DESIGN OF DISTRIBUTED APPROACH FOR WORMHOLE ATTACK DETECTION IN WIRELESS SENSOR NETWORKS

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

MANPREET KAUR

11508950

Supervisor

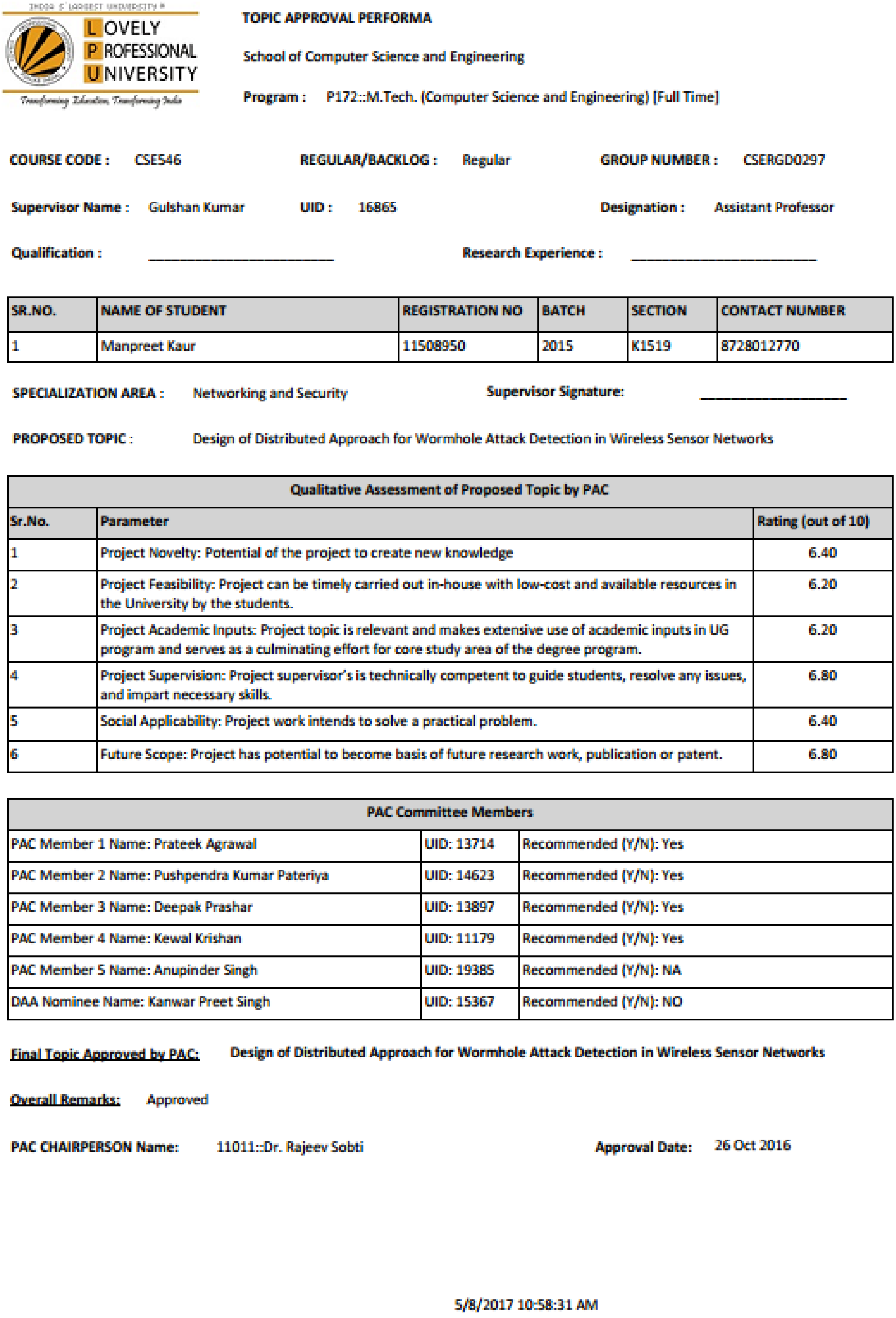
MR. GULSHAN KUMAR

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

May, 2017



INDIA'S LARGEST UNIVERSITY
LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE546 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0297

Supervisor Name : Gulshan Kumar **UID :** 16865 **Designation :** Assistant Professor

Qualification : ________________________ **Research Experience :** ________________________

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Manpreet Kaur	11508950	2015	K1519	8728012770

SPECIALIZATION AREA : Networking and Security **Supervisor Signature:** ___________________

PROPOSED TOPIC : Design of Distributed Approach for Wormhole Attack Detection in Wireless Sensor Networks

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	6.40
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	6.20
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	6.20
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	6.80
5	Social Applicability: Project work intends to solve a practical problem.	6.40
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	6.80

PAC Committee Members		
PAC Member 1 Name: Prateek Agrawal	UID: 13714	Recommended (Y/N): Yes
PAC Member 2 Name: Pushpendra Kumar Pateriya	UID: 14623	Recommended (Y/N): Yes
PAC Member 3 Name: Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member 4 Name: Kewal Krishan	UID: 11179	Recommended (Y/N): Yes
PAC Member 5 Name: Anupinder Singh	UID: 19385	Recommended (Y/N): NA
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): NO

Final Topic Approved by PAC: **Design of Distributed Approach for Wormhole Attack Detection in Wireless Sensor Networks**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11011::Dr. Rajeev Sobti **Approval Date:** 26 Oct 2016

5/8/2017 10:58:31 AM

ABSTRACT

In wireless sensor network, the problem of wormhole attack is very common and can exploit the most of the information of the network characteristics, leaving network being compromised. In order to deal with this attack many authors have published their work, but still the problem persists. In our work, we present wormhole detection by using cryptographic mechanisms. The wormhole detection methodology consists of three phases: initialization phase, neighbourhood discovery with only one hop neighbours and wormhole detection process. Cryptography is used for the confidentiality, authentication and non-repudiation of message in wormhole attack. The clustering is used to create cluster of nodes with base station as cluster head. These cluster heads then provide its cluster's base station to another cluster's base station communication for sensor nodes communication. The overhead for message transmission is also less. This scheme can help to find the wormhole attack in given network, if exists. The scheme does not even use any special hardware like directional antennas, or highly synchronized clocks.

Keywords: Wireless sensor network, Wormhole attack, Cryptography, Closeness function, Public and private cryptosystem, Clustering, ZRP.

DECLARATION

I hereby declare that the research work reported in the dissertation entitled "DESIGN OF DISTRIBUTED APPROACH FOR WORMHOLE ATTACK DETECTION IN WIRELESS SENSOR NETWORKS" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Gulshan Kumar. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Manpreet Kaur

11508950

CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled "**DESIGN OF DISTRIBUTED APPROACH FOR WORMHOLE ATTACK DETECTION IN WIRELESS SENSOR NETWORKS"**, submitted by **Manpreet Kaur** at **Lovely Professional University, Phagwara, India** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Mr. Gulshan Kumar

Date:

Counter Signed by:

1) **Concerned HOD:**
HoD's Signature: ________________
HoD Name: ____________________
Date: ___________________

2) **Neutral Examiners:**

External Examiner

Signature: _______________

Name: __________________

Affiliation: ______________

Date: ___________________

Internal Examiner

Signature: _______________

Name: __________________

Date: ___________________

ACKNOWLEDGEMENT

I would like to express my profound gratitude and my deepest regards to my guide and mentor Mr. Gulshan Kumar for his exemplary guidance, monitoring and constant encouragement throughout the course of my dissertation work. The blessings, guidance and help given by him time to time shall carry me a long way in the journey of my life.

This work could not be successfully completed without the valuable teachings of our professors. Their ideal teachings help me through the course of my dissertation study. I would like to take this opportunity to deliver the truest respect and deepest admiration to my professors.

I would also like to express my gratitude towards my educational institution Lovely Professional University for providing the immense opportunities for research and exploration.

Lastly, I would like to thank my almighty and my parents for their constant encouragement which also helps me to carry out my course of dissertation work with full enthusiasm and diligently.

TABLE OF CONTENTS

CONTENTS **PAGE NO.**

TABLE OF CONTENTS

TABLE OF CONTENTS

CONTENTS PAGE NO.

