A Novel Scheme of Detection and Eradication of Wormhole Attack

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted By

Svarika Goyal

(801333028)

Under the supervision of:

Dr. Anil Kumar Verma

Associate Professor

&

Ms. Tarunpreet Bhatia

Lecturer

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

May 2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*A Novel Scheme of Detection and Eradication of Wormhole Attack*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Anil Kumar Verma and Ms. Tarunpreet Bhatia* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Svarika Goyal

Svarika Goyal

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

(Ms. Tarunpreet Bhatia)
Lecturer
Computer Science and Engineering
Thapur University

(Dr. Anil Kumar Verma)
Associate Professor
Computer Science and Engineering
Thapur University

Countersigned by

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapur University
Patiala

(Dr. S. S. Bhatia)
Dean (Academic Affairs)
Thapur University
Patiala

ACKNOWLEDGEMENT

No volume of words is enough to express my gratitude towards my guides, ***Dr. Anil Kumar Verma****, Associate Professor and* ***Ms. Tarunpreet Bhatia****, Lecturer, Computer Science and Engineering Department, Thapar University, who have been very concerned and has supervised the work presented in this thesis report. They have helped me to explore this vast field in an organized manner and provided me with all the ideas on how to work towards a research oriented venture.*

I am also thankful to ***Dr. Deepak Garg****, Head of Department, CSED and* ***Ms. Jhilik Bhattacharya****, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.*

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thanks my ***parents****,* ***friends*** *and the* ***almighty*** *for showing me the right direction out of the blue, to help me to stay calm in the oddest of the times and keep moving even at times when there was no hope.*

Svarika Goyal

(801333028)

ABSTRACT

Wireless Sensor Networks are one of the research areas which are continuously explored by researchers. There are multifaceted applications associated with them. The smart sensor nodes are the building blocks of WSN. These are capable of processing and computations but are shorten of resources. As security consideration is not given to WSN; these are prone to various threats.

One of the attacks is wormhole attack subjected for replaying and data drop; causing destruction in networks. A lot of exploration has been done by research scholars to deal with security affairs. Although, various routing techniques cropped with security mechanisms but still the problem is not vanished. There is an urgent demand of robust security mechanism for WSN to be more reliable.

In this thesis, a wormhole detective scheme is proposed. Scheme has advantages of not using hardware or any synchronization. The simulation is done on NS2. The network parameters have been evaluated. The results of simulation verified the functioning of nominated scheme.

Keywords: WSN, AODV, Wormhole Attack, NS2

TABLE OF CONTENTS

ANNEXTURES

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ADC	Analog to Digital Convertor
AODV	Ad-hoc On-Demand Distance Vector
CBR	Continuous Bit Rate
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
DARPA	Defense Advanced Research Project Agency
DSN	Distributed Sensor Networks
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
NAM	Network Animator
NRL	Normalized Routing Load
NS	Network Simulator
OTcl	Object Oriented Tool Command Language
PDR	Packet Delivery Ratio
RREQ	Route Request
RREP	Route Reply
RERR	Route Error
RRT	Round Trip Time
Seq	Sequence Number

Tcl	Tool Command Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VINT	Virtual Internetwork Test-bed
WSN	Wireless Sensor Networks

CHAPTER 1

INTRODUCTION

1.1 Introduction to Wireless Networks

In this 21st century, there are various electronic devices including smart phones, RFID and various other intelligent devices which are admired by common man these days. These devices are mobile in nature and small in size but have the capacity of a large device. Micro electro mechanical systems make possible for small and smart sensors to be deployed at any place. Wireless communication helps these smart sensor sensors to have wide range of applications ranging from military applications to industry control etc.

The major revolution in networking is caused by wireless networks. To have significant development in these networks exhaustive research has been going on for the decades and because wireless media only it is now possible to have mobile communication. Wireless media is the sole of WSN. Wireless networks use radio frequencies, micro and millimeter wave etc for communication. As no line of sight and Omni directional links are provided by radio frequency, these form the basis of WSN.

As the wireless standard for the WSN is released in 2003, there are a lot of points to be explored in this field and one such point is of security as these networks are also hit by the attackers to cause severe threats to them. Many attacks can be deal with various approaches with taking care of the constraints associated with these networks and thus increasing networks lifetime.

1.2 Motivation

Wireless Sensor Networks are said to be the network having huge number of smart small sensors communicating wirelessly with each other and are capable of with computation limitations. Military applications used these networks initially but now these are popular in various other fields too. WSN have many different features as compare to other wireless networks. In WSN the resource starved nodes are heavily crowded, and have somewhat amount of energy and computation capacity, their development requires innovative approach. Therefore, a lot of research is done for the significant amount of development of these networks.

In present world WSNs are widely used in many of the applications but these networks are vulnerable to severe malicious activities. Wireless nature and low cost of these networks there are no such hardware which may be resistant to various attacks; these networks are easily disturbed by attackers. The malicious activities may disrupt the network behavior badly by affecting the throughput, good put and many other network parameters which necessitates security features to be prevalent in sensor networks. Though many restrictions are prevalent to have security in these networks because of their open nature and bounded resources, networks must be secure enough as these networks have potential applications in battlefield surveillance, home security and other commercial applications. Security schemes must uses optimum amount of resources including energy, less computation and bandwidth overhead and can responds against malicious activity in very less time. Therefore, network security is one of the interesting research areas which include various challenges while designing the various security mechanisms.

1.3 State of Art

There are different security schemes presented by a lot of researchers to defend against severe threats in WSN. The different security techniques are built on different concepts including cryptography, etc which are not good at resource usage and highly affect the lifetime of sensor nodes. There are various issues which need to be addressed while designing the security algorithms for WSN. These are:

- Tradeoff between the good security scheme and the resource utilization. Therefore, there is always a need to have equilibrium between the great security solution and utilization of node resources.
- Security solution for WSN is also dependent upon the hardware used at its platform.
- As the topology of the WSN is Ad Hoc in nature which attracts the attackers to perform various malicious activities including actively disrupt the network or silently listen to information flowing through network.
- As WSN’s are based on wireless transmission media, therefore wired security schemes are not able to be implemented in these networks.

- The topology of WSN is dynamic in which entrance and exit of the node is random. Therefore system dynamics creates obstacles for designing the security technique.

To defend against severe attacks different protocols have extended versions for security issues [1]. To deal with one of the severe attacks called wormhole and to have optimum use of the node resources the RTT of messages, link usage and amount of number of neighbors, etc can be helpful. As there is no hardware or fixed synchronizations these basis may provide better approach to handle wormhole attacks with more efficiency. Therefore the objective is to design the security scheme against wormhole attacks and accessing the efficiency of the scheme by evaluating the network performance metrics including throughput etc.

1.4 Thesis Outline

The organization of thesis is done in 6 chapters including Introduction, Literature Survey, Problem Statement and Objectives, Installation, Implementation and Design, Results and Performance Analysis, lastly Conclusion and Future Scope.

Chapter 1 details about WSN in terms of Motivation, succeeding with State of Art, introduction to wireless networks and Importance of study, details and finally the Thesis outline is described. Chapter 2 details the literature survey about WSN, its routing protocols and information related to WSN security issues, threat models including routing protocol, classification of attacks, wormhole attack details and schemes defending wormhole attacks. Chapter 3 details about the problem statement and objectives. Chapter 4 details the whole installation of software's, implementation part and design of proposed wormhole detection scheme. Chapter 5 details the results and performance analysis made on obtained results. Chapter 6 concludes the complete thesis with the description of future research scope.

CHAPTER 2
LITERARURE SURVEY

2.1 Wireless Sensor Networks

WSN constitutes smaller sized smart nodes which are present in large amount and with other computing devices generally said to be the base stations. These nodes interface physically with the environment, cooperate with one another, process the data and then pass to base stations for final decision making. USA National Council of Research defines WSN as follows [2]:

"Sensor networks comprises of heavily crowded small, low priced, autonomous-powered devices common for the overall electrical and mechanical systems and permeating the environment for invigilating and controlling various facets of physical world".

2.1.1 WSN Evolution

During the cold war United States [3] starts with the process of development of sensor network which was having wired media thus do not possess any constraints associated with wireless communication. The network was deployed under the ocean to locate submarines of soviet in which considerable role was assigned to human operators and the system is said to be the Sound Surveillance System.

DARPA (Defense Advanced Research Project Agency) started a program of Distributed Sensor Network (DNS) in around 1980 which was modern research initiated by the agency. This program involves communication of sensors on protocols which are at higher levels, various techniques, algorithms and software required for processing.

Nowadays, the fields of communication and computing have achieved lot developments including low cost processors, wireless transmission, small smart sensors, ad hoc continuous changing network infrastructure which leads to deployment of these networks for various monitoring, sensing applications. These days' smart homes etc are just the results of advancement of sensor networks. Now these days there is no major difference between the bandwidth provided by wired networks or wireless networks. This details how the evolvement of sensor networks takes place. There is ongoing development of sensor networks in a more efficient vision.

2.1.2 WSN Model

The model of WSN having a lot of differences than that of other ad hoc networks, former consists of nodes which are much larger in number, resource constrained and regular transform of topology. The WSN model consists of the following components as depicted in Figure 2.1.

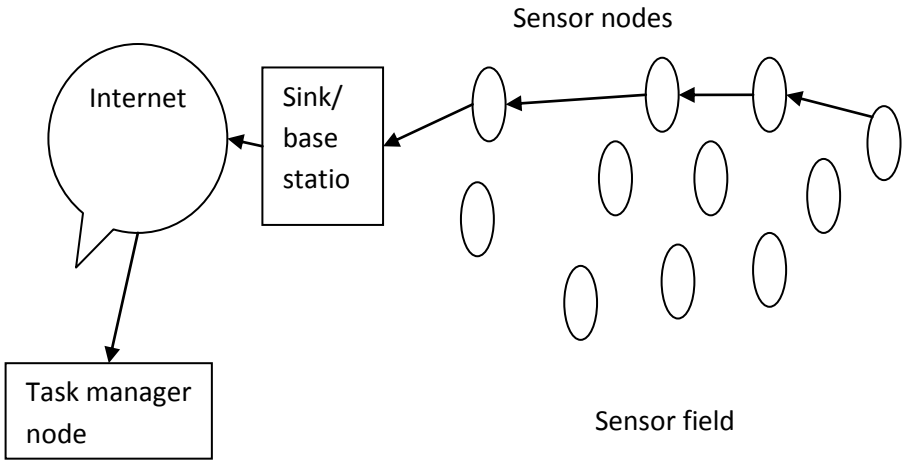

Figure 2.1 WSN Components

Sensor Field: The region for the deployment of sensor nodes.

Sensor node: Smart nodes which physically interface with environment and transmit the so collected information to the sink node.

Sink/ Base station: Aggregation points are another name for sink or base station having the job of data storage and processing that is gathered from other sensor nodes.

Task Manager: It is a high powered device or a workstation central controller of the network, responsible for extracting the information and then disseminating back to the network.

2.1.3 Sensor node of WSN

A mote is another name of sensor node as it is a small in size having technology of micro sensor and functionalities of sensing, processing and interfacing with other nodes. The typical components of sensor node include a sensor, a processor, a radio transceiver and a power supply/battery as depicted in Figure 2.2 [4].

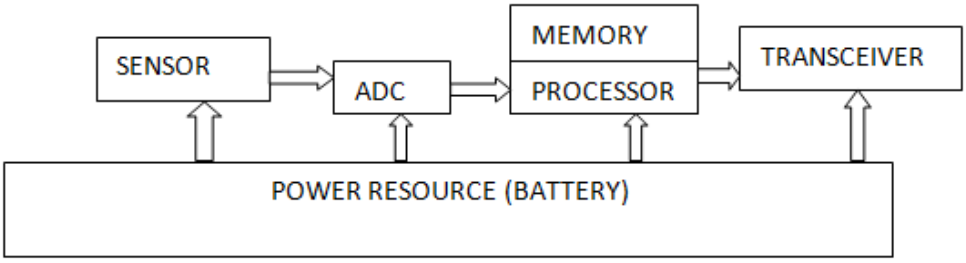

Figure 2.2 Components in Sensor node

Lifetime of the network is controlled by the power supply. Analog signals are analyzed by sensors and ADC is responsible for digitization of signals which are then processed by processor. Collaborative tasks performed by sensor nodes are managed by the memory. Radio transceivers act like a transmission media for connecting the sensor nodes to the network.

2.1.4 Wireless Sensor Node Communication Architecture: Protocol Stack

The design of the protocol stack used by wireless sensor networks is depicted in Figure 2.3. The protocol stack binds the power and location awareness, integration of data with networking protocols, communicates efficiently in terms of power through the wireless medium, and raises the collaborative efforts of sensor nodes [5]. Model also withstands the limitations of WSN.

This model of protocol stack consists of seven layers as of OSI model i.e. Application Layer, Transport Layer, Network Layer, Data link layer, Physical Layer and a Power Management Plane, Mobility Management Plane, Task Management Plane.

- **Application softwares** can be built according to the sensing applications and can be used at application layer. Application layer is responsible for forwarding the various requests from this layer to the lower layers.
- **Transport Layer** task is to maintain the flow of data if the application needed the flow control. This layer has major role when the sensor networks are accessed by the internet
- **Network Layer** task involves forwarding the information received from the transport layer by selecting the most efficient path between source and destination.

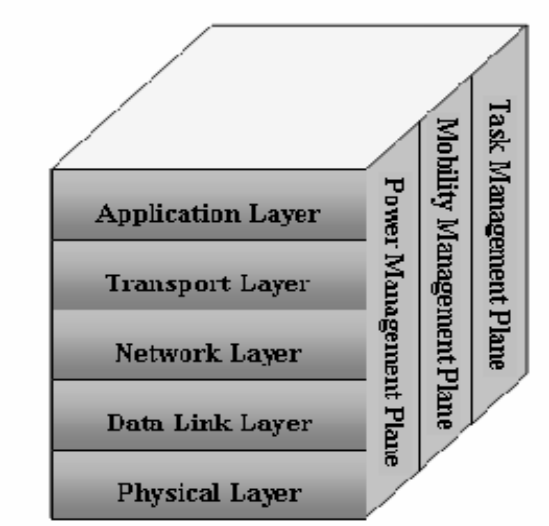

Figure 2.3 Protocol stack [6]

- **Data Link Layer** task is to the control of medium access by various nodes and error control. The medium access protocols must be able to minimize the collision and must use minimal amount of energy.
- **Physical Layer** is having responsibility for modulation, frequency generation and selection, and for various methods of receiving and transmitting the data.
- **Power management plane** task involves describing the nodes that how they can utilize their power.
- **Mobility management plane** is there for the management of mobility of sensor nodes in the network which helps the user to keep the record of the route and also enable the sensor nodes to locate their neighbor sensor nodes.
- **Task management plane** is for scheduling the sensing activities for a specific area.

