SUMMARY OF 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

TABLE OF CONTENTS

1.1 Introduction

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, 4], 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 [1, 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 [4, 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 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.

1.3 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.

1.4 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.

1.5 Research Contributions

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'. The developed algorithm is given below:-

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.

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 above. 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 figure1 given below:-

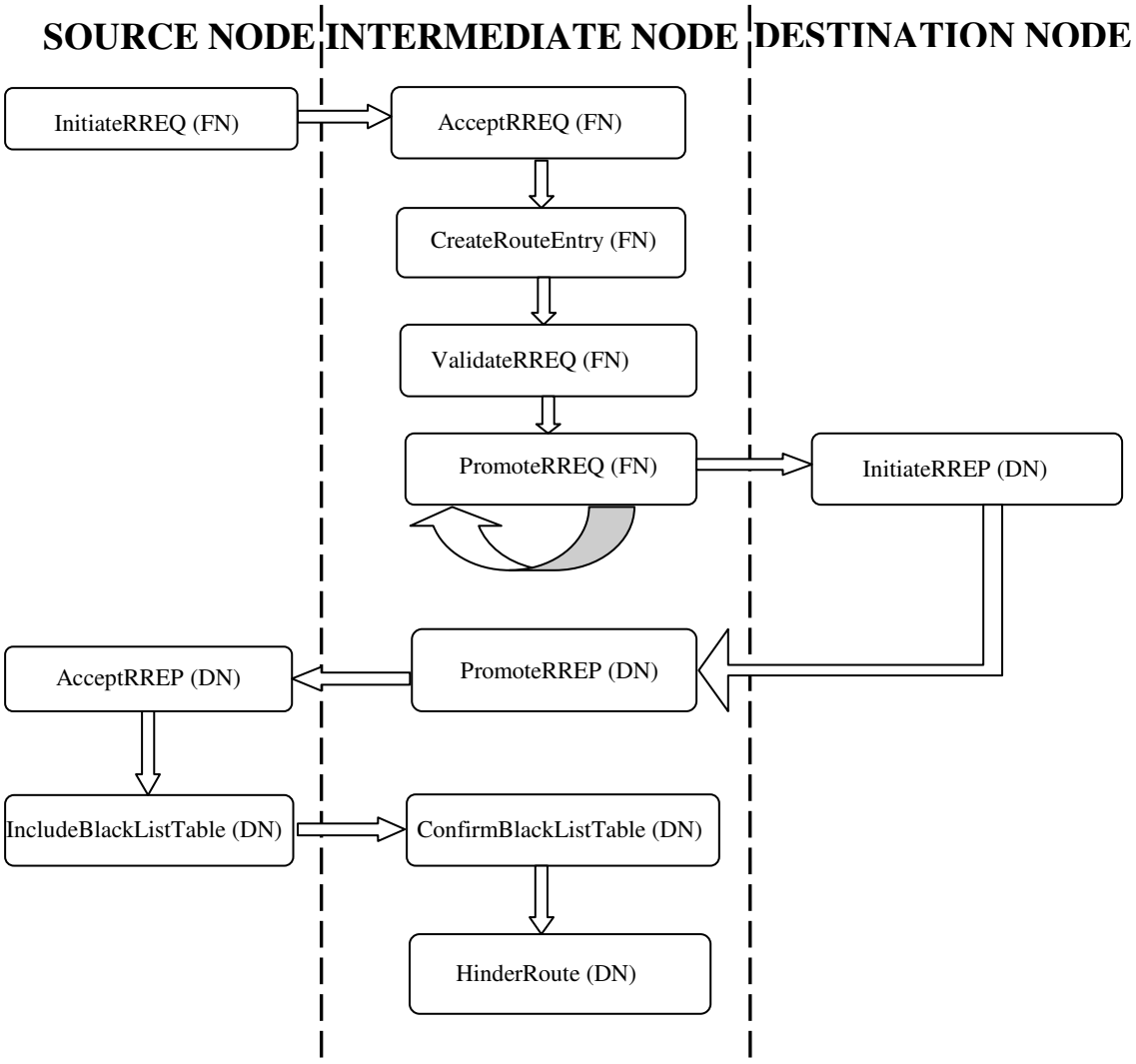

Figure1: Flow Chart showing Working of SAODV

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.