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

In today’s technology era, we have immense power of technological advances which enable today’s man to perform good for society and contribute to mankind by developing new technologies and researches in this huge world. In today’s world network is a backbone of any organization and this network can be of different types varies from requirement to requirement of an organization. The burning trend is of wireless sensor networks. These networks are infrastructure-less, distributed, ad-hoc and dynamic in nature. As these are widely used networks, then it need to be secure from various attacks launch by the attackers. Wireless sensor networks are very prone to the variety of attacks due to its open, distributed and dynamic nature. One of the major attacks on the sensor networks is wormhole attack. The wormhole attack is launched by adversary to exploit the network topology and perform other malicious attacks such as blackhole attack, gray hole attack, DoS attack etc. many of the research has been done over years on wormhole attack affecting the sensor networks. But still we have not find any plausible and competent solution to this problem. We proposed a distributed solution to tackle the problem occurred by wormhole attack in the wireless sensor networks.

1.1 Wireless Sensor Networks (WSNs)

The term Wireless Sensor Networks [1] can be defined as:

> "A wireless network with no fixed infrastructure that consists of sensor nodes which communicate with each other in the network via wireless transceivers."

WSNs are mainly deployed in large remote areas where other networks are either infeasible or very difficult to deploy. WSN provides an ease to access the landscapes which previously were inaccessible. The sensor nodes deployed in large numbers in such areas in order to collect and extract information nearby environment. WSN are very helpful in emergency and time alert situations. Basically, WSN has a wide variety of applications in almost every field of study. The sensor nodes used in WSN comes in different shapes and sizes, and also cost differently from a penny to thousands and lakhs of rupees. These sensors nodes are configuring in such a way that it can perform a specific single operation or can perform multiple operations too. Each sensor node comes with different configurations and some are customizable.

A wireless sensor network consists of three major components[2]:

- Sensing node
- Sink node
- Wireless transceivers

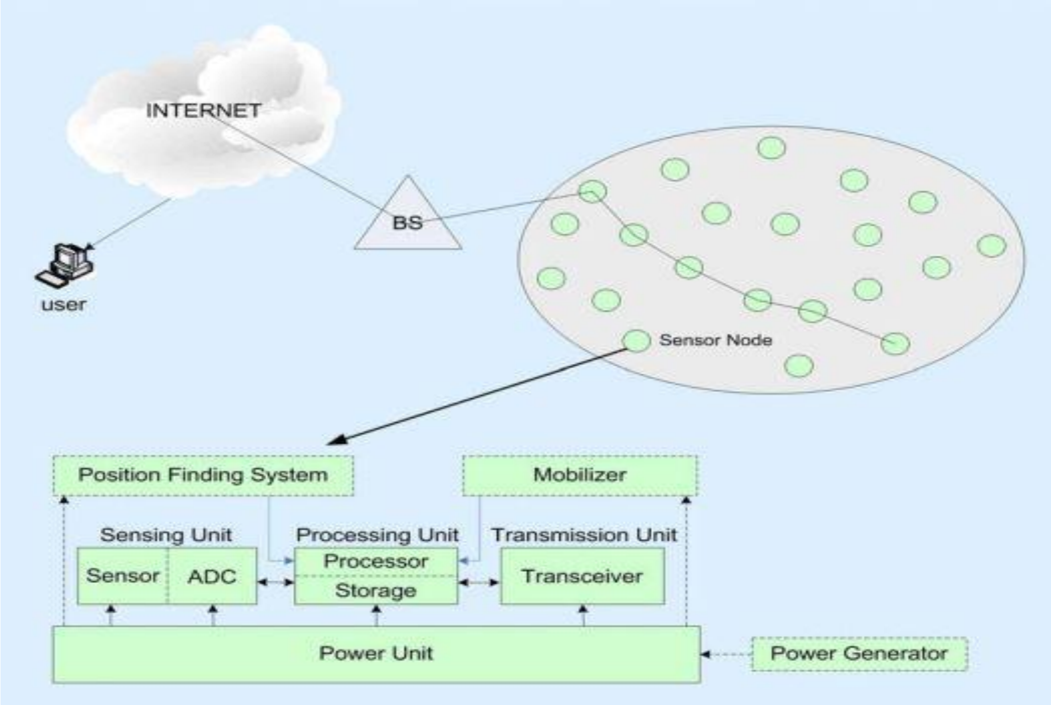


Figure 1.1: Wireless Sensor Network

1.1.1 **Sensing node** is any normal sensor node that collects data from surrounded environment and process that collected data and transmit to the nearby sink node. Sensing node senses the environment in which it is deployed.

1.1.2 **Sink node** is like a cluster head or we can say 'sensor head' which receives the collected data from sensor nodes and process them for further transmission to the base station. Sink node performs the local calculations over sensed or observed information sent from sensing nodes. For multiple sensing nodes, there is one sink node.

1.1.3 Wireless transceivers help sensor nodes to communicate with one node to another node within the network. It is responsible for message exchange between sensor nodes and makes communication possible between them.

There are different types of wireless sensor networks ranges from low cost to high cost. Some of the types of wireless sensors are: acoustic, seismic, heat, image, direction, temperature, light, smoke, etc.

The deployment of sensor network can be affected by various constraints. These constraints affect adversely on performance of wireless sensor networks. Some of them are[3]: memory requirements, energy requirements, security alternatives, suitability of protocols, type fabrication of the device, computational speed and communication bandwidth required, cost factor, etc.

Wireless sensor network has huge application area. It can be implemented using multiple techniques in almost every field of study. Some of the various application areas for WSNs are[4]: military services, surveillance setup, commercial sector, medical field, battlefield, logistics and manufacturing, home automation, etc.

Due to the characteristics of WSNs, it is very prone to threats and exploits most of the network vulnerabilities. Security in WSNs is a very crucial issue for today's scenario. As a network grows day by day, the threats to the network also increasing day by day. Securing WSN is essential to keep the services of WSNs going smoothly and efficiently.

Attacks on wireless sensor network are categorized on different grounds. There are numerous of attack possible to launch in wireless sensor networks. Some of those attacks are[5]: blackhole attack, grayhole attack, sybil attack, sinkhole attack, hello flood attack, selective forwarding of packets attack, replaying routing information attack, byzantine attack, DDoS attack, vampire attack, wormhole attack, etc.

Wireless sensor network meet with piles of challenges which need to be dealt. For dealing with these challenges various techniques are adopted. The major challenges faced by WSNs are[6]:

- Spectrum allocation for network and purchase of the same
- Media access to network
- Routing techniques used for routing information in network
- Multicasting in network
- Energy efficiency of nodes in network
- TCP performance in network
- Service location in network, provision granted and access granted for nodes in network
- Security of information and privacy for the same in the network.

1.2 Wormhole Attack (WHA)

In this study, we are focusing only on wormhole attack as it is a very big issue in WSNs.

The wormhole attack can be defined as[7],

> “the scenario in network when an intruder/s create tunnel/s at distinct ends in network and bypass the communication channel of other valid nodes by providing them false neighborhood information and receiving most of the network traffic and discarding it”

The WH attack is very common in networks and is difficult to figure it out initially. WH attack occurs when two or more malicious nodes creates a tunnel between them and tunnels the packets received at one end to another end in order to provide false routing information to the valid nodes. Due to this false behavior, the valid nodes may have false neighborhood information and be tricked into delivering the packets to these malicious nodes, without even knowing their existence because nodes may believe the network is always safe. The malicious nodes in the network are called as wormhole nodes and the tunnel they created is called as wormhole link.

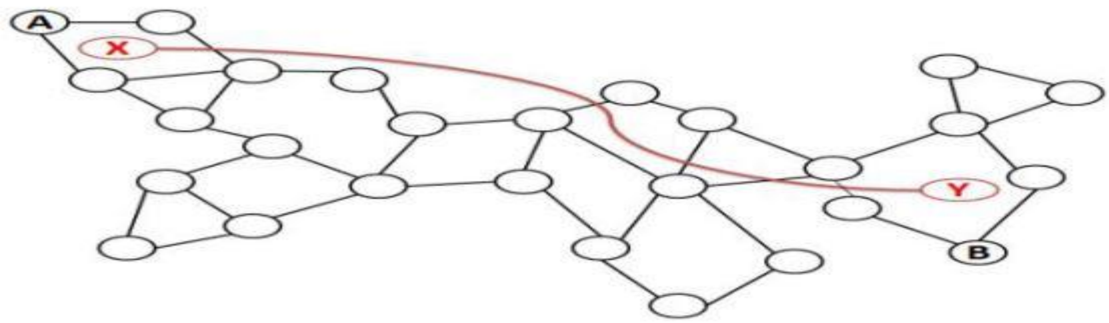


Figure 1.2: Wormhole Attack

Let us consider a scenario, here two malicious nodes X and Y are forming a tunnel and tunneling the packets between them. Here node A is the source node want to send packets to destination node B. There are other nodes present in network also. There exist two wormhole nodes X and Y. At first source node initiate route discovery process by broadcasting hello packets in the network. Again, in the process, on receiving hello packets by node 2, it broadcast them to its neighbor and so on. When X receives hello packets it tunnels them to the other end making source node A believes that it is the shortest path to the destination. Accordingly, source node A makes the entries in the routing table and start transmitting actual data packets via this link which leads to wormhole attack. Hence, wormhole attack is successfully implemented.