2.1.5 WSN Characteristics

The various characteristics of WSN are as following:

- Sensor nodes possess very less amount of energy resource and have short life.
- There are frequent changes in topology of network.
- Nodes are heterogeneous in nature includes memory, computation power etc.
- Communication failures are one of the pro because of unbound delays in these networks.

2.2 Routing protocols in WSN

Routing is interpreted as the method to have best path to direct the data from one point to another. Network layer plays a vital role in routing. To reach the data to the sink node data travels through the multihop, therefore every intermediate node have to pass the data through. The composition and maintenance is taken care by algorithm of routing and of routing protocol. There is a difference in routing mechanisms used in wireless sensor networks as compared to traditional approaches because of their unique characteristics. The aim of WSN's is to have the data communication by extending the network life time and prevent the depletion of resources. There are many challenges associated with the design of routing protocols some of them are discussed below:

- **Energy**: Energy considerations have a vital role in establishing a route as multihop routing needs less energy with comparison to direct communication.
- **Data Gathering:** Redundant data should be aggregated at fixed point from different nodes so to avoid more number of transmissions.
- **Capabilities of node**: Routing depends upon the working of nodes as nodes performing more work can deplete its energy early as compare to those which just have functionality of sensing.
- **Data Delivery Models**: Data delivery models also decides the type of routing as in case of continuous model nodes directs the data regularly whereas driven or query driven nodes directs the data only after the occurrence of some event.
- **Deployment of node**: Node deployment can affect the routing protocol. It can be deterministic or self configurable. When there is deterministic deployment, manually nodes are deployed and data is routed according to predefinition and when nodes are placed in ad hoc fashion of self configurable network, efficient cluster head must be selected.
- **Network Dynamics:** Whether the nodes are mobile or static in nature is also one of the issues in routing.

Routing protocols can be classified according the path establishment and network structure. Figure 2.4 shows the classification of the routing protocols based on different schemes.

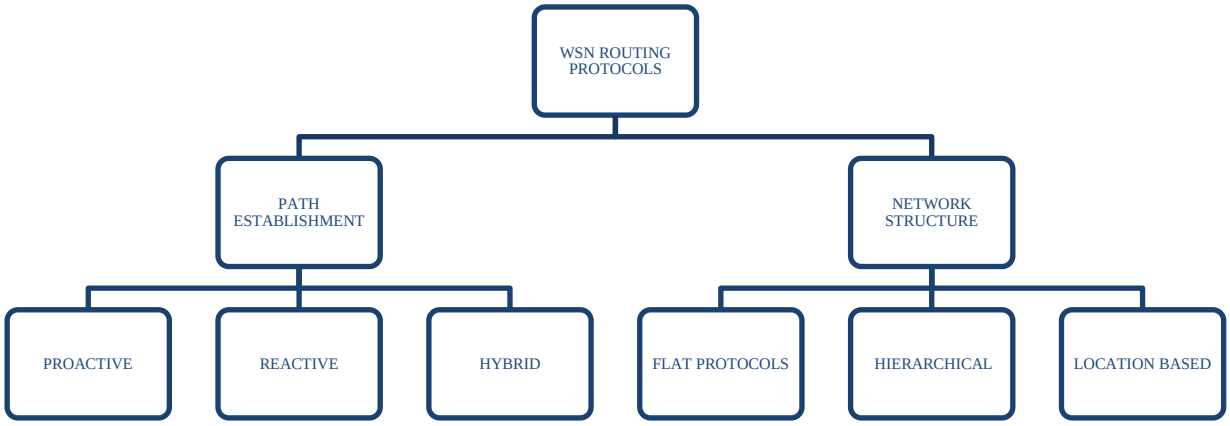

Figure 2.4 Classification of routing protocols

Based on path establishment

- **Proactive**: Sensor nodes sense the data and forwards to the sink node through a predefined path. For example LEACH (Low Energy Adaptive Clustering Hierarchy) which uses clustering hierarchy, organizing nodes into clusters and selecting one of the nodes as a cluster head.
- **Reactive**: Sensor nodes react immediately when there is a change in the sensed attribute and the value of this attribute is beyond some predefined value of threshold. For example TEEN (Threshold sensitive energy efficient sensor networks).
- **Hybrid**: It involves the concepts of reactive as well as proactive concepts. According to this scheme, protocols first compute all the routes and forward the data on the best selected path, APTEEN (Adaptive Periodic TEEN) is one such example.

Based on network structure

- **Flat (Data Centric Protocols):** As there is large number of nodes deployed in these networks, there is no identification number due to which it is difficult to select a particular set of nodes. Therefore, every sensor nodes transmits the data. In case of data centric routing, the sink node queries to the specific set of nodes and waits for the reply or data from this specific set of data. For example SPIN (Sensor Protocols for Information via Negotiation).

- **Hierarchical**: As scalability is one of the major designs consideration in WSN's the hierarchal routing is used which operates in two layer strategy. The first layer selects the cluster heads and the second layer routes the data. These protocols increase the network's lifetime, energy efficiency. LEACH, TEEN, APTEEN are examples of this routing scheme.
- **Location Based**: In this scheme, the location information of sensor nodes is required to route this information by consuming less amount of energy. Location information may be collected using GPS (Globally Positioning System) signals and by calculating the coordinates of the neighbor nodes. For example GEAR (Geographic and Energy Aware Routing).

2.3 Security in WSN

Security in WSN is required a great attention. The overall structure of network and protocols should be designed by taking security as one of the utmost important factors.

2.3.1 Security Parameters

The main aim of security is to provide privacy of the data, its chorency, the resources must be up i.e. is always available for legitimate users and most importantly the authentication of the users. The security parameters are discussed here:

- **Confidentiality**: The sensor networks must be capable of providing the privacy of the message and one such technique to achieve the same is encryption with the secret key of legitimate.
- **Integrity**: Integrity is required to make the networks reliable i.e. the message is not changed while it is on the network.
- **Authentication**: Authentication is the verification of identity of users. Authentication is achieved by MAC (message authentication codes) which is computed through secret keys shared by sender and receiver node by symmetric or asymmetric means.
- **Availability**: This is said to be that the resources and network must always be available for the legitimate users.
- **Data Freshness**: This is required in wireless sensor networks that the data must be recent i.e. attacker has not replayed the old messages.

2.3.2 Security challenges in WSN

The features of the WSN's that expose them to various types of threats are discussed.

- **Radio frequency:** The use of radio frequency makes them open to all and indirectly invites the attacker to have vicious activities.
- **Standard routing protocols**: Due to lack of security incorporation in standard routing protocols, it is easy to take the advantage of security holes in these protocols.
- **Infrastructure less networks:** As WSN are not deployed with any kind of infrastructure, therefore it is quite not possible to keep the check on them.
- **Energy limitations**: Limited resources become one of one major obstacle while designing the powerful security algorithms.
- **Low cost networks**: Tamper resistant hardware is not available for these networks which makes possible to capture the nodes physically.
- **No security mechanisms**: Major security mechanisms like frequency spread spectrum, asymmetric cryptography, etc are not there as they demand more resource absorption.

2.3.3 Threat Models

Wireless media is the foundation of WSN which causes them to expose to powerful attacks. The various categories of threat models are detailed here:

- **External and Internal Threats**: External attacks appear from apart from the network ranging from simple snooping the network traffic to abstaining of service Internal attacks appear internally from the networks like stealing the essence of legitimate nodes.
- **Mote-class and laptop-class attacker**: Mote class and other nodes possess the same capability whereas in laptop-class attackers are more dominant devices as laptops.
- **Passive and Active attacker**: Passive attackers show interest in overhearing the traffic whereas the active attackers try to breach into the network and try to alter the operation of the network. Thus, it is effortful to detect passive attacks as alteration of data is not there as compare to active threats.

2.3.4 Need of Secure Routing in WSN

WSN are only useful when producing results with more accuracy. Thus there is a requirement to guard the information against attacks. In many applications the data processing is very crucial and if the data is disrupted by the attackers it may greatly affects the performance of the corresponding application. Therefore to safeguard the WSN it is the need of the hour that the routing protocols must be able to thwart different kind of attacks and can provide as much security as they can. Furthermore, security features in these protocols to be added in such a way that they can work well with resource constrained devices and can work more efficiently by removing various attacks related to routing and thus increasing the lifetime and robustness of the whole network.

2.4 Outline of AODV (Ad-Hoc On-Demand Distance Vector) Routing Protocol

For wired or wireless networks the extensively used protocol is the AODV [7]. This protocol is efficient at determining the shortest path and consumes less power. This scheme establishes the hop to hop path between the sensors. This is more common for Ad hoc networks but is also used in WSN. The main approach included in the algorithm is the path discovery and maintaining the route discovery process. The AODV determines the route to destined node only when there is a need i.e. based on demand concept. Thus its essential goals are:

- When there is desideratum only then the broadcast discovery packets are flooded.
- To differentiate the management required for provincial i.e. neighborhood connectivity and general maintenance of network topology.
- To disperse the information regarding the alterations in provincial connectivity to those nodes who need this information.

This protocol is not devoted for the identification messages which are advertised in whole network to other nodes. HELLO message is broadcasted to locate the neighbors periodically. After receiving the reply of HELLO message the node locate its neighbors and then use the collected information for the routing process. The HELLO message is broadcasted as depicted in Figure 2.5

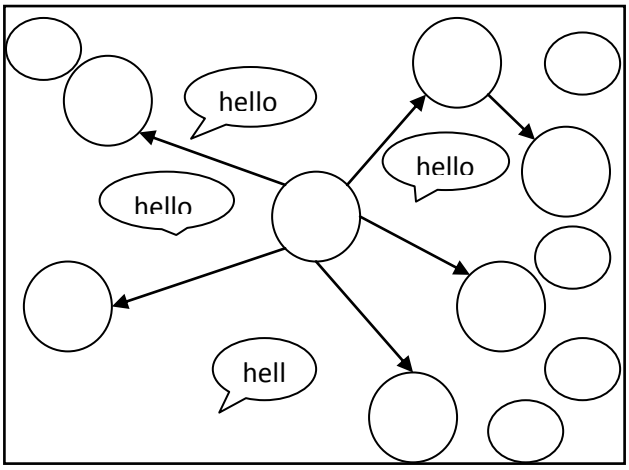

Figure 2.5 Hello packet broadcasting

Whenever the node wants to transmit the data to another node which is not in its province or neighbor, source node begin the process of locating the route and send RREQ message to local nodes and the latter one after receiving the RREQ renew the information regarding source node and in routing table create a backward link to source node. The format of RREQ is depicted in Figure 2.6.

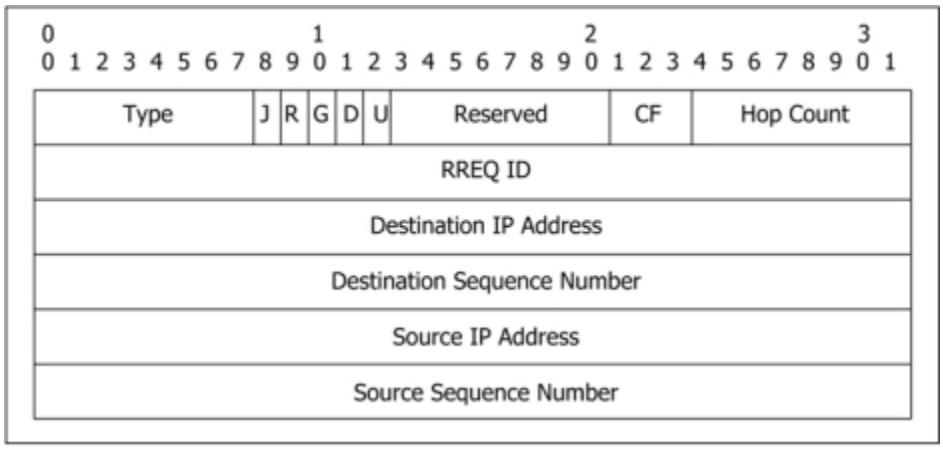

Figure 2.6 Format of RREQ [8]

In RREQ packet the IP Address and the Broadcast ID recognizes the source node. The freshness of route is uttered by sequence number of message, Higher the sequence number more the route is fresh. The count of hops from source node utters by Hop Count. Then node embraced with RREQ, it is checked by the node that whether it has already received the same RREQ, if that is the case then the RREQ is abandoned and if the RREQ is received by the intermediate node which do not have the direction of path to the destination then it is re broadcasted to the neighbor nodes. After the destination node is

with RREQ or with intermediate node which knows about the way to final node RREP is propelled back. RREP wander the same track as that of RREQ. At times of actuation of RREP pointers leading to the destination are set by intermediary nodes.

Upon receiving RREP source node verifies the routing table for the route entry, if it is not existed then refurbishment is performed. When sequence number is existed already it is to be evaluated. Further similar value of sequence number cause the route with least hop count is selected else ways sequence number with large value is indication of fresh way. Routing table entry for target node is added by source. Sketching for the same is in Figure 2.7

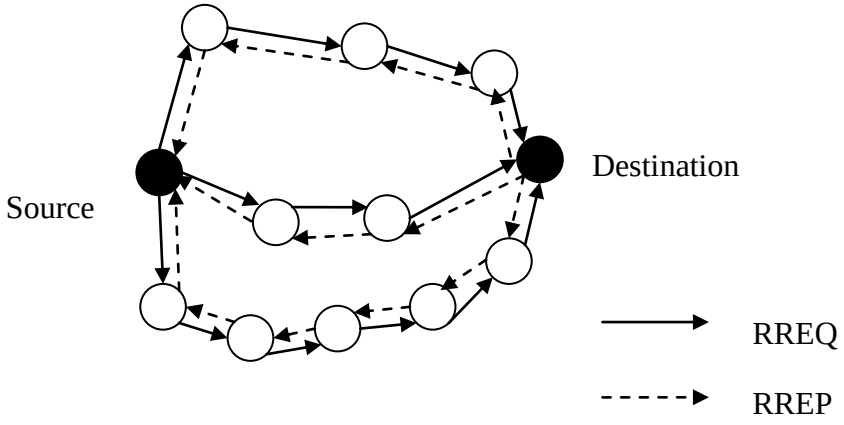

Figure 2.7 Route discoveries in AODV

Routing table updating is done whenever RREP is received and the always fresh route or low hop count route is elected. Reactive AODV aids loop free routing and effective bandwidth thus it worthwhile to be studied.

2.5 Attack Classification in WSN

The networks implementing AODV can be threatened by numerous attacks including passive and intervening. Cataloging of attacks at individual layers of OSI as depicted in Figure 2.8

Physical layer: Attacker can accomplish non mechanical attacks including wrecking of sensor nodes and professional attacks like wiretapping etc.