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.

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.

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.

Hypothesis Testing for In-Band Wormhole Attack

It is mandatory to check the validity of the proposed framework for acceptance. The corollary 1 [39] has been introduced to test the significance of the framework.

H0: (Null Hypothesis): Wormhole Nodes identified using corollary 1 [39] 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, 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:-

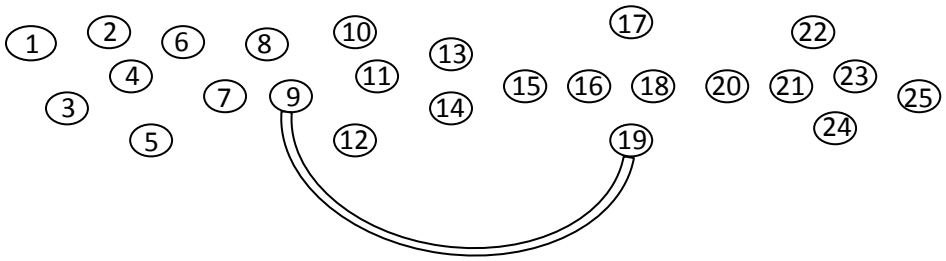

Figure2: A Wireless Ad hoc Network with In-Band Wormhole Attack

From figure2, 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:-

$$G_9 = 000000110111000000000000$$
$$C_9 = 000000110111000001000000$$
$$\oplus = 000000000000000001000000$$

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)

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.

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:-

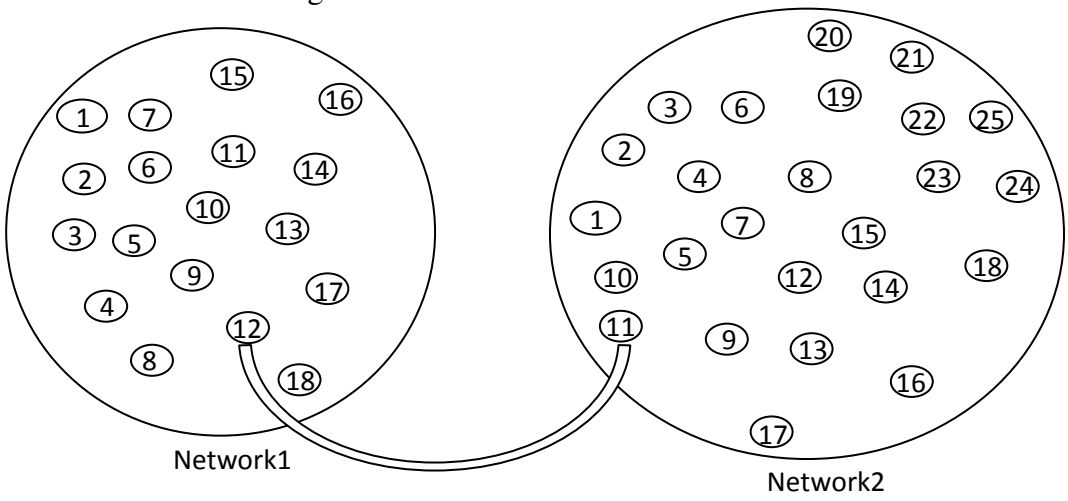

Figure3: A Wireless Ad hoc Network with Out-of-Band Wormhole Attack

From figure3, 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
$\oplus$ = 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 $\mu 0$ = 12, 11……..(3)

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 $\mu 1$ = 12, 11…….(4)

From the equations 3 and 4, it is shown that the value of $\mu 0$ and the value of $\mu 1$ are same. These same values are 12 & 11.

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.

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 [40]. 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.

The t-test history for in-band wormhole attack of packet delivery ratio is given in Table1.

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				

.

Table1: 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.

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 [40]. 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.

The t-test history for out-of-band wormhole attack of packet delivery ratio is given in Table2.

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				

Table2: 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.

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 [40]. 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.

The t-test history for in-band wormhole attack of end-to-end delay is given in Table3.