In WH attack, the malicious nodes create in-band or out-of-band or dedicated channel tunnel through which they tunnel the packet from one end to another end, which is present at some distinct location not known by other nodes in its vicinity. The malicious nodes will project themselves as valid nodes having shortest path to the destination node, it is because of the wormhole path. The sender node will then transmit packets to this route and hence tricked into the false routing information provided by the malicious node.

WH attacks can be of two types:

1.2.1 **Hidden wormhole** attack is launched by node present external to one network.

1.2.2 **Exposed / byzantine wormhole** attack is launched by node present internal in the network. Internal nodes are assumed to be part of legitimate valid nodes that is why they successfully bypass security mechanisms. Hence it is difficult to detect at initial stages.

WH attack can be launched in many ways:

- WH launched against routing protocols
- WH launched against local broadcast protocols

In the former technique, WH launched on periodic and on-demand protocols. In the latter technique, WH launched as providing false local information consequently degrading the performance of the estimation algorithm used by cluster head in WSNs for monitoring and broadcasting local computations by sensor nodes.

There are various countermeasures to deal with WH attack each with their different advantages and disadvantages[8]:

1.2.3 In **time-based solutions**, WH detected by checking if packet traveled too far by comparing time information. This solution is reliable and detection rate of WH is also high. But, it requires tightly synchronized clocks, overhead also increase the size of packet increases.

1.2.4 In **location-based solutions**, time synchronization is not required. The attacker is identified as it appears to be at multiple locations. But still, it requires geographical leashes with radio propagation model which is expensive and upper bound on velocity is also difficult to define.

1.2.5 In **end-to-end based solutions**, cross-examination approach. Not much of computation overhead is required and also not tightly time synchronized. But, it cannot scale well for long routes and also byte overhead is increased with increasing path length.

1.2.6 In **Hop-count analysis based solutions**, an attacker cannot intercept the content on any route completely. No clock synchronization and location information are required. Although, the dynamic information of the packets can still be easily modified and also attacker can add fake routes so that routes have longer distances to reach to particular destinations and having message overhead.

1.2.7 In **Statistics based solutions**, there is limited overhead and only need routing information. It can work well under different network topologies and with different radio transmission ranges of the nodes. The lower rate of the false alarms. But it cannot be directly applied to table driven routing algorithm. If attacker nodes behave normally, it cannot be detectable. It also cannot pinpoint the location of WH.

There can be various problems due to WH attack in WSN which is discussed in underlying section. We provide a distributed solution to address underlying problems in wireless sensor network.

1.3 Problems due to wormhole attack in wireless sensor networks

As we know WSN is very prone to WH attack, it can create various problems and security related issues in WSN. Some of the problems are:

1.3.1 The **confidentiality of data** is essential for any node in the network. But it is broken due to WH attack in the network. As the packet flows through the tunnel, the malicious node can easily bypass the security mechanisms and decrypt the whole packet data. As such gains data within the packet.

1.3.2 The **integrity** loses when the malicious node corrupts the data before sending it to the valid nodes. The integrity of the data will be lost. The valid destination node cannot get the valid data send from the valid source node. Hence causes a problem in the network.

1.3.3 The **authenticity** can be broken easily with WH attack. The valid nodes cannot get to know which the valid node are and which the malicious nodes are. The valid nodes will be confused with the identity of t=its neighbor nodes due to WH attack being launched in their neighborhood.

1.3.4 The **problem of repudiation** can occur when malicious node route false routing information to the nodes in their vicinity. The malicious nodes can deny for any route request and reject the packets for particular routes, causing a problem in the network.

1.3.5 The **authorization** can also be violated when there is some malicious node launching WH attack. The node will not be able to recognize the authorized node in the network, hence, failing to establish a secure communication channel.

1.3.6 The **characteristic of anonymity** in WSN is exploited while the network is under WH attack. The malicious nodes can exploit the identity of the nodes in their vicinity. This can become a big issue in the network.

1.3.7 The **availability issues** can also arise due to WH attack, as the malicious node tries to trick the valid nodes with false routing information. Hence, the valid destination node will not be available to the valid source node, thereby non-availability of nodes and other resources can occur.

These problems can be dealt with using different types of mechanisms. Some are discussed in the above section and some can be:

- Security aware ad-hoc routing protocol
- Routing using pre-deployed security infrastructure
- ARIADNE
- Self-securing ad-hoc wireless networks
- On-demand secure routing protocol resilient to byzantine failures
- Secure distance vector routing protocol using SEAD
- Optimized inter-router authentication scheme
- Analytical hierarchy process methodology
- SECure NeighborhooD creation in wireless ad-hoc networks using hop-count discrepancies
- Localization based scheme
- Schemes based on trust value of a node
- Local connectivity tests
- AOMDV
- Wormhole Resistant Secure Routing, etc.

There can be other techniques as well for these problems. In our research study, we put focus on a distributed manner to tackle with wormhole attack scenario to developing a solution for the same.

1.4 Parameters to measure the effectiveness and performance

To come to a conclusion, we must define some parameters on which the different schemes can be judged for their effectiveness and performance. The parameters we define for our research work are as under:

i. **Wormhole detection or prevention:** shows if the proposed schemes are able to detect or prevent the wormhole attack.
ii. **Delay:** shows the delay dealt by schemes.
iii. **Throughput:** shows the maximum number of transmission per unit time.
iv. **Computation Overhead:** shows the overhead dealt by schemes in various computations.
v. **Support dynamic topology:** shows whether or not the schemes support dynamic topology changes.
vi. **Hardware constraints:** shows whether schemes require extra constraints on hardware.
vii. **Impact of scalability:** shows the effect of scalability.
viii. **Impact of network load:** shows the effect of load in network.
ix. **False positives:** shows the rate of false positives detected.
x. **Cryptographic mechanism required:** shows that if some security features like cryptographic mechanism are required.

These are the parameters we employ to measure the efficacy of our proposed work and already proposed work.

1.5 Clustering in wireless sensor networks

The clustering in the wireless sensor network can be defined as[9]:

> **“**The process of classifying group of nodes and group them on the basis of their characterization or attributes**”**.

The process of grouping sensor node on the grounds of some common attributes is called clustering. The groups created by clustering process is called clusters. These clusters are group of such sensor nodes which common in some aspects and share some common attributes. The clustering shows the distributed nature of deployed network. The main reasons for emergence of clustering is the decentralized nature of operation.

1.5.1 Structure of Clustering

In clustering we are having two important nodes that is cluster head and member nodes. The cluster head are the only form of communication with another cluster's nodes. Member nodes are the other nodes present in the cluster and is monitored by the cluster head.

There are two types of communication possible in clustering:

- **Inter-cluster communication:** In this the cluster head are communicating with other cluster head for the communication purposes from one source to another which is not present in the same cluster but present in the other cluster far away.
- **Intra-cluster communication:** In this communication takes place within one cluster only, no other nodes from other cluster than itself is involved. No foreign nodes will participate in intra- cluster communication.