- **Device Tampering**: This is usually accomplished for the large set of sensor nodes and more threatening for sink nodes as the wrecking or modification of sensor nodes takes place by grabbing them physically then deriving private data.

- **Eavesdropping**: Eavesdropping exemplifies the invigilating of network traffic on the communication carrier without the acquaintance of sender and receiver.
- **Jamming**: Number of nodes is set for the attack. Jamming devices creates the noise in extremity and makes channels inaccessible for other nodes.

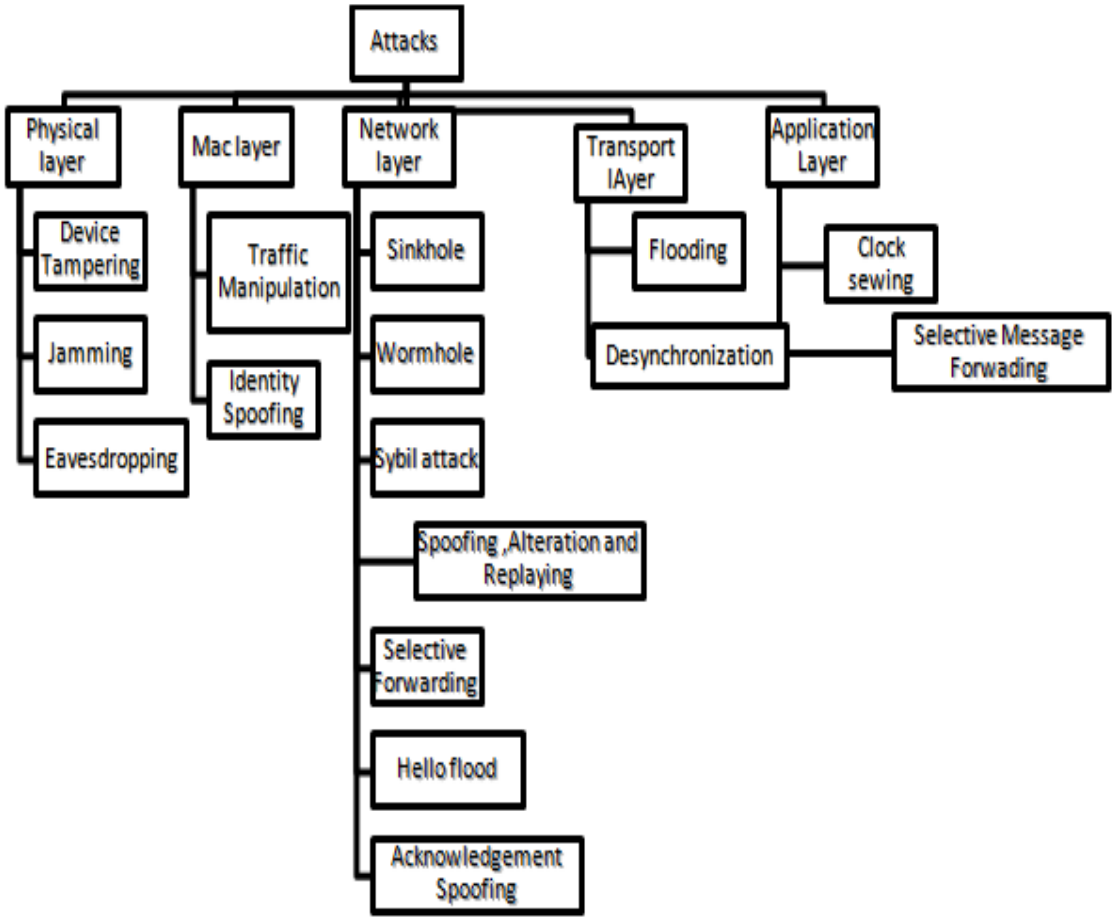

Figure 2.8 Attack Classification on layers of protocol stack

MAC layer: Customarily fooling of identities collapsing the coordination rules is done at this layer.

- **Traffic Manipulation**: Genesis of traffic is made by attackers in correspondence of legitimate users by thoroughly studying the MAC layer protocols so that auditing of network channels is done and collisions of network packets take place.
- **Identity Spoofing**: MAC identities are spoofed by attackers and pretend to be real users. Sybil attack is one of suited illustration where attacker posses multiple fake

identities at distinct locations. Identity Spoofing can be of sensor node or of base station; by spoofing the identity of base station global control of network. These are cross layer attacks as incorrect routing information is rendered by Sybil attacks.

Network layer: Selective Forwarding and manipulation of routing information are common malicious activities accomplished at this layer.

- **Spoofing, Alteration and Replaying**: Producing latency, replaying messages, loop generation and destroying routing information are usual attacks here.
- **Selective Forwarding:** Abjuring to forward the packets is done by adversary or may starts dropping. If packets are randomly forward then it is more threatening as then adversaries' detection is tough.
- **Sinkhole Attacks**: Attackers to lure the traffic from the nodes to a special node called a sink node by broadcasting the message regarding high quality route. As WSN works on base station concept these are more prone to these attacks. Some protocols are good at locate but then also by using higher devices like laptops etc can accomplish sinkhole attacks. Figure 2.9 depicts i.e. the node's' sinkhole node is accumulating the packets from ({1},{2},{4}) are destroyed and forward the data ({2}) to 'BS' i.e. base station.

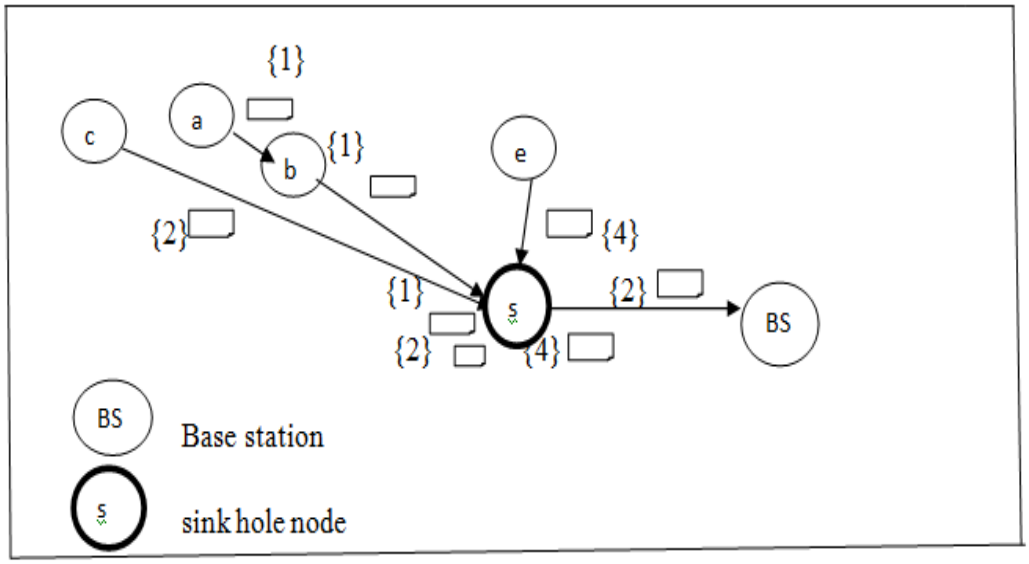

Figure 2.9 Sinkhole Attack

- **Sybil Attack**: Bad node represents itself with multiple forged identities. Fault toughness, scattered storage [9], retainment of structure [10] etc. is distressed the most. Location and geographic based protocols are the major hit points for them. Figure 2.10 depicts the behavior of bad node ‘m’ possessing of similar identities displaying bogus high quality route.

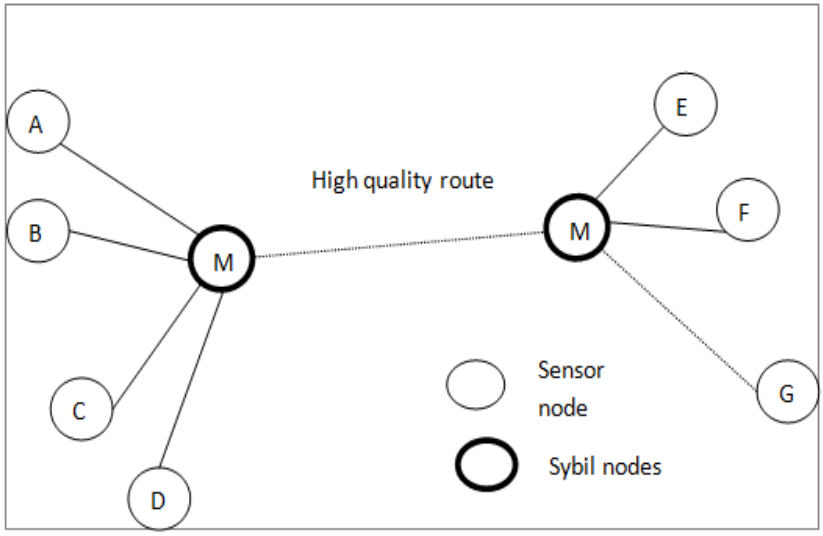

Figure 2.10 Sybil Attack

- **Wormhole attack:** The definition of wormhole attack includes that the hacker node captures the packets which may not addressed for itself and tunnels the received packets over the low latency link to remote malicious node which further may drop or replay the packets.
- **Hello Flood attack**: Protocols use hello packets for neighbor identification [11]. High resource device is used by critic node and make the nodes feel as if they are its neighbor and latter adopts that path only.
- **Acknowledgement spoofing**: Acknowledgment signals are present in protocols for reliability but malicious node can bluff the acknowledgements and may make the sender feel that dead node is alive and a weak link has much strength.

Transport Layer: The most frequent attacks are Flooding and de-synchronization at this layer.

- **Flooding attack:** When there is a need to have a connection state at any point of connection. Frequent connection requests are generated until the resources get exhausted.

- **De-synchronization**: De-synchronization is to muddle the established connection. Here, bad node depletes energy by involving end nodes to recover bugs which may not exist.

Application Layer: Destroying the application by transforming application's data is the foundation of attacks.

- **Clock sewing attack**: Incorrect timing information is scattered to the sensor nodes which requires synchronization functions.
- **Selective message forwarding attack**: Semantics of the message is studied by attacker and then message forwarding is done according to his wish or also forwards the imperfect message. Figure 2.11 sketches the bad node 'm' randomly sends the message from's' to 'BS'.

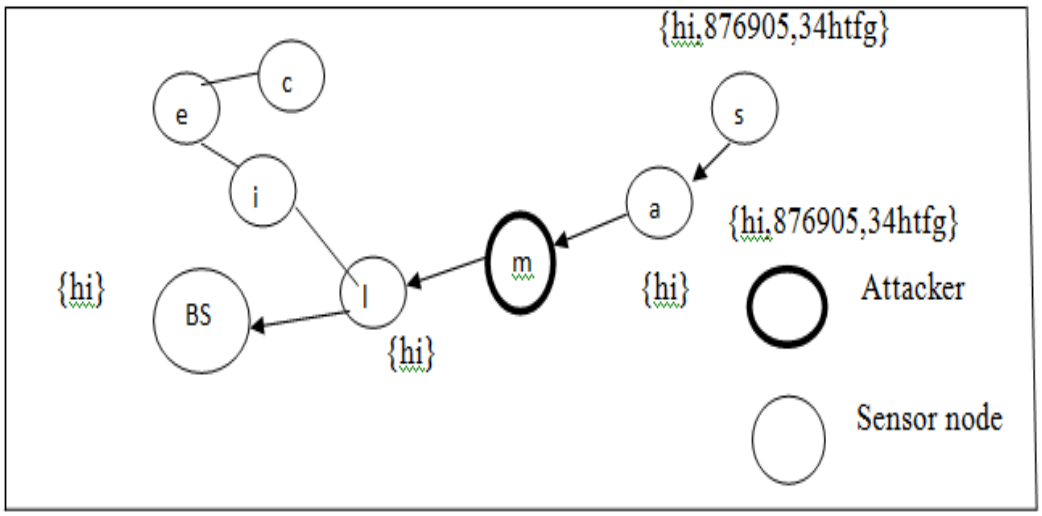

Figure 2.11 Selective Message Forwarding

2.6 Wormhole Attack

The attack includes that the bad node captures the packets which may not addressed for itself and tunnels the received packets over the low latency link to remote malicious node which further may drop or replay the packets[12,13]. Figure 2.11 sketches that h and d are the malicious nodes connected by the wormhole tunnel. In this attack the neighbors of node h assume that they are close to the node d neighbors. After the way of node h to d is established, as it will be the low latency link the traffic of network follows this route and malicious nodes may drop or replay the network traffic which will distort the network.

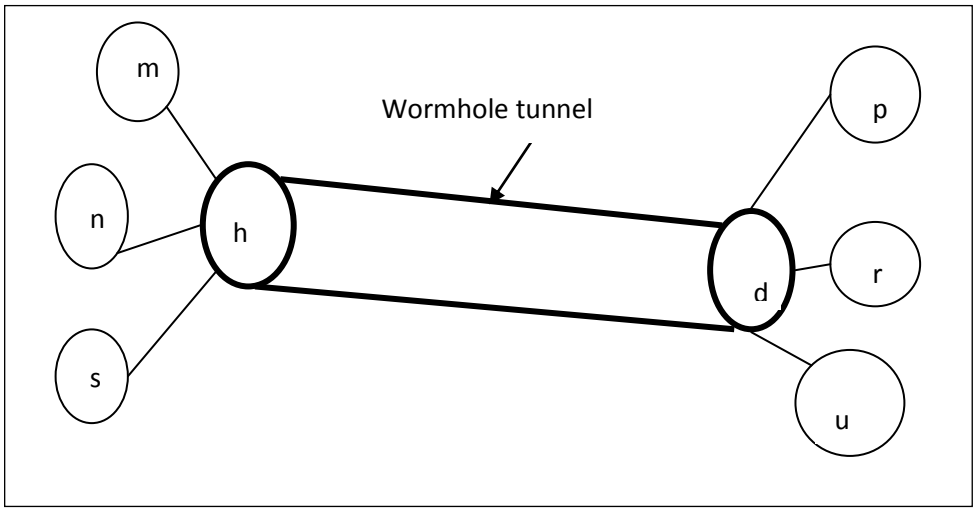

Figure 2.11 Wormhole attack

Classification of wormhole attack

Different norms for categorization of wormhole attacks [14], the technique a wormhole tunnel is created or the medium used by the wormhole nodes.

Wormhole Attacks based on implementation

There are different ways in which the attack can be implemented in the network. Different methods are described below.

