**-** Source Node
SNT	- Scalable Network Technology
SRIP	- Secure Routing Information Protocol
STAR	- Source Tree Adaptive Routing
STCD	- Space & Terrestrial Communications Directorate
SURAN	- Survivable Radio Network
SZRP	- Secure Zone Routing Protocol
TBRPF	- Topology Dissemination Based on Reverse-Path Forwarding
TC Message	- Topology Control (TC) messages
TDMA	- Time division multiple access
TI	- Tactical internet
TIK	- TESLA with instant key disclosure
TORA	- Temporally-Ordered Routing Algorithm
TTL	- Time to Live
TTM	- Transmission Time based Mechanism
UCB	- University of California, Berkeley
UCLA PCL	- University of California, Los Angeles Parallel Computing Laboratory
UCSC	- University of California, Santa Cruz
VRC-99A	- Vehicular Radio Communication
WARP	- Wormhole-Avoidance Routing Protocol
WIM-DSR	- Witness Integration Multipath DSR
WINGs	- Wireless Internet Gateways
WRP	- Wireless Routing Protocol
ZRP	- Zone Routing Protocol