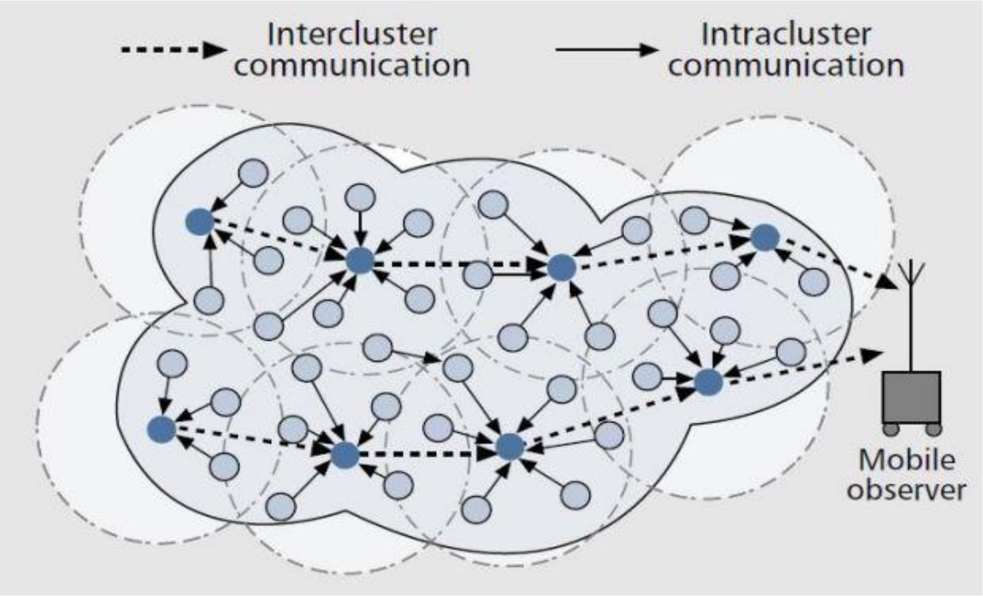


Figure 1.3: Clustering

1.6 Zone Routing Protocol:

The zone routing protocol is a hybrid protocol for routing in clustered networks[10]. It is hybrid because it make use of good things from both proactive and reactive protocols. In ZRP, we are having the nodes clustered into different zones based on some distance or range.

In ZRP we have two nodes: peripheral node, those which lie on the border of a zone and involves in inter-zone routing, and interior node, those which lie inside a zone and performs intra-zone routing. In ZRP, we are having two types of routing algorithms[11]:

- **Inter-zone routing protocol,** for communication between different zones and uses reactive protocol features.
- **Intra-zone routing protocol,** for communication within same zone and uses proactive protocol features.

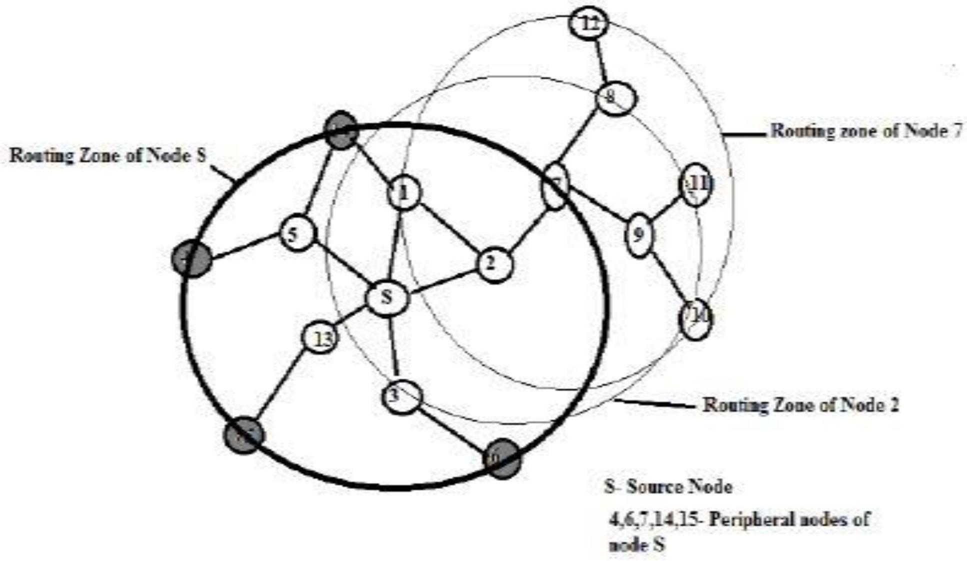


Figure 4: Zone Routing Protocol

Example of ZRP shows the routing zones for source node and node 2 and node 7. The peripheral nodes are also shown.

CHAPTER 2

REVIEW OF LITERATURE

In order to come to a conclusion, first thing that is needed is to gather knowledge of that particular topic. For research study, various available literature on wireless sensor networks and wormhole attack which describes the state of art of the topic very well, are reviewed. In literature review, different techniques in order to mitigate the problem are found. But they are not enough for the growing need of security for the networks. Today's time requires a distributed approach.

In study of [12]work proposed for fault tolerance using spider-net ZRP in the mobile sinks of WSNs proposed by Shih Hao Chang and Ping Tsai Chung, aim is to propose a scheme for energy-efficiency, reliability and improved performance in WSNs mobile sinks. The author uses the phenomenon of spider, that how it create its web and collect silk moving in its web. The author make use of the spider-zone routing protocol for tackling the fault. The scheme is based on the query based data dissemination. The authors make some initial assumptions for the execution of their planned methodology. At first the mechanism for topology creation of zone in spider-net is initialized. There will be 3 cluster heads by election: core-cluster head, gateway-cluster head and intermediate-cluster head. After electing cluster heads a mechanism for data dissemination will start in the spider-net. Finally a mechanism for managing fault tolerance boot up to deal with any fault residing in inter spider-net, the data is collected and redirected to the mobile sinks. At last if fault occur then a consensus based fault tolerant algorithm is come into play.

In study of [13] key management methodology for securing transport and network layers in MANETs using ZRP and WTLS key management proposed by Dr. G. Padmavathi, Dr. P. Subashini and D. Devi Aruna, aim is to providing security to layers authentication, communication privacy and integrity of data and to defend against DoS attack. The main focus of the authors is on the DoS attack prevention by providing security to the two discussed layers. The authors use public key cryptosystems for encryption of data packets in order to provide the essential security. The use of encryption will surely prevent from confidentiality and integrity threats. For the scope of their work the authors use ZRP and WTLS for securing communication in the network.

In study of [14] a scheme for detection as well as prevention of wormhole attack exists in WSNs using AOMDV routing protocol which is proposed by Parmar Amish and V.B. Vaghela, aims to detect and prevent wormhole attack in WSN using AOMDV protocol. According to the proposed work, when source node broadcasts RREQ packet, it will note the time, t. Then for each RREP received by source node, time is noted, say, tr. Sender node then calculates round trip time for all routes using formula, tx=tr-t. Then threshold round trip time is calculated by using formula, z= tx1+tx2+txi/i. if tr is less than threshold and hop-count on route i is equals to 2 the it detects that route i as wormhole link. Sender detects first neighbor node as wormhole node. Then sender sends dummy RREQ through route i. receiver on receiving dummy RREQ from its neighbor and detects it as wormhole node. Routing entries for that route is removed from routing table and broadcasts to other nodes as well. No special hardware is required. It performs well in dense networks. Less end to end delay and improved packet delivery fraction. But mobility mode is fixed also overhead in calculating round trip time for every node.

In study of [15] an approach for design and implementation of trust based approach in order to reduce the various attacks occurring in MANETs presented by Nilesh N. Dangare and M.S. Mangrulkar, the aim is to mitigate Vampire and DDoS attacks. They proposed a technique in which they form a cluster based network, then selection of two nodes having highest energy called trusted nodes, takes place. Then packets and route responses for each node in network is counted. After this a comparison of threshold value with counted values has been made to get malicious nodes. Lastly routing table of nodes are updated accordingly. They choose AODV routing protocol as it is loop free and no central administration is required also it avoids count to infinity problem. This technique use no special hardware. Overhead of calculations is also less and it is easy to implement. But it restricts its functionality to very low mobility networks. It fails when network is highly dynamic and continuously changing.

In study of [16] wormholes virtualization concept in WSNs presented by Weichao Wang and Bharat Bhargava, aim is to propose such a mechanism that can detect wormholes in sensor network. They proposed scheme named MDS-VOW. It will reconstruct the network by using the distance between sensor nodes. Then it will perform distance error compensation and lastly it will start detecting for wormhole present in the network, if any. Proposed work does not need any special hardware and every module is performing their designated task independently. But the proposed schemes is centralized in nature and also less adaptable. MDS–VOW can detect almost all the fake terminals and connections with very less chance of producing false positives.