- **Wormhole using packet encapsulation**: In this mode when the nodes request for the path the malicious node encapsulates the packet through the wormhole low latency link and due to encapsulation there will no increase in hop count, further the target decapsulates the clone packet. Here wormhole nodes are not connected directly but creating the virtual tunnel in the network.
- **Out of band channel Wormholes**: Here, wired link is used by critique nodes for direct connection with each other. The wireless link of long range is also helpful in wormhole. This is tough to launch as it requires some additional hardware but it is comfortable as it does not require encapsulation and decapsulation process.
- **High Power Transmission for Wormholes**: Here, the bad nodes have capability of higher power then other nodes in the network and thus increasing its chance to be the part of established route.
- **Wormhole by deviating protocol rules**: In this mode wormhole attack is launched when the malicious nodes do not comply with the rules of protocol. For

instance some of the protocols use back off time before retransmission but the malicious nodes do not use this back off time and try to be the first at destination where destination node also denies any further legitimate requests.

Wormhole attacks based upon medium used

The cataloguing can be as detailed below.

- **Wormhole In Band Attacks**: Here, wormhole nodes use the same medium for tunnel creation between them as in case of encapsulation and protocol deviation modes.
- **Wormhole Out of Band**: Here the wormhole nodes use some different communication channel between for tunnel formulation as in case of high power transmission mode.

2.7 Countermeasures against Wormhole Attacks

There are different solutions provided by the researchers to defend against wormhole attacks by putting efforts in changing the hardware design and by using various techniques of signals processing to resist the wormhole attacks but it is very difficult to defend against these severe attacks by implementing software approach only. Furthermore, the security extensions in routing protocols may not alleviate the problem of wormhole attacks completely. Therefore, many researchers have put a lot of efforts to fight against this severe attack. In this section of thesis related work to defend against these attacks is discussed.

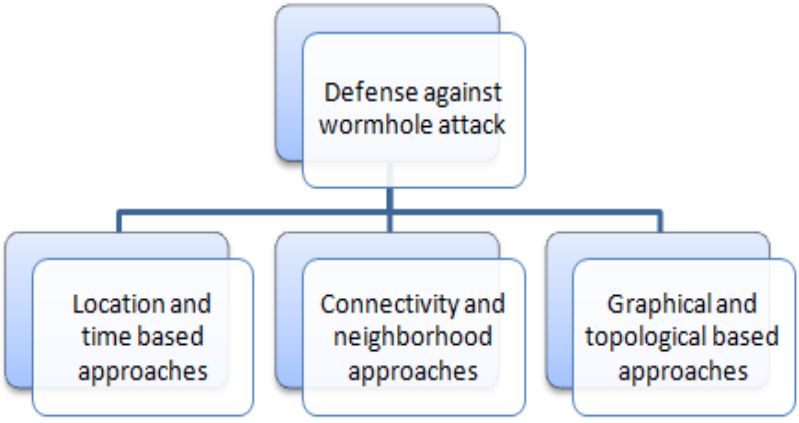

Figure 2.13 Countermeasures against wormhole attacks

2.7.1 Location and Time Based schemes

Hu et. al [15] nominated the mechanism of "packet leashes". Extra information added to message so that it can be transmitted in some allowed range only. There is temporal leash and geographical leash. Lifetime of the packet is decided by temporal leash. In this scheme also sends sending time with packet and on other hand whenever the receiver receives the packet it compares the send and received time of the packet. This scheme has a drawback i.e. synchronization of clocks is needed. Geographical leash makes certain that packet will only be sent to that recipient which is in the range of sender. In this scheme also includes the location and time information to packet. Whenever target grabs the value it compares the distance value between sender and itself to the upper bound location value. Locality and time information is used to defend against wormhole attacks. The pro of the technique includes that every node in the network posses its own position and time information. The synchronization of clocks is very resource consuming, therefore this technique is less applicable to wireless sensor networks.

Hu and Evans [16] proposed a mechanism where some special equipment called directional antennas is used. When directional antennas are used each node uses its own specific sector to communicate. Therefore, each node knows the location of the neighbor from where it received the message. The directional antennas and direction of the packet is considered and only messages from verified neighbors are accepted to defend against the attack. The disadvantage of this scheme is that the use of directional antennas is not possible in wireless networks.

Capkun et al [17] proposed a mechanism called Sector. This scheme involves sending of one bit challenge with the help of specialized hardware without any involvement of CPU and some distance-bound algorithm is used to verify radius between nodes. To defend against wormhole attacks every node propagates a bit challenge to other nodes and then they stand by for the instant response and receiving node replies. Further, the calculated distance is compared that whether it is in the maximum range of communication.

Jakob Eriksson et.al [18] proposed a mechanism named TrueLink where node verification is done by nodes themselves by first sharing the nonce and then nodes sign the messages for authenticity.

Park et al. [19] proposed a scheme LISP where key sharing takes place for immobile sensor networks. This Light Weight Security Protocol is less applicable for these networks.

Ozdemir et al. [20] proposed scheme for wireless sensor networks involve trust as well as time to locate wormholes. It requires the use of special clock therefore less applicable approach.

2.7.2 Connectivity and neighborhood based approaches

Gupta et.al [21] proposed a scheme where the nodes create a packet named hound packets which includes the message digest with private key before transmitting to destination and then the destination detects the change in hop number to locate wormholes.

Vani and Rao [22] proposed a schemed WARRDP based on the approach that wormhole nodes competitively participate in the route discovery process then hop count and neighbor list is used to detect wormholes.

Weichao et al. [23] proposed a scheme where end to end GPS location is calculated and then change in neighbors is determined.

L. Lazes et al. [24] proposed a mechanism which involves location aware Guard nodes. These guard nodes uses the range of communication constraint and detects the flow of message between nodes. This scheme considers that if there is wormhole attacker node then it will receive the same message more than once and then if the two guard nodes are able to locate this type of node then this is the wormhole node. The disadvantage of this scheme is that it is not very useful for sparse networks.

N. Song et al. [25] nominated a method depends upon on simple Statistical Assortment. This scheme detects that whether the network is under wormhole attack or not by considering the relative frequencies of the links which are there in the set of acquired routes. If the variation of the topmost highly used link and the next highest used is abruptly high then the network is under wormhole attack and the nodes attached to highest used link are the wormhole nodes.

Wang et.al [26] nominated a mechanism which is similar to packet leashes but this scheme considers the end to end position values of nodes rather than node by node. This scheme details that when the node needs to sends the packet it also adds location and time

information which is secured with message authentication code. Whenever the packet is reached to destination node it evaluates all location and time values so that these values must be in range. The disadvantage of this scheme includes that all the verification has to be done by the last node and there should be the accurate values of location and time.

2.7.3 Graphical and Topological Based Schemes

Shokri et al. [27] proposed a mechanism where position verification is done by generating local graphs and neighbors are discovered securely. The scheme is able to detect two end wormholes.

Chen et al. [28] proposed a mechanism where changes in messages are considered with resistant system of conflicting set for localization. The conflicting set is created according to the change in message which is transmitted to the neighbors for each of the locator. The scheme mainly works on idea of localization as per the range of nodes.

Alzer et al. [29] proposed a mechanism social theory of diffusion of innovations. The method is a decentralized method having different network monitoring elements which monitors the various networking parameters including transmission power, back off time etc. This method is implemented in five stages and the route is obtained by using penalties and the node which is having higher threshold value to some defined parameter is said to be the malicious node. The phases included in scheme sketched in Figure 2.14

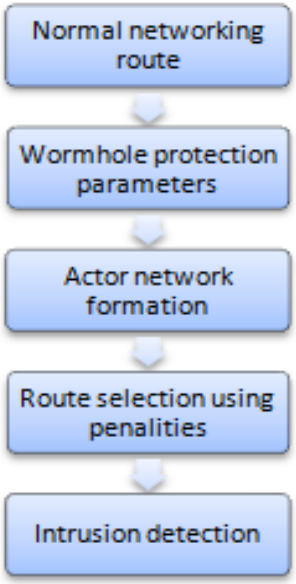

Figure 2.14 Phases of theory of innovation

Wang et al. [30] nominated scheme MDS-VOW known to be (Multi Dimensional Scaling Visualization of Wormhole). In this scheme reconstruction of network is done with the help of multidimensional scaling and any kind of anomaly is detected by measuring the distance of nodes to the central controller of the network. Initially with the use of radio signal strength each node calculates its distance to central controller and sends the same information to this controller. Further, this controller calculates the physical topology without wormholes and when the wormhole attack is there this central controller is able to watch the change effect in physical topology of the network. The major disadvantage of this scheme is that it requires central controller which is not be applicable for decentralized networks.

Merits and Demerits are associated with each of the schemes which are compared in Table 2.1

Table 2.1 Merits and Demerits of schemes against wormhole attacks

Scheme	**Approach**	**Merit**	**Demerit**
Time and Location based	Time synchronizations and location info	Less Negative false error rate	Tough synchronizations and Hardware Requirement
Connectivity Based	Neighbor link , number of hop	No Hardware requirements	More Negative false rate
Geographical and Topological based	Central nodes for monitoring	No tight synchronization No hardware need	Central nodes with more resources High resource utilization

CHAPTER 3

PROBLEM STATEMENT AND OBJECTIVE

3.1 Gaps in Study

WSN networks are prone to severe threat of wormhole attacks. These may cause the lot of destruction in networks by just tunnel formulation. The different solutions proposed by various researchers [31] are already discussed. Some of the solutions are based on radio range; some on the central controller and other are on the visualization techniques. There are various merits and demerits related to the given solutions as tight time synchronization techniques, hardware requirements and more energy and bandwidth usage. Although a lot have research has been done to defense against wormhole attacks but still there is a demand of sensor networks to have a firm and adaptive solution with more efficiency and can remove wormholes completely.

3.2 Problem Statement

Security is not in the consideration of WSN protocols which make these networks prone to numerous attacks. Most of the security schemes demand more energy consumption and one of the issues always related to WSN is energy. If security methods are incorporated with the protocols, it is possible that there is degradation in network performance. Therefore, protocols just follow the normal routing behavior and unable to locate bogus nodes.

AODV protocol is one of the extensively used protocols as it facilitates with the finding of shortest path with as low as possible energy absorption. Ad hoc networks are using more frequently this protocol but it is not less popular in WSN as power limited networks take the protocol advantage of less power need. No security is integrated with AODV protocol, thus hit by discrete malicious tasks including wormhole attacks etc. The security essentials for this protocol as discussed here:

- **Coherence of Message**: The verification of message content by the destination node should be prevalent.

- **Authenticity of Source node**: The certification of identity of source node i.e. whether it is the same node for what it is claiming for verified by the task node.
- **Authenticity of Neighbor node**: The certification of the previous node i.e. one previous node can be made by the receiver.

Wormhole attacks are one such threat causing major damage to WSN. These attacks are not easily detected as they can be in hidden mode where it is difficult to know that whether there is bad node formulating tunnel, replaying or just dropping the legitimate packets.

There is no confusion that research has been done to prevent WSN from wormholes with providing distinct solution with merits and demerits associated with them. There is a need to have the defensive mechanism with more efficient results in terms of resources and accurate at locating wormhole nodes.

3.3 Objectives and Sub Tasks

To defend WSN against wormhole attacks, the scheme with improved results is demanded. The main goal is to implement wormhole attack against AODV, proposing a defensive scheme, study the performance parameters including throughput, packet delivery ratio, and normalized routing load for the proposed scheme. The objectives of the thesis are accomplished by performing following subtasks.

- To analyze the AODV protocol.
- To implement the wormhole attack so that the message between two malicious nodes is replayed where one forwards the packet to second malicious node and latter drops the message.
- To analyze the proposed defensive scheme against wormhole attack
- To study the network parameters like throughput, packet delivery ratio and normalized routing load for different scenarios.

CHAPTER 4

INSTALLATION, IMPLEMENTATION AND DESIGN

4.1 Installation

To achieve the objectives of thesis various software packages has been installed. The description of them is discussed below.

4.1.1 Ubuntu 12.04

Ubuntu 12.04 [32] is an open source UNIX like operating system**.** This is a Debian based Linux operating system. The development of UNIX like operating system is led by UK based company called as Canonical Ltd. The Ubuntu 12.04 is the sixteenth and fourth long term support release of Ubuntu.

4.1.2 Network Simulator (NS 2)

Simulation is the act of imitating the real world events. Simulation works on some cropped model which represents behavior of physical process and the operational part with time is handled by simulation.

Overview of NS 2

NS [33] is the network simulator which is event driven, developed at UC Berkley with the support of various organizations in 1989. Nowadays, this is named as a VINT project which funded by DARPA. NS is not a complete finished simulator; it is still under research work.

NS is a simulator which can simulate different types of IP networks. This allows the users to implement networking protocols like TCP and UDP, generates traffic behavior like FTP, Telnet, VBR and CBR and also provides the mechanism for router queue management such as Dijkastra, Drop Trail etc. It also implements some MAC layer protocols.

C++ and OTcl (Object Oriented Tcl, an extension of Tcl) are the two languages which are part of NS. Users have to write a OTcl program according to their own requirements of network topologies and protocols. This script creates a event scheduler objects and the form of output is also set during writing this script according to user requirements. The

results so produced after running these scripts can be used to analyze the simulation or as a input to NAM which is a graphical software.

In order to achieve the objectives of thesis, ns-allinone-2.35 [34] package is ensconced on Ubuntu 12.04. The various files related to NS2 are installed and finally the full package of ns-2.35 is installed on Ubuntu 12.04 machine.

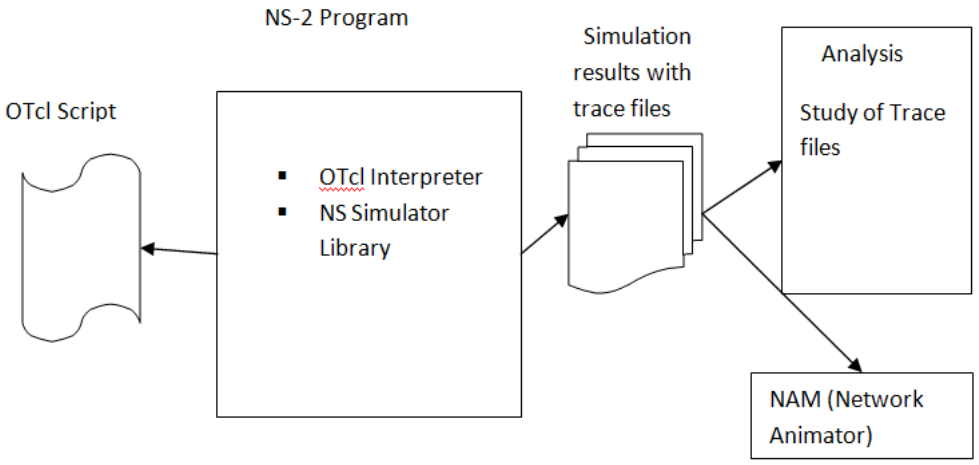

Figure 4.1 User's view of running NS2 program

TCL (Tool Command Language)

Tool Command Language is abbreviated as TCL [35]. It is the compelling, interpreted and dynamic programming language. It is highly expandable and fully compatible language with C programming. It has a wide variety of applications including web, networking, testing, etc.