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				

Table3: 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.

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 [40]. 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.

The t-test history for out-of-band wormhole attack of End-to-End Delay is given in Table4.

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: 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.

1.6. 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.

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.

1.7 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.

1.8 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.

1.9 Thesis Outline

The thesis has five chapters. Chapter wise summary is as follows:-

Chapter 1: Introduction

This 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: Wormhole Attack in Ad Hoc Network: A Review

This chapter 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: Proposed Methodology

This chapter shows the major contribution by researcher in the form of SAODV to mitigate wormhole attack in ad hoc networks.

Chapter 4: Implementation and Validation

The implementation of SAODV in presence of in-band wormhole attack and out-band wormhole attack is described and results validation in Chapter 4.

Chapter 5: Conclusion & Future Work

Conclusions with major findings are drawn in chapter 5 along with discussion of potential future work followed by references and appendix A that includes the abbreviations.

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] 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.

[40] 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.

List of Publications

- **An Assessment of Frequently Adopted Security Patterns in Wireless SensorNetwork: Requirement and Security Management Perspective**, **International Journal of Advances Computer Engineering and Architecture**, ISSN-22489452, Volume 1, Number 2, 2011, pp. pp. 129-138.
- **MFCC and Prosodic Feature Extraction Techniques: A Comparative Study, International Journal of Computer Applications**, 9789380747972, **pp. 9-13.**
- **The Economic Impact of Cyber Crime and Future Challenges,** National Seminar on History of Crime and Economy in Existing Society and Future Challenges,

organized by AIRO in association with Department of Ancient Indian History and Archaeology, University of Lucknow, LKO, on 12/11/13 to 13/11/13.

- **Track Down Worm Hole Attack in WSN,** International Conference on Nanoscience and Nanotechnology, organized by Department of Physics, BBAU, LKO on 18/11/13 to 20/11/13.
- **Equal Error Rate and Audio digitization and Sampling Rate for Speaker Recognition System,** International Conference on Nanoscience and Nanotechnology, organized by Department of Physics, BBAU, LKO on 18/11/13 to 20/11/13.
- **Detection of Wormhole Attack in Distributed Wireless Environment,** 8th National Conference on "Thermodynamics of Chemical, Biological and Environmental Systems-2013", organized by Department of Applied Chemistry, BBAU, Lucknow on 25/12/13 to 26/12/13.
- **Attacks in Mobile Ad hoc Networks,** International Conference on Emerging Technologies in Electronics and Communication, at GNDU Amritsar, 20/12/23to 22/12/23.
- **Layered Based Classification for Various Attacks in Mobile Ad-Hoc Networks,** 5th National Conference on Nanotechnology & Materials Science, organized by Department of Physics, University of Lucknow on 21/12/13 to 23/12/13.
- **Applications of Speaker Recognition,** Procedia Engineering of Elsevier, ISSN: 18777058, **pp. 3122-3126.**
- **Equal Error Rate and Audio Digitization and Sampling Rate for Speaker Recognition System (1085-88), Advanced Science Letters,** ISSN: 1936-6612 (Print): EISSN: 1936-7317 (Online).
- **Detection of Wormhole Attack in Mobile Ad hoc Network,** Women Science Congress, 101st Indian Science Congress, organized by University of Jammu, Jammu, on 03/02/14 to 07/02/14.
- **Characteristics of Mobile Ad hoc Networks,** International Conference on Scientific and Technological Advancements: Social Issues and Health Concerns, organized by School of home science, BBAU, LKO on 18/02/14 to 19/02/14.
- **Cyber Terrorism: A Latest Challenge for Society,** National Conference on Youth, Naxalism and Terrorism, organized by Department of Sociology, BBAU, Lucknow on 21/02/14 to 22/02/14.

- **Simulation of SAODV under Wormhole Attack in MANETs,** national Conference on Information Security Challenges, by deptt. Of IT, BBAU, Lucknow, 28/03/14.
- **Design Enhancements in AODV to Detect Wormhole Node in Wireless Networks,** National Conference on Leveraging Science and Innovation for Development, organized by BBAU, Lucknow on 27/03/14 to 28/03/14.