In study of [17] a mechanism for defense against wormhole and DoS attack in WMNs presented by G. Akilarasu, S. Mercy Shalinie, aims to introduce technique that find wormhole free routes in networks by some finite state model and priority mechanism. The authors apply finite state model in which node keeps info of sender and receiver with neighbor nodes. Each node acts as monitor node, each monitor checks sequence of local message block with authorized certificates. By collecting information from RREQ and RREP, wormhole links are detected and then wormhole aware routing is initialized. For detecting DoS attack a priority table is created for each node. Packets with low priority is discarded first to ensure transmission of legitimate nodes. No additional information regarding location is needed. Lesser delay and packet drop than WRSR. Delivery ration is also more in case of WRDAD. Eliminates both selfish and DoS attacker nodes. It induces overhead, also not efficient for dynamic topology. Length of wormhole may affect the discovery of wormhole routes. This scheme is also reducing packet drop and increases packet delivery ratio.

In study of [18] RFAF localization in WSNs under wormhole attack presented by Yurong Xu, Yi Ouyang, Zhengyi Le, James Ford, and Fillia Makedon, aim is to study localization protocol effects under wormhole attack and also provide a distributed remedy to address wormhole attack. In this presented work, authors implemented RFAF algorithms to act as routing algorithms, 3 in particular, and a bootstrap node to count the number of hop with Carnegie Mellon University wireless extensions. A wormhole is implemented as wired connection so that higher throughput can be achieved to obtain low latency for forwarding packets from one node to another node. The authors used two configurations for wormhole to simulate RFAF localization:

1. a single wormhole with two ends in network
2. variable number of wormhole in network

The authors introduces a parameter to evaluate how much localization is affected by the wormhole. It is named as WID, wormhole induced distortion, and is based on localization error.

In study of [19] a technique of WRSR for WMNs proposed by Rakesh Matam and Somnath Tripathy, aims to detect presence of wormholes during route discovery process. In this proposed work authors allow nodes to monitor two-hop sub-path on received RREQ and identify RREQ that traverse wormhole. Nodes maintain neighborhood relations with all nodes in their two-hop range. For this extended Ethernet beacon frame including flag bit and neighbor address is used. Intermediate nodes received broadcasted RREQ and verifies their identity for two-hop neighbors and create routing entry for that RREQ_ID, sets it's state as transient and rebroadcasts it, otherwise drops it. The proposed work is able to defend against all types of wormholes with no extra requirement of specialized hardware. No synchronized clocks and no cryptographic mechanisms are required. But If no alternate path is discovered other than wormhole, then all process need to be re-done from start. It fails to detect wormhole link when both wormhole nodes are neighbor of each other.

In study of [20] schemes for secure routing proposed for mobile wireless ad hoc networks presented by Siddhartha Gupte, Mukesh Singhal, aims to criticize and get to know available protocols aimed at secure routing in mobile wireless ad hoc networks. In this piece of work, possible attacks on routing protocols are categorized and explained differently and very unambiguously. After that properties that should be in a secure routing protocol is discussed. Then some protocols such as security aware ad hoc routing protocol, ARAN protocol, ARIADNE, TESLA, on demand secure routing protocol, SEAD etc. are explained very precisely with this, self-securing ad hoc wireless networks, mitigating malicious behavior and optimized inter-router authentication scheme is discussed. Every protocol has different advantages and disadvantages. No protocol is in all aspects is efficient for routing and we cannot say all present protocol are fail-safe or secure.

In study of [21] comparison of wormhole attack prevention techniques in mobile adhoc networks presented by Subhashis Banerjee and Koushik Mujumdar, aims to carry out detailed comparative analysis of well-known countermeasures against wormhole attack according to their relative advantages and disadvantages. The authors compare different protocols and review the countermeasures against wormhole attack based on location and time, end-to-end detection, hop-count analysis, statistics. This work exploit the features of different types of protocols and helps to find out efficiency of proposed protocols. Protocols suffer from their own weaknesses. Need for specialized hardware. Larger overheads due to computation, communication, message, packet size and storage capacity. Most protocols proposed are not sufficient for MANET. Routing protocols for MANET are vulnerable to inherent design disadvantages. Time synchronization based prevents only closed wormhole attack. Statistical analysis based prevents multiple wormholes but require enough routing information and low mobility network. Reliability of hop count based are inversely proportional to communication overhead. A technique is required which combine features of both software and hardware driven techniques.

In study of [22] a mechanism against wormhole attacks in mobile adhoc networks with the help of AHP methodology proposed by Fei Shi, Weijie Liu, Dongxu Jin and Jooseok Song, aims to elect local most trustable nodes for source and destination to detect and locate wormholes using AHP. The authors proposed electing LMT nodes with largest weight value for source and destination by using relative stability of node, credit value of node and reciprocal of forward rate of node. AHP is measurement of pairwise comparisons and priority scales to elect LMT nodes. First is detecting phase, in which LMT node will set timer for HELLO messages sent and HELLO reply received. Then minimum hop is estimated proceeding with hop count extracted from RREP. After this locating phase started, LMT node set its timer for TRACE sent and TRACE reply received. Then Hop count is tested by comparing current value with last obtained values by which location of wormhole is located. At last bi-directional location mechanism phase starts, to solve collaborative wormhole issue. It can detect and locate wormhole nodes with high precision. It is a hierarchical approach and use bi-directional location mechanism. It has large computation overhead and so time consuming. The assumed network is Static so difficult to implement in dynamic and changing environment. Wastage of resources if wormhole does not exist in network. Delay in transmission of packets with bulk of computations performed.

In study of [23] creating a secure neighborhood in wireless ad hoc networks with the help of discrepancies in hop count proposed by Thaier Hayajneh, Prashant Krishnamurthy, David Tripper and Anh Le, aims to create secure neighborhood by using hop count discrepancies in routing to detect true neighbors and remove those links that appear to be neighbor but in real are not. In the proposed work by authors, source node will discover its one-hop neighbor. Neighbors could be elements of either NA or NA*. Source asks b to provide its one-hop neighbor list NB. Source picks some nodes belongs to NB-NA and makes it as target node T. Source will then find shortest paths to T, paths must not be direct and avoid one hop neighbors of source and B. Source node employs select(route) and compare it with route that have wormhole. If difference between selected and wormhole route is > threshold then SECUND declares wormhole link. There is small overhead in terms of number of links checked for wormholes. No need for location information, very high node degree and accurate sync. But it does not work well with high value of threshold. It fails when source picks bogus node as target node. It demonstrated excellent wormhole detection rate with few false alarms, also capable of removing bogus links from network while removing only few legal links.

In study of [24] localized scheme for detection and prevention of wormhole in wireless networks presented by Tassos Dimitriou and Athanassios Giannetsos, aims to defend against wormhole attacks in wireless networks by not adopting any specialized hardware. This work is based on assumptions:

a) SMA1: all sensor nodes run some neighbor discovery routine and can record their neighbor ids.

b) AMA1: wormhole link is long enough so that regions A and B are well separated from each other

c) AMA2: there is some initial interval t where no attack is taking place and nodes can safely establish neighborhood information.

Algorithm is strictly localized and only nodes undergo topology changes need to run it. Each node u, upon discovery of new suspect node v, searches for such paths using k-hop neighborhood knowledge. K should be a small value. The parameters for the performance measurements are small paths, path existence %age, detection time, memory footprint and time required for detection and prevention. It only uses connectivity information and is efficient in memory and processing overhead. It is fails safe, easy to implement and support dynamic networks. But attacker can fool algorithm with small wormholes. It fails if attacker make fake links in neighborhood of wormhole end-points. It is also unable to prevent combined wormhole attack. It is lightweight enough to run on sensor nodes.

In study of [25] identifying wormholes on the basis of local connectivity tests in wireless networks proposed by Xiaomeng Ban, Rik Sarkar, Jie Gao, aims to detect and remove wormhole using LCTs. This approach is to examine graph connectivity and detect fundamental connectivity change. This approach is classified into four steps:

1. rigorous definition of wormhole attack.
2. guaranteed detection on wormhole sets
3. robustness to different communication models and dimensions
4. scalability and communication costs

It guarantees to detect true wormhole nodes. Longer wormholes are easy to detect. It is not influenced by placement of wormhole and has smaller communication costs. Multiple wormhole can be well recognized. But there is greater chance of false positives with smaller length of wormhole. It is not suitable for highly dynamic environment.