NAM (Network Animator) [36]

NAM is the animation tool. It is the graphical tool used to animate the trace data of packets in the network. The output of network simulator provides with the trace data. Steven MacCanne wrote NAM but then further improved by Marylou Orayani. It was also under VINT project but now is handled by ISI.

Trace File

Trace files are the files which are in ASCII format. There are 12 different fields.

Event	Time	From node	To node	Pkt type	Pkt size	Flags	Fid	Src addrs	Dst addrs	Seq num	Pkt id

Figure 4.2 Trace File Fields

- Event: Specifies the type of event.
- Time: Time of event.
- From node: Input node of link of the event.
- To node: Output node of link of the event.
- Packet Type: Specifies the type of packet example CBR or TCP.
- Packet Size: specifies size of packet.
- Flags: Specifies flags used.
- Fid: Fid specifies stream color of NAM.
- Source Address: Address of source node.
- Destination Address: Destination node address.
- Seq No: Specifies UDP seq number.
- Packet id: Unique id of packet.

The AWK Language [37]

AWK is a scripting programming language. It is named with the initials of three authors. Its main use is elicitation of data. Text File processing is done with it. The illustration of AWK program is:

Begin

{ print

"HELLO, THAPAR!"

}

The syntax to use awk is:

awk –f "[program file]" [flags] [files]

program file : awk program file.

Files: text file from where data to be fetched.

XGRAPH [38]

It is a data plotter in x-y coordinates. It has a lot of interactive features. It is easy to plot large number of files with huge data set in single graph with XGRAPH. Any kind of graphical touch can be given to graphs.

Tracegraph

It is used for data portrayal. There are not much options so it is not user friendly. It works for both windows and linux.

4.2 Implementation

The implementation part of thesis includes the simulation of simple AODV protocol, simulation of AODV with wormhole attack and the designing of the proposed scheme.

4.2.1 Simulation of AODV protocol

AODV is simulated on NS2. The various simulation parameters taken for AODV simulation are depicted in Table 4.1

Table 4.1 Simulation parameters for AODV

Parameter	Value
Traffic Model	CBR
Simulation Time	500 sec
Grid Size	750 X 750 cm
Number of nodes	Varied(20,25,32,40,60,80,100)
Routing Protocol	AODV
Channel Type	Channel/Wireless Channel

There is interrelation of files of AODV as shown in Figure 4.3

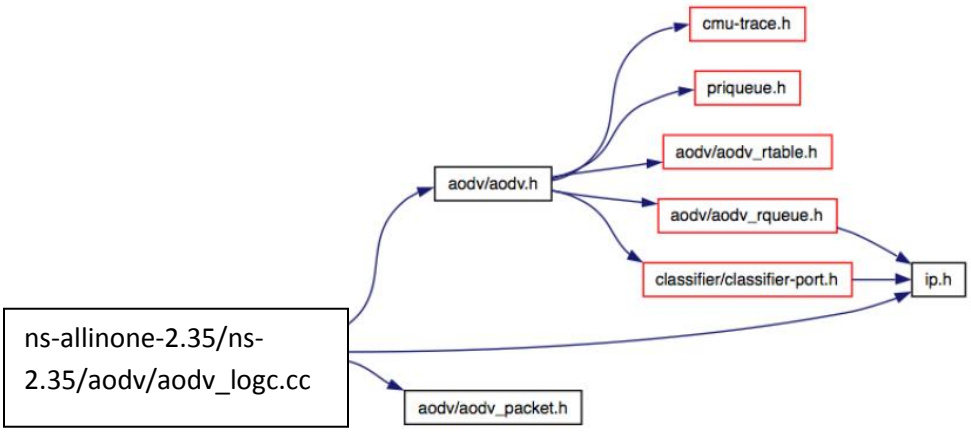

Figure 4.3 AODV File Interrelations

The Trace File after AODV simulation is depicted in Figure 4.4

```
--- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 2.255 -Id 1.255 -It AODV -Il 44 -If 0 -Ii 0 -Iv 30 -P aodv -Pt
0x4 -Ph 1 -Pd 2 -Pds 4 -Pl 10.000000 -Pc REPLY
r -t 2.561161957 -Hs 16 -Hd -2 -Ni 16 -Nx 114.33 -Ny 325.62 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw
--- -Ma 0 -Md ffffffff -Ms b -Mt 800 -Is 11.255 -Id -1.255 -It AODV -Il 48 -If 0 -Ii 0 -Iv 29 -
P aodv -Pt 0x2 -Ph 2 -Pb 1 -Pd 2 -Pds 0 -Ps 1 -Pss 4 -Pc REQUEST
```

Figure 4.4 AODV Trace File

4.2.2 Simulation of Wormhole Attack

For the implementation of wormhole attack a new protocol is added [39] so that wormhole nodes follow this newly added protocol to become the part of network. To achieve this goal alterations have been made in ns-2.34.

All the protocols reside in ns-2.34 folder, AODV protocol is duplicated with the name "wormholeaodv". All the files in wormholeaodv have the name wormholeaodv.cc, wormholeaodv.h, wormhole_rqueue.cc, wormholeaodv_rqueue.h etc by not changing the aodv_packet.h. The idea of adding the new protocol is that the wormholeaodv is able to send the same packets as of AODV. All the variables etc are changed accordingly leaving behind the structures related to packet.h file.

After these changes some of the more changes have been done in more files of ns-2.34. These changes are sketched below.

The changes in the makefile is done to create object files as depicted in Figure 4.5

```
Add wormhole.o
Add wormhole_logs.o
Add wormhole_rqueue.o
Add wormhole_rtable.o
```

Figure 4.5 changes in ns-2.35/makefile

To create the agents of wormholeaodv node the sketched changes has been done in Figure 4.6

```
Create ragent wormhole;
At time ragent "start";
Node ragent_node;
return node;
```

Figure 4.6 changes in ns-2.35/tcl/lib/ns-lib.tcl

To insert new packet type the sketched changes in Figure 4.7 have been done.

```
PacketType_name = “wormhole”;
PacketType_constant=”last id”;
If ( Packet_type ==wormhole)
{
 return Routing;
}
```

Figure 4.7 changes in ns-2.35/common/packet.h

The two variables are defined as bool wormhole1and bool wormhole2 in aodv.h file of wormholeaodv which are depicted in Figure 4.8 [40].

```
Add variable Boolean womrhole1;
Add Variable Boolean wormhole 2;
```

Figure 4.8 changes in wormholeaodv.h file

The variables are first initialized to false in wormholeaodv.cc file of aodv as sketched in Figure 4.9

```
Initialize variable wormhole1 =false;
Initialize variable wormhole2=false;
```

Figure 4.9 Initialization of variables in wormholeaodv.cc

Wormhole node definition in wormholeaodv.cc file as depicted in Figure 4.10

```
If (hacker1)
{
 set variable wormhole1 =true;
return tcl;
}
If (hacker2)
{
set variable wormhole2=true;
Return tcl;
}
```

Figure 4.10 Wormhole node definition in wormholeaodv.cc

The action performed by one of the wormhole node is to forward the packet to another wormhole node as sketched in Figure 4.11

```
If ( wormhole1 ==true)
{
forward packet to wormhole2;
}
```

Figure 4.11 Wormhole Node Behaviour

The action performed by another wormhole node of the network is to drop the packets as sketched in Figure 4.12

```
If (wormhole2==true)
{
Drop the packets;
}
```

Figure 4.12 Wormhole Node drops the packets

For the tunnel between wormhole nodes the encapsulation and decapsulation is done. To attain this IP header is extended. The extension posses encapsulated values. When the packet reaches to other end of tunnel decapsulation removes all new values. This is achieved as depicted in Figure 4.13

```
If (packettype_wormhole and wormhole1 ==true)
{
encapsulate packet_wormhole;
return;
}
If (packettype_wormhole and wormhole2==true)
{
decapsulate packet_wormhole;
return;
}
```

Figure 4.13 Encapsulation and Descapsulation

The simulation parameters for wormhole attack are in Table 4.2

Table 4.2 Simulation parameters for wormhole

Parameter	Value
Traffic Model	CBR
Simulation Time	500 sec
Grid Size	750 X 750 cm
Number of nodes	Varied(20,25,32,40,60,80,100)
Routing Protocol	AODV
Number of wormholes	2
Channel Type	Wireless Channel

4.3 Proposed Wormhole Attack Detection Scheme

Here, a novel method against wormhole attack in AODV protocol is discussed in detail. AODV protocol is selected for validating the proposed work because it is one of the protocols based on route establishment phase and wormhole attack greatly affects these type protocols.

Short outline of the scheme

The proposed scheme considers the network to be homogeneous. The variable round trip time between nodes is taken and then the average limit of neighbors is calculated to detect the wormhole link. The proposed method uses no appliances and synchronization of time. While designing the mechanism main focus is to have low energy and bandwidth utilization. The buffer time is also taken into consideration while designing the algorithm. The whole scheme is divided into different stages which are discussed as below in detail.

Stage I: Formulation of neighbor list

1. Every sensor node in the network keeps the information regarding its neighbors (the nodes with which it can communicate directly) with the help of local "HELLO" message. Every sensor node keeps this track by listening to this "HELLO" message at regular intervals of time.

Stage II: Route Establishment and Wormhole Node Suspicion

1. Whenever source node needs to send the message to other node and node is not in neighbor list of source node, latter broadcast a packet which is Route Request

(RREQ) as depicted in Figure 4.14 and also save the current time of its request message TRREQ.

Type	J	R	G	D	U	Reserved	Hop Count
RREQID							
Destination IP Address							
Originator IP Address							
Originator Sequence Number							

Figure 4.14 RREQ message format

2. The sensor node when receive the RREQ message and if it is not that node which is target or it do not posses routing entry to final node, it will rebroadcast this message until the destination is not found and also correspondingly save the current time of their RREQ message.
3. When the node having path to destination or destination node itself granted with Route Request Message (RREQ) , that responds with message called Route Reply (RREP). RREP by copying its sequence number field also save its Round Trip Time (RTT) in RREP message (modified) as shown in Figure 4.15. This whole information is then sent to source node.

Type	R	A	Reserved	Prefix Size	Hop Count
Destination IP Address					
Destination Seq. Number					
Originator IP Address					
Lifetime					
Type	Length	Round Trip time (RTT)			

Figure 4.15 Modified RREP message format

The Round Trip Time (RTT) for each node (N_i) is calculated as:

$RTT\ (N_i) = (T_{RREQ} - T_{RREP}) + PT\ (N_i) + PD$

Where PT = Processing Time

PD = Propagation delay due to buffering time

4. Now the source node calculates the RTT between all the nodes which are intermediate to the established path. If the RTT is almost same for each of the link of the established path then there is no wormhole present otherwise there may be wormhole present.

If the RTT between (N_i) and (N_j) (any two nodes) < Average $_{all}$ then no wormhole present

Else

Wormhole may be present

5. Now when the routing table entry is created, the path which is used for highest number of times may indicate about the wormhole link. Although, it is possible the same path is used many a times but presence of similar nodes have less probability in routing table entry of many other nodes.

   Therefore, by modifying routing table and by adding one more entry of full path for each node can be helpful to be more accurate to find the wormhole link between N_i and N_j.

   Go to Wormhole Detection Stage.

Stage III: Wormhole Detection

This Stage has the foundation which is dependent upon the consideration that the malicious wormhole node increments the amount of neighbors in its radius.

Now, if the RTT between N_i and N_j is greater than the average value then there is a requirement of verification.

1. If Number of Neighbors (N_i) and Number of Neighbors (N_j) > Average Neighbor_limit, then the wormhole is located between N_i and N_j, where Average Neighbor_limit is calculated as:

   Average Neighbor_limit = $(N -1)\pi r^2$ / A [41] ; A = Region Area, N = Node Number, r = radius of transmission.

2. Go to Removal of Wormhole node Stage.

Stage 4: Removal of Wormhole node

1. Send the error message called Wormhole_propound to every sensor nodes which are part of network as depicted in Figure 4.16.

Type	N	Reserved	Destination count
Unreachable Destination IP Address			
Unreachable Destination Sequence Number			
Additional Unreachable Destination IP Address			
Additional Unreachable Destination Sequence Number			
Type	Length	Worm_propound	

Figure 4.16 Modified RERR message format

2. Whenever this message is received by any node it will remove corresponding id of wormhole node from routing table and the source node restart the process of route discovery with no wormhole node. Flowchart of whole scheme is depicted in Figure 4.17.

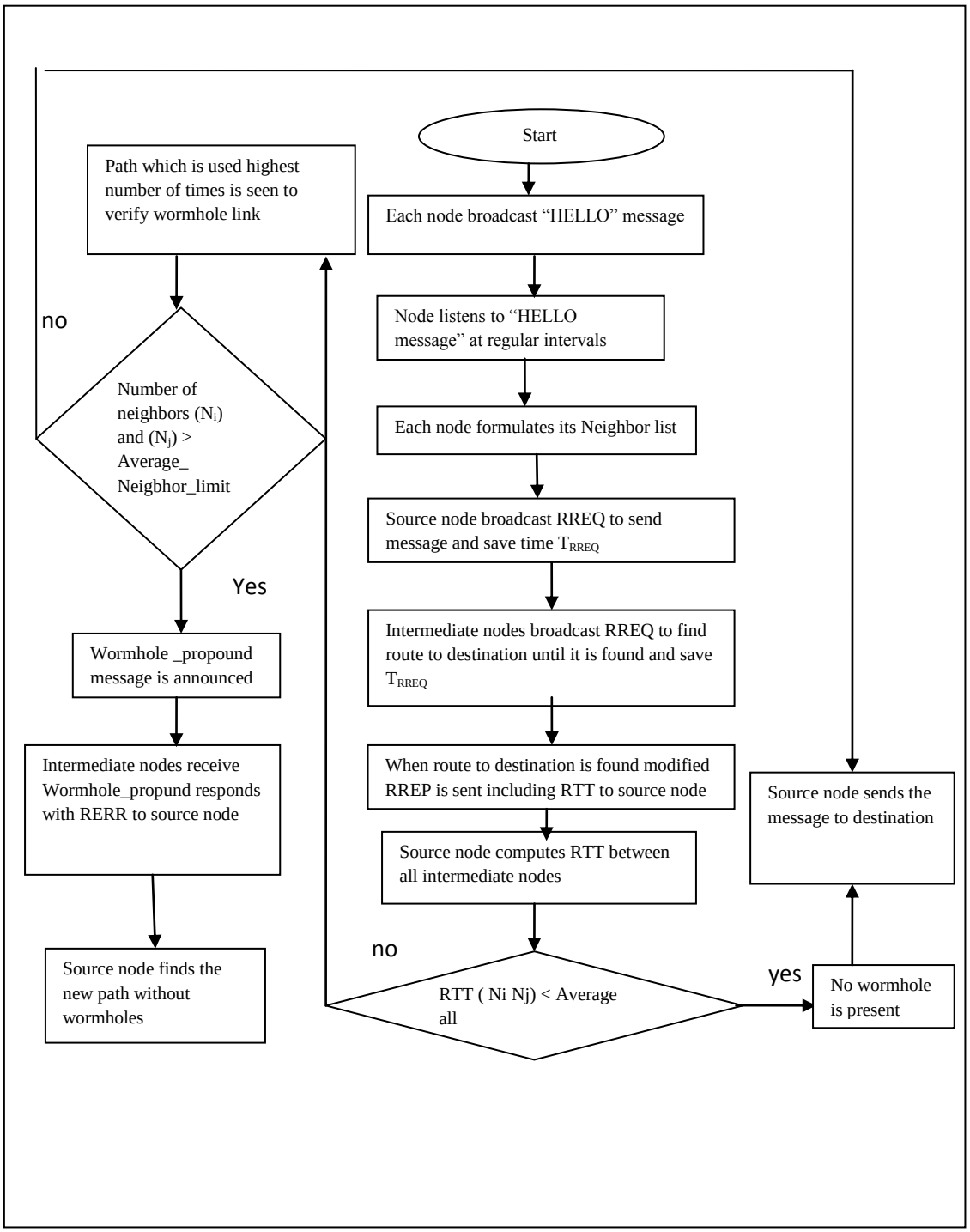

Figure 4.17 Flow Chart of nominated scheme

CHAPTER 5

RESULTS AND PERFORMANCE ANALYSIS

Simulation results are discussed in this part. The performance analysis [42] is made through the results of .nam and .tr file in Network Animator and by plotting 2D XGRAPHS. AWK programming is also used to obtain the results. To review the performance of the protocol also AWK is used. The results are attained by division of simulation in parts as shown below:

- Simulation of AODV protocol with different number of nodes.
- Simulation of AODV with two wormhole nodes and varying other nodes.
- Simulation of nominated defensive scheme.