In study of [26] a detailed case study on mobile adhoc networks protocols for routing to check their performance over transmission control protocol and hypertext transfer protocol presented by Yamsani Ravikumar and Sarath Kumar Chittamaru, the aim is to find out efficient routing protocol for routing among DSR, OLSR and AODV. For this Two scenarios created in NS2 one with 10 nodes and other with 50 nodes. Firstly, impact of scalability on protocols performance is taken under consideration. Secondly, impact of network load on protocols performance is measured by creating two scenarios with 50 nodes each with constant speed of 10 m/s but with different profiles one as HTTP heavy load traffic and other as HTTP light load traffic. Thirdly, impact of node mobility on protocols performance is measured by creating two scenarios each with 50 nodes with speed of 10 m/s and 28 m/s respectively over 1000mX1000m area. Fourthly, impact of TCP over protocols performance have been measured by creating two scenarios each with 50 nodes and HTTP heavy and light load respectively over 1000mX1000m area simulated for each protocol separately for 10sec for two scenarios. The parameters for comparison is less. We found that OLSR is scalable and can work in high node mobility also delay is less when load is also less, AODV can handles network load and delay is less even when the load is high. TCP only shows less delay when load is also less.

In study of [27] a statistical approach to detect wormhole in multi-path routed wireless ad hoc networks proposed by Lijun Qian, Ning Song and Xiangfang Li, aim is to develop an approach, which is based on Statistical Analysis of Mutli-path, to detect wormhole attack and helps to identify the malicious nodes in network. The author implemented the proposed work deploying two network topologies i.e cluster and uniform. The proposed method consists of three steps:

1. At first node will initiate route discovery, based on this route discovery a statistical analysis on the routes will be performed. If any malicious or ambiguous patterns exists then continue to step 2 else choose the paths to reply the source.

2. Now need to test those suspicious routes by sending probe request packets and then wait for acknowledgement packets.

3. If there really exists an attack and is confirmed, acknowledge the same to admin or acknowledge the source and other nodes so that it can cut-off from network.

It can detect and locate wormhole nodes with varying topologies with varying transmission ranges. It can also extend to detect DoS attack, also can act as an IDS module. It involves very less overhead and only requires route information. If the wormhole nodes behave normally as other nodes then difficult to detect. This technique cannot be directly applied to table driven protocols.

In study of [28] a secure routing protocol SeRWA to provide reliable and secure routing under wormhole attack in WSNs proposed by Sanjay Madria and Jian Yin, aim is to implement such a technique for secure routing when wormhole attack exists in sensor networks. The scheme proposed by author is consisting four steps:

1. 1-hop neighbor discovery
2. Route discovery initially
3. Dissemination of data and detecting wormhole nodes
4. Discovering secure route against existing wormhole route.

It assures to provide a real secure route against wormhole route. It gives very less of the false positives and use very less energy. It does not require high memory to perform its functions. It is only a detection scheme. The scheme use symmetric key cryptography.

In study of [29] localization of in-band wormhole tunnels based on timing in MANETs presented by Jinsub Kim, Dan Sterne, Rommie Hardy, Roshan K. Thomas and Lang Tong, aim is to detect those malicious nodes involving in wormhole attack. At first binary hypothesis testing is used to test if there is a path which is using tunneled packet traffic. The author evaluate the detection process using VoIP traffic that is generated in network. Later, multiple hypothesis testing is considered in order to find out most probable tunneled path in whole network. An estimation algorithm for tunneled path is presented and fro its evaluation Poisson traffic is generated. The presented work is robust against chaff packets, loss of packets and different clock skew. It can definitely identify the wormhole nodes. But still there are some situations when detection of tunneled traffic is hard.

In study of [30] 6LoWPAN security in accordance to avoid hidden wormholes by using the reciprocity of channel proposed by Konrad-Felix Krentz and Gerhad Wunder, aims is to propose a mechanism to reduce false positives and false negatives in wormhole detection. For this a mechanism named SCREWED is proposed. It is Secure Channel Reciprocity-based WormholE Detection. It is implemented in 2 phases: Sampling and Judgements. It eliminates the need of calibrating RSSIs ad avoids false positive and false negatives. It waive special hardware, no calibration problems, nodes are battery-powered and operation is localized. But the nodes will consume more energy. It is unable to detect adaptive wormholes. It starts again for every dropped neighbor.

In study of [31] defense mechanism against wormhole attack while using OLSR routing protocol presented by Liang Fan Cai, aim is to create a trust model for tackling wormhole in OSLR. The author place a trust evaluator for every node to collect data from surrounding neighbor events, filter those events assign a value to those events and calculate trust level. The evaluator is performing 3 tasks: deriving trust, quantize and compute. There is no need for any network sync and global positioning system apparatus. It may not be able to operate well in dynamic or high mobile networks, also the trust evaluated lag from attack.

In study of [32] wormhole attack detection in WSNs using a distributed approach, proposed by Yurong Xu, Guanling Chen, James Ford and Fillia Makedon, aim is to give a distributed detection of wormhole algorithm for WSNs, detection is based on distractions in network created by wormhole. The proposed work follows three phases: a procedure of probe, computation of local map and procedure for detection. In the algorithm probe procedure is based on a technique of hop counting, then node will reshape their local map and use a special feature i.e diameter feature for detection of distractions created in network by wormhole nodes. It finds out the location of wormhole with very less false positives and negative.

In study of [33] attack of wormhole in the WSNs presented by Raj Shree and R.A. Khan, aim is to scrutinize wormhole attack in WSNs and those schemes that stand against wormhole attack with no special requirements. The author mainly focused on the packet leashes concept. Other mechanism are also discussed for varying networks.

In study of [34] detection of wormhole attack in WSNs presented by Zaw Tun and Aung Htein Maw, aim is to review the wormhole attack nature with its already proposed schemes, also authors propose their own RTT mechanism and neighbor numbers depending detection of wormhole. The methods contain 3 steps:

1. Construct list of available neighbor in vicinity of each node.
2. Initiate route discovery to destination.
3. Locate the wormhole links and take appropriate step.

The proposed work show good performance results and have very little overhead, also it does not require high energy.

In study of [35] discrete wavelet transform detection of wormhole in WSNs proposed by Mohammad Nurul Afsar Shaon and Ken Ferens, aim is to detect the wormhole link in network consists uniform and non-uniform sensor distributions using DWT. The author set a detector node for giving a series of neighbor count into discrete wavelet transform, and scrutinize the produced wavelet coefficients for detection of wormhole. It has low network overhead and high precision with minimal false positives.

In study of [36] wormhole detection in WSNs presented by Kashyap Patel and Mrs. T. Manoranjitham, aim is to simulate launching of wormhole attack in order to detect it and to provide security in WSNs. The author described the launching of wormhole and detecting it. The wormhole is implemented in 2 steps:

1. Wormhole node send rogue capacity of link to all nodes in its vicinity.
2. Sender node make wormhole node as root node.

In literature review, the findings push towards the creation of some distributed approach to overcome at least some of the current scenario problems, as we know that not only a single approach can stand against for whole of the problems cropping up in the networks. This is the reason for creating a distributed approach, which may integrate with other approaches to overcome most of the anomalies facing by networks today.

CHAPTER 3
SCOPE OF STUDY

The scope the study lies in the limitations of the study. The current network scenarios are not reliable and the protocols used for the securing the network is also not doing exceptionally well. As a solution to current state of art problems we need a distributed approach. In this study, we try to exploit the research areas where a distributed approach can fit into and proposed a distributed approach.

The scope of this study covers the huge range of network routing protocols and the protocols securing the networks. In network, we cannot say that there is no malicious node present at initial stages or at latter stages, but we can always try to be defensive towards such attacks because if once attack is launched it might exploits valuable information about the network and may harm the useful information running in network.

A distributed approach hence might be a reliable solution to face the scenarios and provide solution to the problem in the network. As this study is focused on wireless sensor networks, but it can be extended to other types of networks also by upgrading the mechanisms provided in the study.

3.1 Limitations of the research

The presented work by different authors is lacking in certain scenarios. Today there is a need of highly dynamic network, which changes rapidly without being unreliable or disrupts any of the network functionality. There are only some of the proposed work which are giving this features of dynamics but then they lack in other aspects.

We need to find a solution which can serve better as the proposed methods and also perform well in adverse conditions. The security must be our main motive as well as the efficiency of communication between nodes in network. Only a distributed approach can solve these problems, so we provide a distributed solution. All the security issues due to wormhole attack can be dealt with this approach.

3.2 Specific data used for research

For the study purpose of this work we refer to different research papers provided by different authors. We study those papers and analyze the areas where their methodology is lacking. Then we try to work on their limitations to overcome the problems faced by their proposed work. In many of the already proposed work by other authors on wormhole and wireless sensor networks exploits major areas where research is possible. Through this study, we also try to deal with the area where we can use the distributed methods reliably and secure the networks and enhance the efficiency of the network.

3.3 Theories used to interpret data

We use basic comparison metrics for the interpretation of the data with various parameters to measure their performance under certain circumstances. Simulation is used to collect the results from the proposed work and to measure its effectiveness. Various simulation parameters are used for this purpose. For the effectiveness of proposed work some evaluation parameters are used.

CHAPTER 4

PRESENT WORK

4.1 Problem Formulation

“The problem well defined, is the problem which is already half solved.”

For the scope of our thesis work that is to detect wormhole attack in wireless sensor network using distributed approach, the problem is stated. The problem that is formulated is based on the available literature on the wireless sensor networks and wormhole attack. The proposed and presented work by different authors help us to derive to a certain problem formulation. The problem is formulated by exploring to different domains for research.

The formulation of problem:

- **WHAT TO DO:** Detect the wormhole attack.
- **IN WHICH:** In wireless sensor networks.
- **HOW TO DO:** By using some distributed approach.

We took our base paper of Parmar Amish and V.B. Vaghela of “Detection and prevention of the wormhole attack in WSNs using AOMDV protocol”. In this paper authors use the methodology of time sequencing and round trip time. This approach is non-distributed in nature because only the initiator or source can detect the wormhole, this makes it centralized. But today’s network demand for a distributed approach.

In our proposed solution, we try to present a distributed approach by using cryptographic mechanisms. Our approach will presumes some conditions and act accordingly. There is use of special node called base station which will act as certifying authority to other nodes and check for any malicious activity. The use of these different base station make the approach distributed and help to correctly identify the wormhole nodes.

4.2 Objectives of the study

The major objective of this study is to propose a distributed approach to detect wormhole attack in wireless sensor networks. As we already know, the networks today cover almost all the geographical area in the world and plays vital role in any organization and even in non-organization. But the network is now not reliable, we need continuous improvement in currently established network infrastructure, for this purpose firstly we need to find an area where improvement can be done. Through this piece of work on wireless sensor networks and wormhole attack launched in it, we in here describes the need of security. The network is not secure, so the objective of this work, also is to provide a secure way to route the packets in network while tackling the adversary affecting the networks maliciously. The major objectives of any study to gather the results on the formulated problem as in problem formulation step of research methodology. Here for proposing an algorithm for our formulated problem we consider some prerequisites to be achieved in the end of study.

We can describe the objectives of this study as under:

a) **To propose a distributed approach:** The current state of network security model requires a distributed approach. Our objective will be to propose an approach which is distributed in nature.

b) **To simulate proposed work:** Once the work is proposed we need to see if it is better in results or not for this purpose simulation of proposed work is important and is our objective.

c) **To find wormhole attack in WSNs:** Our main goal for this study is to detect the wormhole in wireless sensor networks. For this we are presenting a distributed approach as per current requirement of network security model.

d) **To provide a better security approach:** All the studied approaches in this work lack in some aspects, our objective is to provide a better security approach than existing ones.

e) **To propose a novel approach:** The proposed work should be novel and should cover the solution of respective problem. We try to create a new approach to address our problem.

f) **To exploit state of art of wormhole in WSNs:** Wormhole attack is discussed in this piece of work for wireless sensor networks. In order to address an issue we need to know about the issue. This is also one of our objectives.

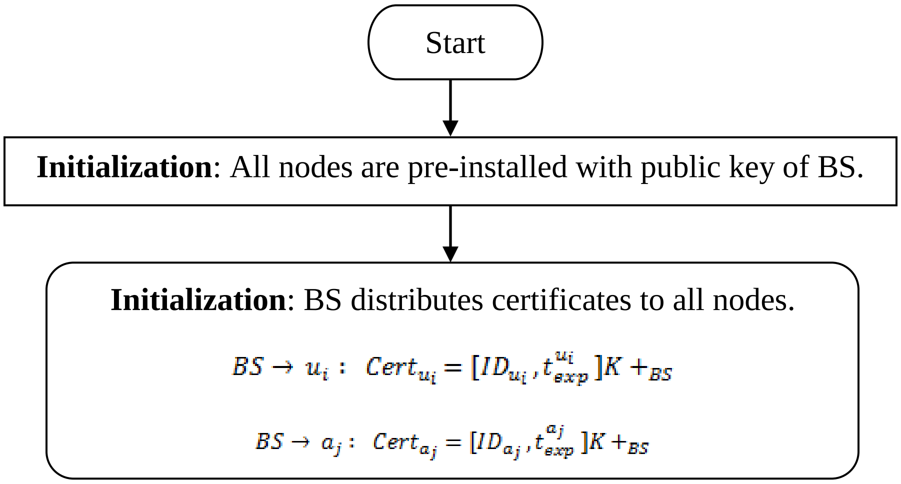
These are the objectives of our study and in some point, we already achieve the success, but still some research is needed to be done. We can look for other favorable objectives also to be achieved by our presented work.

4.3 Research Methodology

For any research to be conducted successfully, we need a well-designed methodology and step-wise hierarchy, which can be followed and help in concluding some results out of the research work.

In our proposed research work, a distributed approach is used. We make use of cryptography concepts of public and private cryptosystems. The concepts of clustering is also used by making base station as a most privileged nodes than other privileged and sensor node, which provide the communication between inter-cluster base stations in order to route the communication of simple sensor nodes and privileged nodes.

For our research work, we us the following flow of research methodology:


Start
Initialization: All nodes are pre-installed with public key of BS.
Initialization: BS distributes certificates to all nodes.
$BS \rightarrow u_i : \; Cert_{u_i} = [ID_{u_i}, t_{exp}^{u_i}]K +_{BS}$
$BS \rightarrow a_j : \; Cert_{a_j} = [ID_{a_j}, t_{exp}^{a_j}]K +_{BS}$