The parameters studied during experimentation are:

Throughput: It is the frequency of useful message delivery i.e. $packets\ moved/\ time$.

Packet Delivery Ratio (PDR): It is calculated as the number of packets reach to the destination to the total number of packets sent i.e. $packets\ receive/packets\ sent$.

Normalized Routing Load: It is calculated as the number of routing packets per data packet i.e. $routing\ packets/data\ packets$

5.1 AODV Simulation

The AODV simulation is carried by varying the number of nodes. The random traffic is generated with the inbuilt cbrgen.tcl file. The visualization of simulation is done with NAM invoked from tcl file. The simulation is done by changing the number of nodes. AODV with 20 nodes is depicted in Figure 5.1

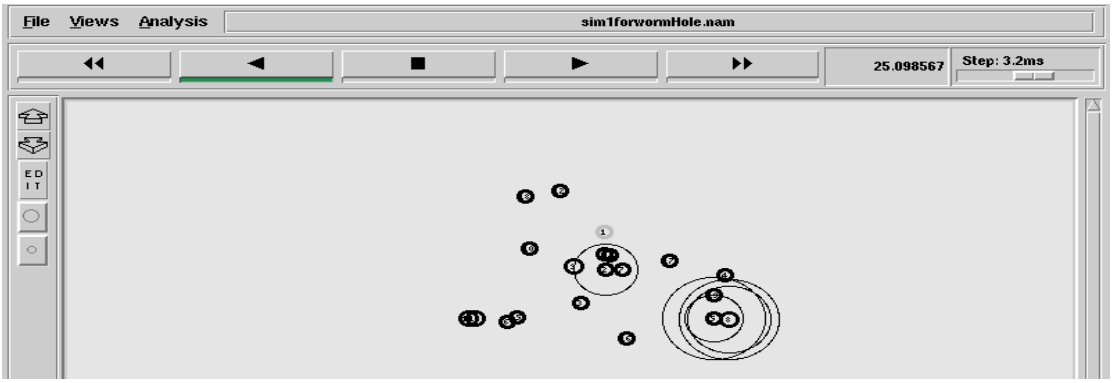

Figure 5.1 AODV with 20 nodes

5.2 Wormhole Attack Simulation

The wormhole attack with two nodes and different normal nodes is simulated. The random traffic is generated by inbuilt cbrgen.tcl. NAM is visualizing the scenario. The wormhole attack with 18 normal nodes and 2 wormholes is depicted in Figure 5.2.

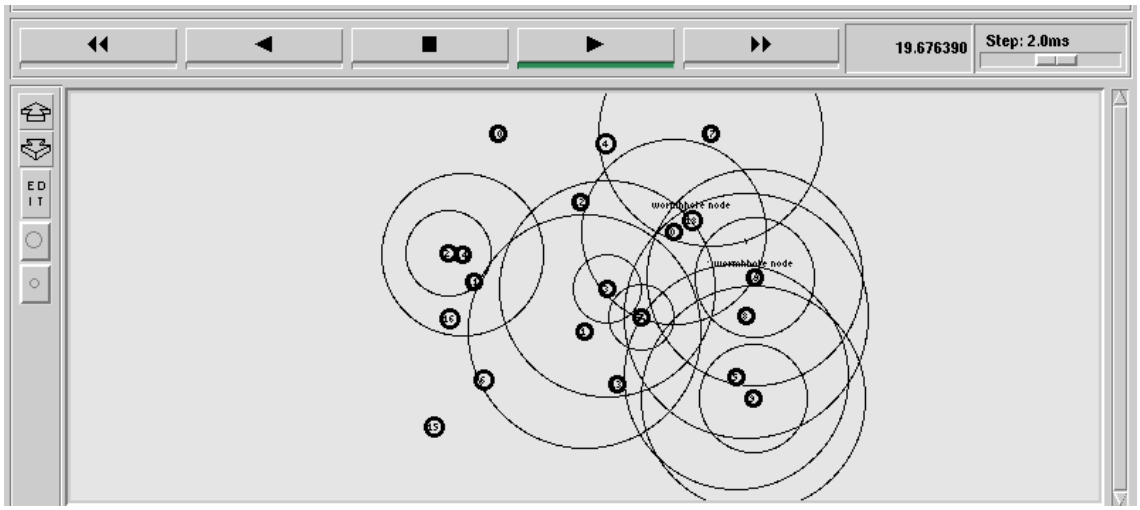

Figure 5.2 Wormhole attack (18 normal and 2 wormholes)

5.3 Proposed Scheme Simulation

The nominated scheme is tested against wormhole attack. The nominated scheme is also experimented by varying number of nodes. The NAM is used to visualize the simulation as in Figure 5.3

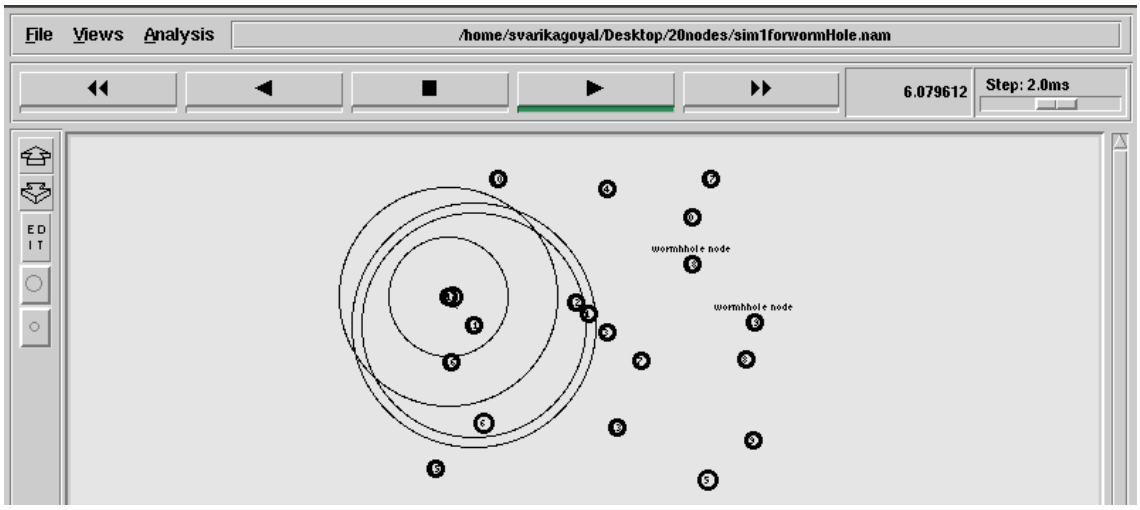

Figure 5.3 Proposed Defensive scheme

5.4 Results

The simulation results are obtained for different scenarios; these include AODV simulated, wormhole attack and the nominated scheme. The metrics throughput, packet delivery ratio and normalized routing load are studied after the results obtained.

5.4.1 Results for AODV

Throughput results are gathered by having different network size. AWK programming is used to take the values from trace files. For illustration throughput for 20 nodes is depicted in Figure 5.4

```
svarikagoyal@ubuntu:~$ cd Desktop
svarikagoyal@ubuntu:~/Desktop$ cd 20nodes
svarikagoyal@ubuntu:~/Desktop/20nodes$ ns aodv20.tcl
num_nodes is set 20
Creating nodes...
INITIALIZE THE LIST xListHead
Loading random connection pattern...
Starting Simulation...
SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
svarikagoyal@ubuntu:~/Desktop/20nodes$ awk -f Throughput.awk sim1forwormHole.tr
Average Throughput[kbps] = 502.35                StartTime=2.56 StopTime=499.98
Average Throughput[kbps] = 502.35                StartTime=2.56 StopTime=499.98
```

Figure 5.4 Throughput of AODV (20 nodes)

Packet delivery ratio (PDR) is also analyzed by varying network size. For illustration PDR for 20 nodes is sketched in Figure 5.5

```
svarikagoyal@ubuntu:~$ cd Desktop
svarikagoyal@ubuntu:~/Desktop$ cd 20nodes
svarikagoyal@ubuntu:~/Desktop/20nodes$ ns aodv20.tcl
num_nodes is set 20
Creating nodes...
INITIALIZE THE LIST xListHead
Loading random connection pattern...
Starting Simulation...
SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
svarikagoyal@ubuntu:~/Desktop/20nodes$ awk -f Throughput.awk sim1forwormHole.tr
Average Throughput[kbps] = 502.35                StartTime=2.56 StopTime=499.98
Average Throughput[kbps] = 502.35                StartTime=2.56 StopTime=499.98
svarikagoyal@ubuntu:~/Desktop/20nodes$
```

Figure 5.5 PDR of AODV (20 nodes)

NRL is studied by taking the values of trace file. For illustration NRL calculated for 20 nodes is in Figure 5.6

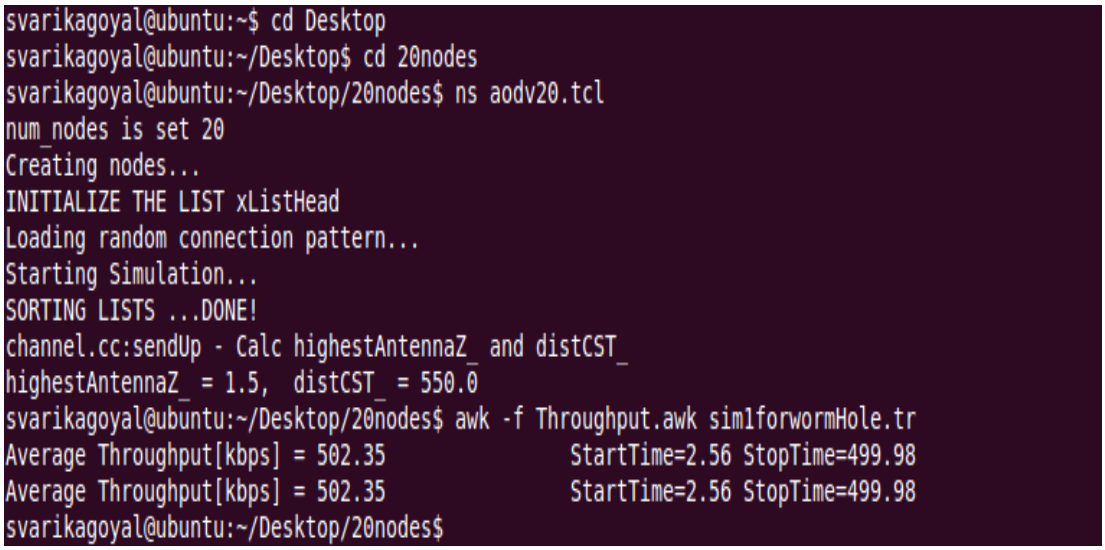

Figure 5.6 NRL for AODV (20 nodes)

Here are the values obtained for the discussed parameters for different amount of nodes. The table 5.1 details the values of parameters.

Table 5.1 Performance result values for AODV

Number of nodes	**NRL**	**PDR**	**Throughput(kbps)**
20	0.284	0.9738	502.35
25	1.086	0.8869	476.99
32	2.397	0.7706	415.45
40	0.702	0.9862	530.72
60	0.882	0.9987	532.93
80	1.482	0.9854	531.78
100	1.374	0.9872	531.58

5.4.2 Results for wormhole attack

Wormhole Attack is implemented against AODV for different network size. The results are then analyzed**.**

It is observed that throughput is highly lowered by wormhole attack**.** The different values are taken by having different number of nodes.

For illustration throughput of 20 nodes is sketched in Figure 5.7.

```
svarikagoyal@ubuntu:~/Desktop/20nodes$ ns wormhole.tcl
num_nodes is set 20
Creating nodes...
INITIALIZE THE LIST xListHead
Loading random connection pattern...
Starting Simulation...
SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
svarikagoyal@ubuntu:~/Desktop/20nodes$ awk -f Throughput.awk sim1forwormHole.tr
Average Throughput[kbps] = 87.15                StartTime=2.56 StopTime=499.93
Average Throughput[kbps] = 87.15                StartTime=2.56 StopTime=499.93
```

Figure 5.7 Throughput of wormhole attack (20 nodes)

PDR is also get lowered by wormhole attack. For illustration PDR of 20 nodes is sketched in Figure 5.8.

```
svarikagoyal@ubuntu:~$ cd Desktop/
svarikagoyal@ubuntu:~/Desktop$ cd 20nodes/
svarikagoyal@ubuntu:~/Desktop/20nodes$ ns wormhole.tcl
num_nodes is set 20
Creating nodes...
INITIALIZE THE LIST xListHead
Loading random connection pattern...
Starting Simulation...
SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
svarikagoyal@ubuntu:~/Desktop/20nodes$ awk -f pdr.awk sim1forwormHole.tr
cbr s:31335 r:5291, r/s Ratio:0.1689, f:16485
svarikagoyal@ubuntu:~/Desktop/20nodes$
```

Figure 5.8 PDR of wormhole attack (20 nodes)

There is rise in NRL value as more of routing information has to be sending again and again during the attack. For illustration NRL of 20 nodes is sketched in Figure 5.9.

```
svarikagoyal@ubuntu:~$ cd Desktop/
svarikagoyal@ubuntu:~/Desktop$ cd 20nodes/
svarikagoyal@ubuntu:~/Desktop/20nodes$ ns wormhole.tcl
num_nodes is set 20
Creating nodes...
INITIALIZE THE LIST xListHead
Loading random connection pattern...
Starting Simulation...
SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
svarikagoyal@ubuntu:~/Desktop/20nodes$ awk -f nrl_nt.awk sim1forwormHole.tr
##############################################################################
##

                      Normalized Routing Load = 2.372

##############################################################################
##
```

Figure 5.9 NRL of wormhole attack (20 nodes)

The different values obtained after implementing wormhole attack for different metrics with change in number of nodes is detailed. Table 5.2 shows the obtained values.

Table 5.2 Performance result values for wormhole attack

Number of nodes	NRL	PDR	Throughput(kbps)
20	2.372	0.1689	87.15
25	6.145	0.0966	52.0
32	8.788	0.0973	56.36
40	9.883	0.1023	55.40
60	15.019	0.0613	36.55
80	25.202	0.0916	51.45
100	14.744	0.1701	91.58

5.4.3 Results of proposed Detection Scheme

The nominated scheme is tested against wormhole attack. It is verified that detection scheme is able to improve the overall performance metrics.

It is evaluated that the detection scheme is able to improve the throughput. For illustration throughput for 20 nodes is sketched in Figure 5.10

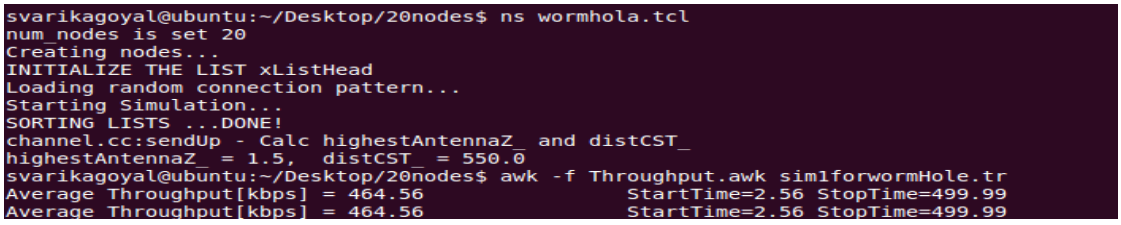

Figure 5.10 Throughput by nominated scheme (20 nodes)

It is verified that the proposed scheme works well and results with better PDR results. For illustration PDR for 20 nodes is sketched in Figure 5.11

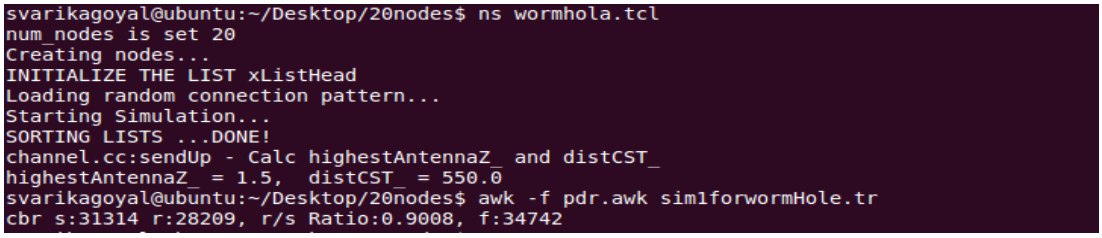

Figure 5.11 PDR for nominated scheme (20 nodes)

It is evaluated that the NRL produced by nominated scheme is less. For illustration NRL of 20 nodes is sketched in Figure 5.12.

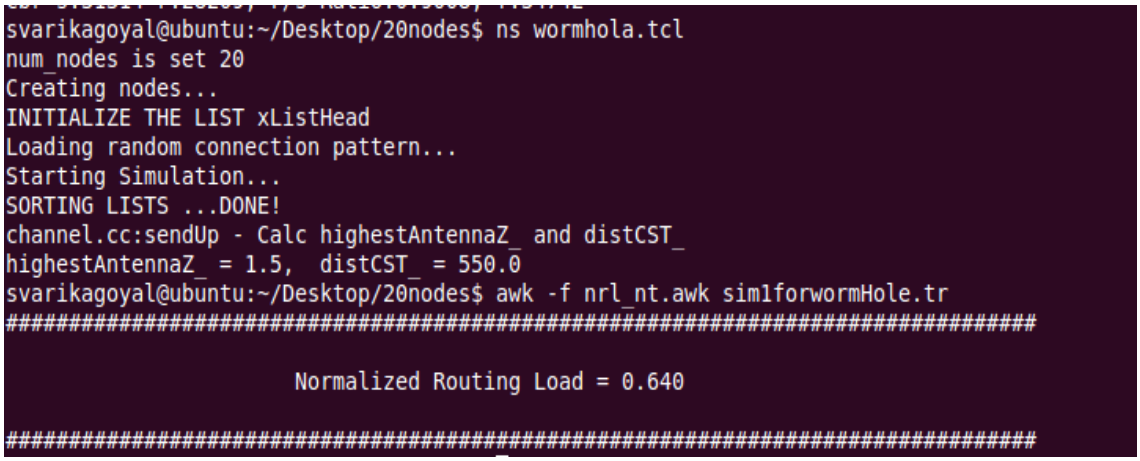

Figure 5.12 NRL for nominated scheme (20 nodes)

The different values obtained for nominated scheme is detailed. Table 5.3 shows all the result values.

Table 5.3 Performance result values for nominated scheme

Number of nodes	**NRL**	**PDR**	**Throughput(kbps)**
20	.640	0.9008	464.56
25	1.145	0.8660	466.68
32	2.4	0.7541	406.10
40	2.611	0.7522	406.02
60	2.094	0.8052	433.12
80	5.939	0.6830	368.55
100	3.204	0.8030	431.90

5.5 Analysis

It is analyzed that how the network parameters got affected by severe threat [43]. It is also verified that proposed scheme works well against wormhole attack**.** The comparison is done for three different scenarios i.e. AODV protocol, for wormhole attack, for nominated detective scheme. The comparison made by plotting 2D XGRAPHS [44] for all the three scenarios.

5.5.1 Throughput Analysis

It is analyzed that Throughput for the wormhole affected network is reduced to nearly 17% i.e. 502(kbps) to 87.15 (kbps) values which depicts that how these wormhole nodes degrades the network performance. The proposed scheme improves the throughput value to 75% after detection of wormhole nodes i.e. from 87.15(kbps) to 464.54(kbps).It is depicted from the results that wormhole attack greatly drops the value of normal AODV protocol which is then improved by proposed detection scheme. Figure 5.13 sketches the comparison for three scenarios.

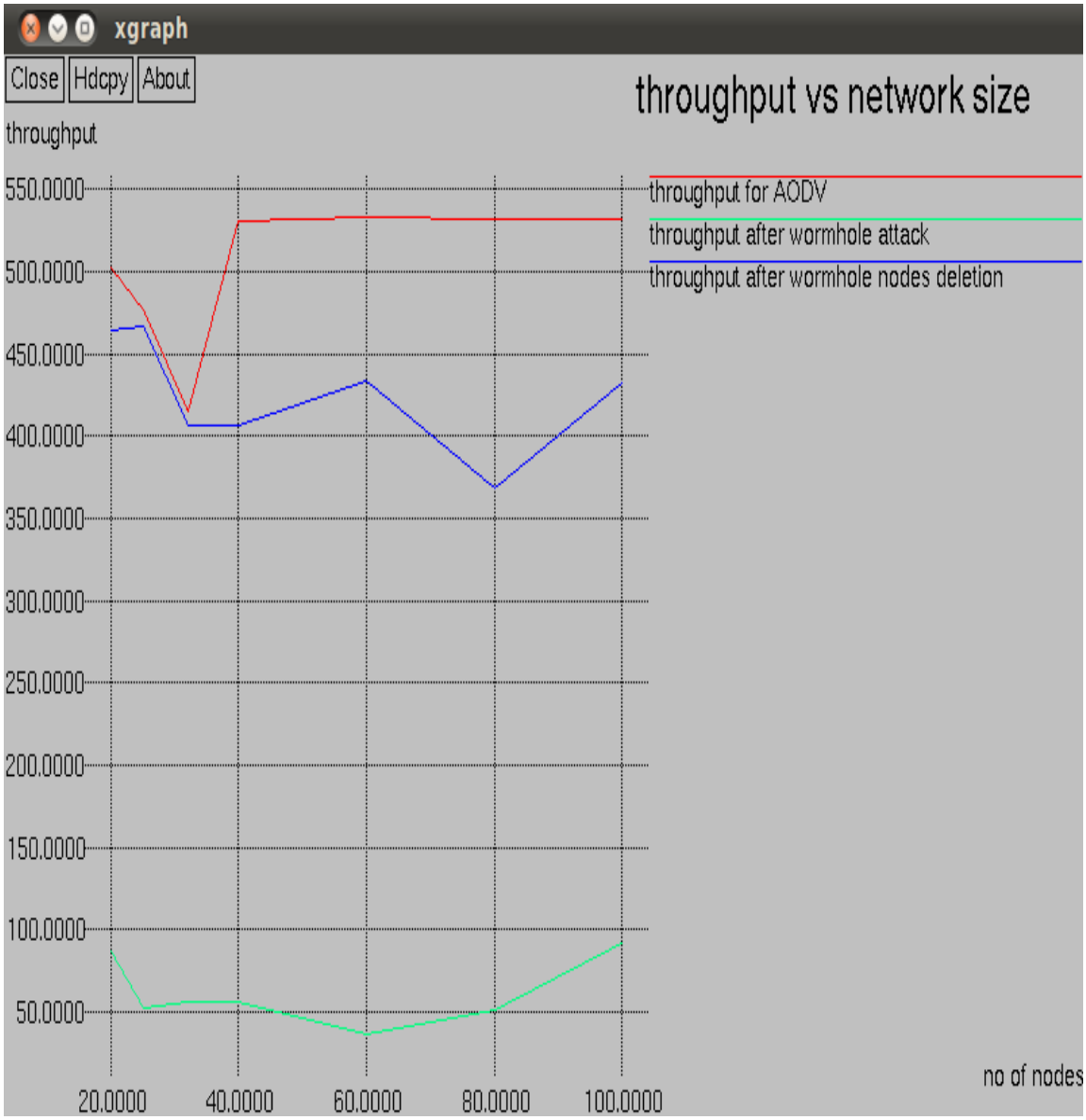

Figure 5.13 XGRAPH for comparison of throughput for AODV, Wormhole Attack and nominated detection scheme.

5.5.2 PDR (Packet Delivery Ratio) Analysis

It is analyzed that the normally the packet loss is nearly 3.62% (0.9738 ratio of packets sent to packets received) which is highly increased by wormhole nodes to nearly 85% (0.1689 ratio of packets sent to packets received) by dropping the packets. The proposed scheme reduces this packet loss to nearly 10 % (0.9008). Results depict that PDR is highly dropped by wormhole attack of AODV which is then improved by proposed detection scheme. Figure 5.14 sketches the comparison for three scenarios.

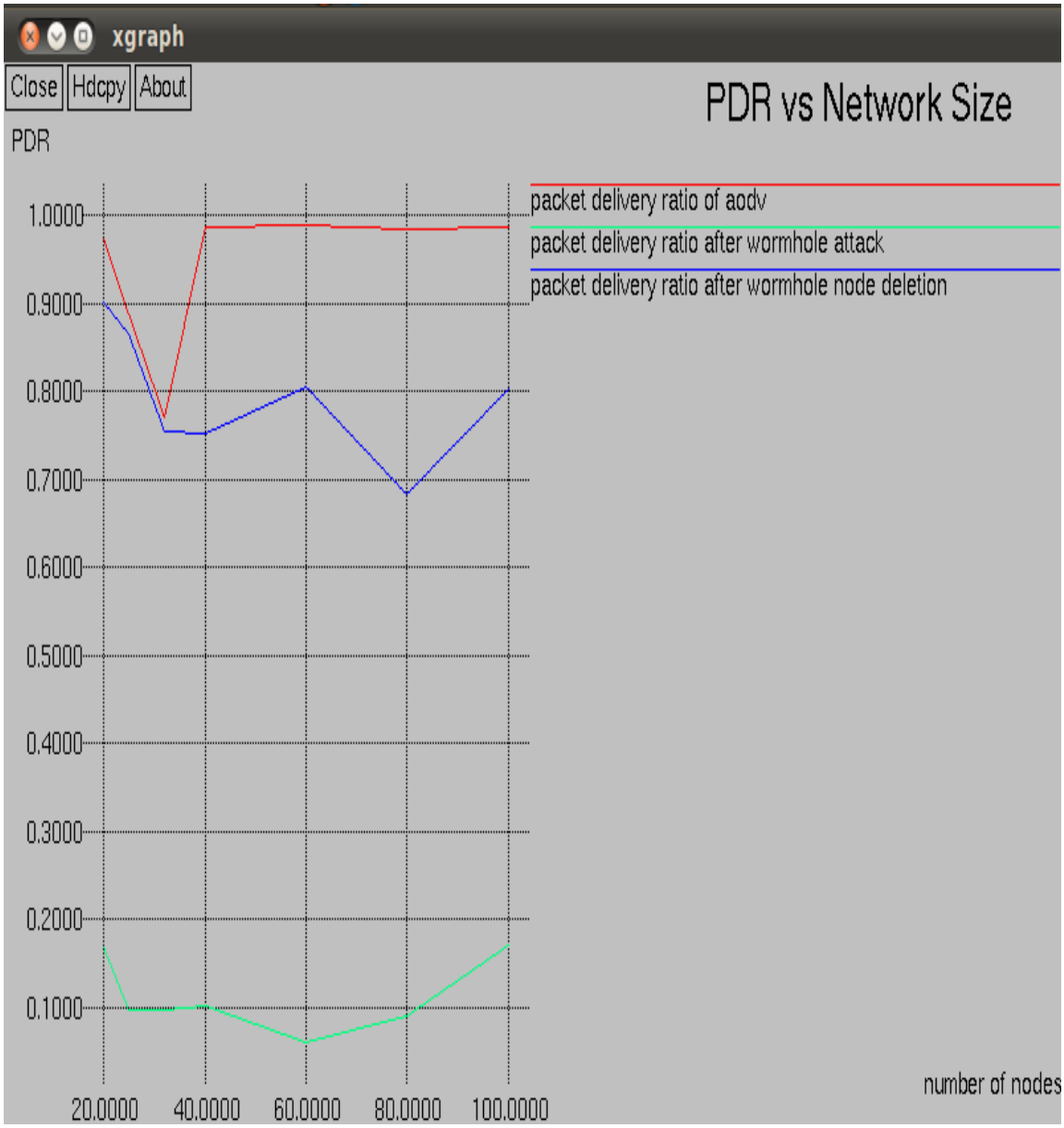

Figure 5.14 XGRAPH for comparison of PDR for AODV, Wormhole Attack and nominated detection scheme

5.5.3 NRL (Normalized Routing Load) Analysis

It is analyzed that in normal networking conditions the routing load on the network is nearly 28 % which is increased by wormhole nodes to 77% because one of the node drops the packets and then more routing information is routed in the network. This increased routing load is reduced by proposed scheme from 77% to 34 %. Results depict that NRL is highly raised by wormhole attack of AODV which is then improved by proposed detection scheme. Figure 5.15 sketches the comparison for three scenarios.

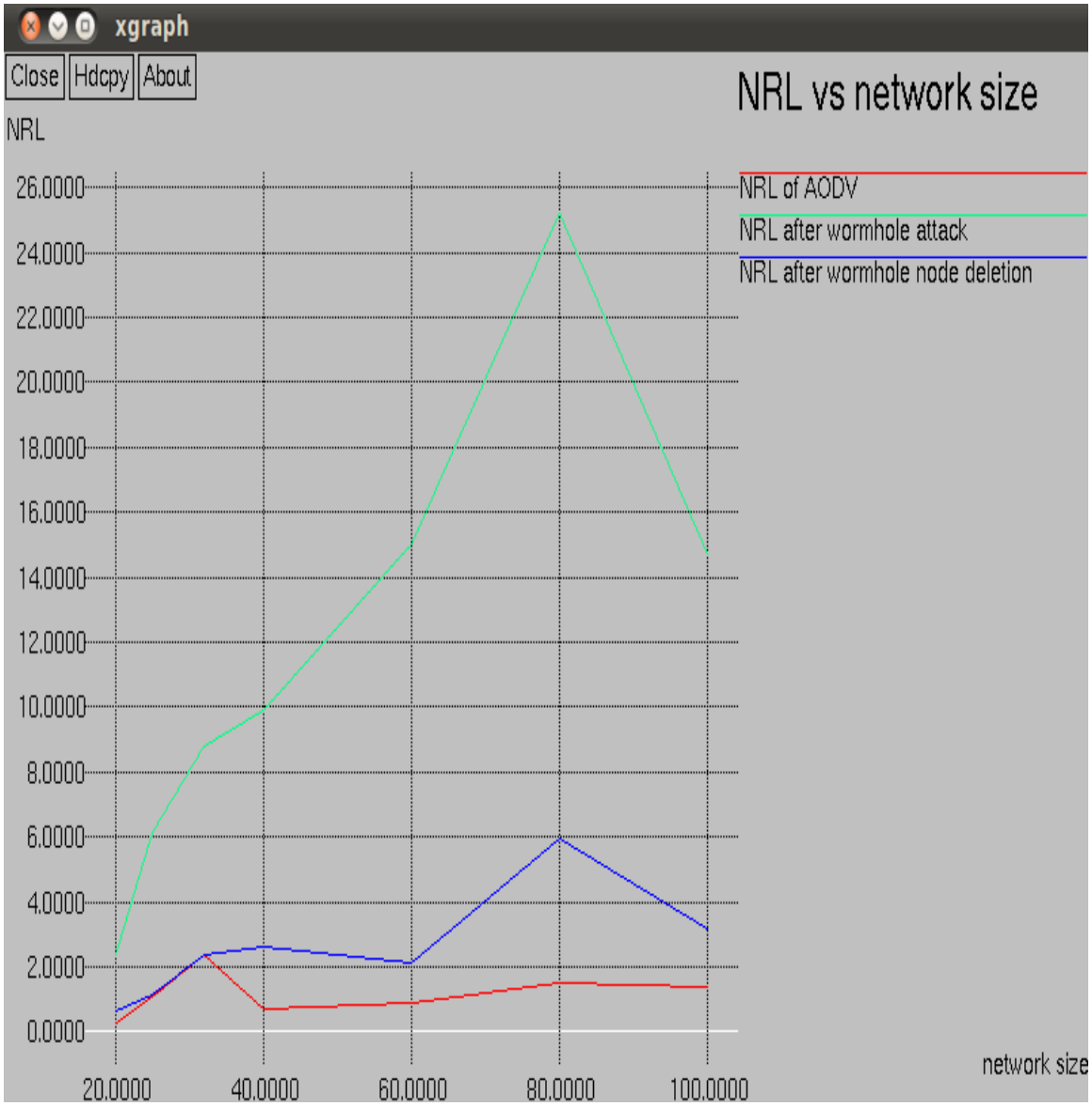

Figure 5.15 XGRAPH for comparison of NRL for AODV, Wormhole Attack and nominated detection scheme.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

As security is also one of the important issues in Wireless Sensor Networks, it is required to deal with the threats related to them and one such severe threat is the wormhole attack in which the hacker node grabs the network traffic from one point and directs to another location that may drop the packets. In this thesis the scheme is developed which includes the RTT, usage level of links and count of neighbors to detect the wormhole nodes in WSN. The proposed scheme is assessed and simulated against AODV protocol on NS-2 simulator. The efficiency of the proposed scheme is validated through results as the degraded throughput from 17% is raised by proposed scheme to 75%, packet loss rate is reduced to 10 % from 85% after the removal of wormhole nodes. It is evaluated that the normalized routing load is significantly reduced by proposed scheme from 77% to 34%. The merits of the proposed scheme also includes that it does not require any kind of synchronizations and any hardware and is efficient at calculation and bandwidth overhead.

6.2 Future Scope

It is required that WSN are to be certain in terms of security to raise their performance, accuracy and reliability. The future scope involves the extension of nominated scheme for other protocols than the current AODV protocol to enhance the secure routing in these networks with better results in terms of energy, bandwidth and computation overhead. The future scope also involves enhancing the security framework of WSN by storing the network data at cloud.

ANNEXURE I

REFERENCES

[1] K. Jones, A.Waada, S. Olaniu, et. al, “Towards a new paradigm for Securing Wireless Sensor Networks”, *New Security Paradigms workshop*, Switzerland, 2003.

[2] S.Olariu and Q.Xu, "Information assurance in wireless sensor networks", *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium*, pp.5-10, 2005.

[3] C. Chong and S. P. Kumar, “Sensor Networks: Evolution, Opportunities, and Challenges”, *in Proceedings of the IEEE*, vol. 91, no. 8, 2003.

[4] B. Karp and H.T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", *Proceedings of the 6th annual International Conference on Mobile computing and networking* ACM pp. 243-254, 2000.

[5] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “*A survey on sensor networks*”, IEEE Communication Magazine, vol.40, no. 8 pp.102-114, 2002.

[6] T. Melodia, D. Tommaso, et al, "Communication and coordination in wireless sensor and actor networks", *Mobile Computing, IEEE Transactions,* vol. 6, no.10, pp.1116-1129, 2004.

[7] R. Govindan, D. Estrin et.al, “Directed diffusion: A scalable and robust communication paradigm for sensor networks”, *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks*, 2000.

[8] C. Ian, E.M. Belding-Royer. "AODV routing protocol implementation design", *Distributed Computing Systems Workshops, Proceedings 24th International Conference on*. IEEE ,2004.

[9] M.Castro and B.Liskov, “Practical byzantine fault tolerance”, in *OSDI: Symposium on Operating Systems Design and Implementation*, USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS, vol. 80, pp.173-186, 1999.

[10] C.Benjie, K.amieson, H.Balakrishnan, and R.Morris, “Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks”, *ACM Wireless Networks Journal*, vol. 8, no. 5, 2002.

[11] C.Karlof and D.Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures” *Ad Hoc Networks Journal*, vol. 1, no. 2, pp. 293-3, 2003.

[12] A. Mpitziopoulos, C. Aristides, et al. "A survey on jamming attacks and countermeasures in WSNs", *Communications Surveys & Tutorials, IEEE*, vol.11, no.4, pp.42-56, 2009.

[13] Y.C. Hu, A. Perrig, and D. B. Johnson. "Wormhole attacks in wireless networks", *Selected Areas in Communications, IEEE Journal*, vol. 24, no.2, pp.370-380, 2006.

[14] A. Pirzada, and C. McDonald, “Circumventing Sinkholes and Wormholes in Wireless Sensor Networks., *International Work-shop on Wireless Ad Hoc networks* ,pp. 132-150, 2005.

[15]Y. Hu, A. Perring, and D.B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”, *Proceedings of 22nd Annual Conference of the IEEE Computer and Commu-nication Societies*, vol.3, pp.1976-198, 2003.

[16] L. Hu and D. Evans, “Using Directional Antennas to Prevent Wormhole Attacks”, *Proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS)*, 2004.

[17] S. Capkun, L. Buttyan, and J. Hubaux, “SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks”, *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.*

[18] J.Eriksson, S.V.Krishnamurthy and M.Faloutsos,“ TrueLink: A Practical Counter measure to the Wormhole Attack in Wireless Networks”, *14th IEEE International Conference on Network Protocols*, pp.75-84, 2006.

[19] T. Park and K. Shin. "LISP: A lightweight security protocol for wireless sensor networks," *Proceedings of ACM transaction on Embedded Computing systems*, vol. 3, no. 3, pp. 634-640, 2004.

[20] S. Özdemir, M. Meghdadi, and Ý. Güler. "A time and trust based wormhole detection algorithm for wireless sensor networks," *3rd Information Security and Cryptology Conference*, pp. 139-145, 2008.

[21] S.Gupta, S.Kar and S.Dharmaraja, “WHOP: Wormhole Attack Detection Protocol using Hound Packet”, *IEEE International Conference of Innovations in Information Technology*, pp.226-231, 2011.

[22] A.Vani and D.Sreenivasa Rao, “WARDP”, in *International Journal on Computer Science and Engineering (IJCSE),* vol. 3, no. 6, pp. 2377-2384, 2011.

[23] W. Weichao, B. Bharat, Y. Lu, and X. Wu. "Defending against wormhole attacks in mobile ad-hoc networks," *Wireless Communication and Mobile Computing*, vol. 6, no. 4, pp. 483-503, 2006.

[24] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L.W. Chang, “Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach”, *Proceedings of Wireless Communictions and Networking Conference, IEEE,* pp.1193-1199, 2005.

[25] N. Song, L. Qian, and X. Li, “Wormhole Attacks Detections in Wireless Ad Hoc Networks: A Statistical Analysis Approach”, *Proceeding of the 19th International Parallel and Distributed Processing Symposium, 2005.*

[26] W. Wang, B. Bhargava, Y. Lu and X. Wu, “Defending Against Wormhole Attacks in Mobile Ad Hoc Networks”, *Wireless Communication and Mobile Computing*, vol. 6, pp.483-503, 2006.

[27] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.P. Hubaux. "A practical secure neighbor verification protocol for wireless sensor networks," ACM WiSec, 2009.

[28] H. Chen, W. Lou, and Z. Wang. "Conflicting-set-based wormhole attack resistant localization in wireless sensor networks," Book Chapter Lecture Notes in Computer Science, Ubiqitous Intelligence and Computing, vol. 5585/2009, pp. 296-309, 2009.

[29] Rogers, M.Evertt ,”Diffusion of Innovations. s.l”, Free Press, 1996.

[30] W. Wang and B. Bhargava, “Visualization of Wormholes in Sensor Networks”, *Proceedings of the ACM workshop on Wireless security(Wise’04)*,pp. 51-60, 2004.

[31] A. Aldhobaiban, D. Dema, K.Elleithy, and L.Almazaydeh, "Prevention of Wormhole Attacks in Wireless Sensor Networks," *Artificial Intelligence, Modelling and Simulation (AIMS), 2nd International Conference on* IEEE, 2014.

[32] http://www.ubuntu.com/download/alternative-downloads *accessed on 1/8/2014.*

[33] http://www.isi.edu/nsnam/ns/ *accessed on 12/8/2014.*

[34]http://en.osdn.jp/projects/sfnet_nsnam/downloads/allinone/ns-allinone-2.35/ *accessed on 15/8/2014.*

[35] http://csis.bits-pilani.ac.in/faculty/murali/resources/tutorials *accessed on 19/8/2014.*

[36] Tcl Tutorial.https://www.tcl.tk/man/tcl8.5/tutorial/tcltutorial.html *accessed on 20/8/2014*

[37] A. V.Aho, B.W. Kernighan, P.J. Weinberger, The AWK Programming Language.

[38] Xgraph tutorial. http://wing.nitk.ac.in/resources/Xgraph.pdf *accessed on 7/12/2014*.

[39] F. J. Ros and P. M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", 2004

[40]http://www.nsnam.com/2014/02/adding-malicious-node-in-ns2-in-aodv.html*accessed on 20/10/2014.*

[41] J. C. Hou and N. Li, "Topology Construction and Maintenance in Wireless Sensor Networks", *Book Chapter of Handbook of Sensor Networks: Algorithms and Architectures*, John Wiley & Sons, Inc. 2005.

[42] A.Dema, K.Elleithy, and L.Almazaydeh, "Prevention of Wormhole Attacks in Wireless Sensor Networks" , *Artificial Intelligence, Modelling and Simulation (AIMS), 2nd International Conference on*. IEEE, 2014.

[43] C. Biswas, U. Biswas. "Intrusion Detection System for Power-Aware OLSR", *Computational Intelligence and Networks (CINE), International Conference on*. IEEE, pp. 142-147, 2015.

[44] A. R., Sahoo, R. R., Singh, et. al "Intelligent Intrusion Detection System in Wireless Sensor Network", *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)*, Springer International Publishing, pp. 707-712, 2015.

ANNEXURE II

LIST OF PUBLICATIONS

Published

Svarika Goyal, Tarunpreet Bhatia and A.K.Verma, "Wormhole and Sybil Attack In WSN: a Review*", INDIACOM 2015:09th INDIACOM, 2nd IEEE International Conference on Computing for Sustainable Global Development*, pp. 1463-1469, 2015. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7100491

Communicated

Svarika Goyal, Tarunpreet Bhatia and A.K.Verma, "A novel secure scheme against wormhole attack using RTT and link usage in Wireless Networks", International Journal of Communication Networks and Information Security, vol.7, no.1, 2015.

ANNEXURE III

VIDEO PRESENTATION

https://www.youtube.com/watch?v=0T7S_HyUKPg&feature=youtu.be