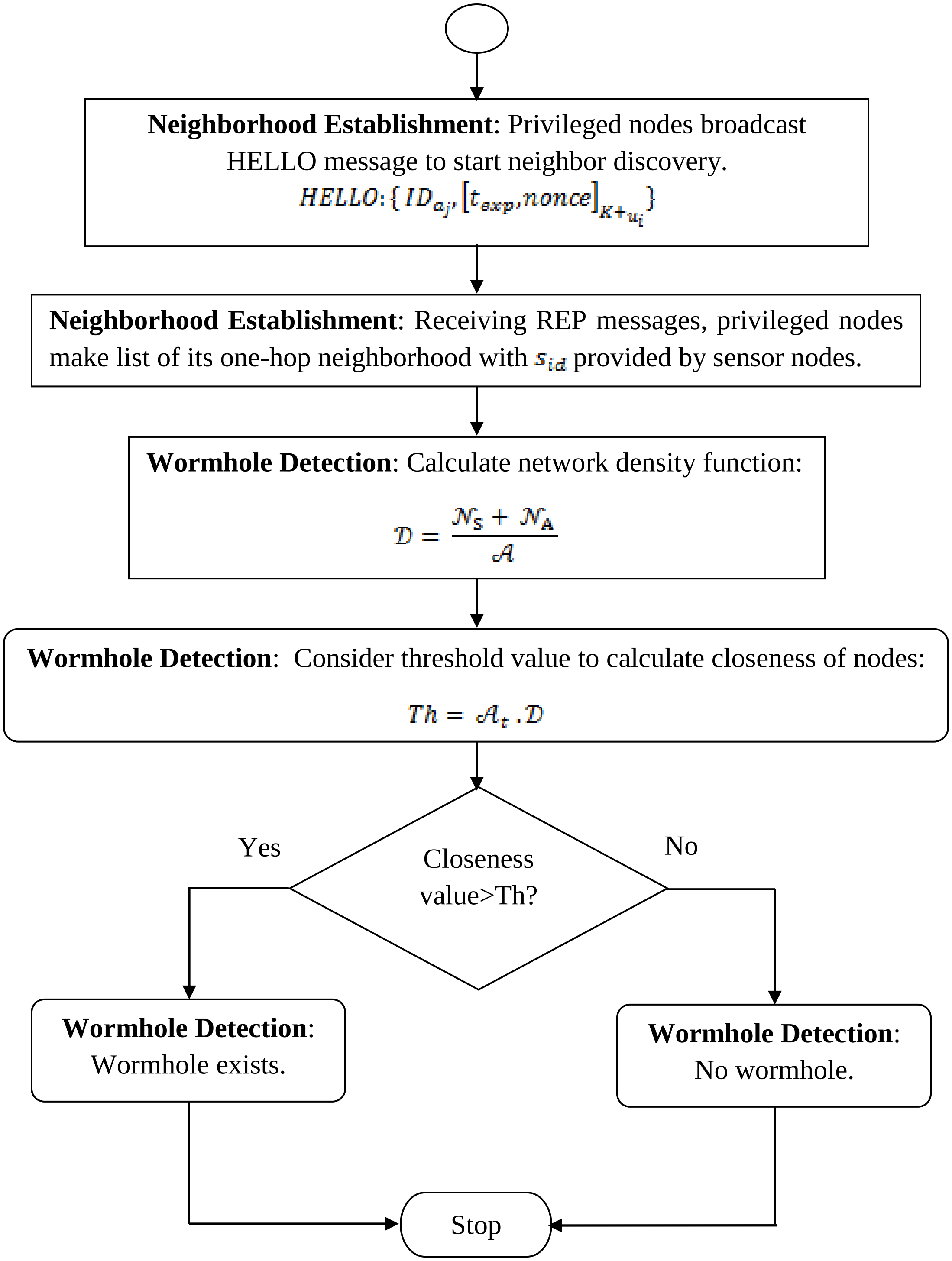

Neighborhood Establishment: Privileged nodes broadcast HELLO message to start neighbor discovery.
$HELLO:\{ID_{a_j}, [t_{exp}, nonce]_{K+u_i}\}$
Neighborhood Establishment: Receiving REP messages, privileged nodes make list of its one-hop neighborhood with s_{id} provided by sensor nodes.
Wormhole Detection: Calculate network density function:
$\mathcal{D} = \frac{\mathcal{N}_S + \mathcal{N}_A}{\mathcal{A}}$
Wormhole Detection: Consider threshold value to calculate closeness of nodes:
$Th = \mathcal{A}_t . \mathcal{D}$
Yes
Closeness value>Th?
No
Wormhole Detection: Wormhole exists.
Wormhole Detection: No wormhole.
Stop

Figure 4.1: Flowchart

4.3.1 Proposed Algorithm:

The algorithm starts with initialization phase followed by neighborhood discovery only with one hop neighbors and then the wormhole detection process is executed. The following assumptions are made for the proposed algorithm:

- Base Station (BS) is secure enough and also works as Certification Authority (CA).
- BS provides certificates and required keys (public or private) to all the sensor nodes and privileged nodes.
- Nodes are pre-deployed with keys and are known to BS.

The proposed algorithm consists of three phases as follows:

- **Phase I: Initialization**

  All the nodes are pre-installed with public keys of base station. Base station distributes the certificates to all the nodes, both privileged nodes and sensor nodes, as follows:

  $$BS \rightarrow u_i : \; Cert_{u_i} = [ID_{u_i}, t_{exp}^{u_i}]K +_{BS}$$

  $$BS \rightarrow a_j : \; Cert_{a_j} = [ID_{a_j}, t_{exp}^{a_j}]K +_{BS}$$

  The u$_i$ is for the sensor nodes and a_{id} is for privileged node.

- **Phase II: Neighborhood establishment**

  The privileged nodes broadcast a HELLO message to start the process of neighborhood discovery. The message is comprised of the following components:

  $$HELLO: \{ ID_{a_j}, [t_{exp}, nonce]_{K+u_i} \}$$

  Where, a_{id} is the ID of the privileged node, t_{exp} is the expiry time of the HELLO message, *[nonce]* is a random number encrypted with sensor node's public key.

Upon receiving the HELLO message, the one-hop neighbors reply with REP message consisting of its ID and time of expiry and nonce sent by the receiver encrypted with the public key of the sensor node.

$$REP: \{ ID_{u_i}, [t_{exp}, nonce]_{K+a_j} \}$$

Receiving the REP messages from the sensor nodes, each privileged nodes make a list of its one-hop neighborhood with the s_{id} provided by the sensor nodes. The s_{id} is the id of sensor nodes provided by them in the REP message. This list helps the privileged nodes to cluster the sensor nodes. For further communication, the sensor nodes willing to send data will send the message along with its certificate to the privileged node and privileged node will further provide privileged-to-privileged communication to transmit the message to a sensor node that does not belong to its own cluster.

Moreover, the cryptographic keys will help the network to avoid any maliciousness in between as data will be encrypted by the keys as necessary.

$$u_i \rightarrow a_j : \{[M]_{K-aj}, Cert_{u_i}\}$$

$$a_j \rightarrow a_{j+1} : \{[M]_{K-a_j}, Cert_{u_i}, Cert_{a_j}\}$$

$a_{j+1} \rightarrow a_{j+2} : \{[M]_{K-a_{j+1}}, Cert_{a_j}, Cert_{a_{j+1}}\}$ and so on.......

Privileged nodes acts like the cluster head of their clusters and provide inter-cluster communication in network for sensor nodes. Clustering shows the distributed nature and operation of the algorithm.

- **Phase III: Wormhole Detection**

Detection of wormhole will lead by calculating the density of network. Once the neighborhood discovery is completed, then algorithm checks for any wormhole existence. The total area of the network is indicated by: $\mathcal{A}$, the total number of sensor nodes in the network is represented by: $\mathcal{N}_S$ and total number of privileged nodes are considered as: $\mathcal{N}_A$. Therefore, the network density becomes as:

$$\mathcal{D} = \frac{\mathcal{N}_S + \mathcal{N}_A}{\mathcal{A}}$$

We have also considered a threshold (Th) value for the wormhole detection which will help to calculate the closeness of the nodes and calculated as:

$$Th = \mathcal{A}_t\,.\mathcal{D}$$

Where, $\mathcal{A}_t = 2\pi R^2 - 2(2\pi R^2.\frac{\alpha}{2\pi} - d.R.\sin\frac{\alpha}{2})$ shown in figure below with shaded region, which shows the area covered by threshold value. Where, $d = \frac{1}{2}\rho\sqrt{Th_c}$, $0 \leq \rho \leq 1$ defined as distance between the centres of two nodes A and B; and R is the average transmission range of the privileged nodes, d is the distance between privileged node and sensor node. Th_c is threshold value of closeness given as: $\frac{\mathcal{A}}{\mathcal{N}_S + \mathcal{N}_A}$.

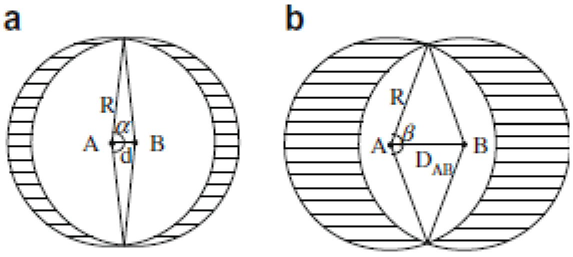


Figure 4.2: Wormhole Detection

If the value of closeness of nodes are greater than the threshold value for closeness of nodes, then there exists the wormhole nodes. Otherwise, no wormhole exists.

This is the proposed algorithm to detect the wormhole attack in wireless sensor networks using a distributed approach. The use of base station and operation in distributed manner makes it a distributed approach.

4.3.2 Tools used:

For gathering proves of our research work's effectiveness we use a simulation software, which is Network Simulator 2. We choose NS2 because of its high clarity of results and ability of simulating the networks very well. Also, it is very simple and easy to work in.

4.3.2.1 Introduction to NS2: NS2 targets the networking domain works, hence provide abilities to portray network requirements and working very well. NS2 provide simulation for TCP routing as well as for multicast protocols over infrastructure-less and infrastructure-oriented networks. The NS2 provide visualization of networks on NAM that is Network Animator. NS2 is Linux operating system based tool but can be used in windows using different available strategies.

- **4.3.2.1.1 Features of NS2:** NS2 has many features, some of these features of NS2 are as follows:

    1. Discrete event-simulator for research in networking domain.
    2. Simulate protocols with substantial support.
    3. Simulate the infrastructure-based and infrastructure-less networks.
    4. Uses two languages: C++ and OTCL.
    5. Use TCL for scripting.
    6. Open source and freeware.
    7. OTCL provide the object oriented support
    8. TCLCL provide C++ and OTCL linkage.

NS2 consists of 2 languages to lay its foundation that is C++ and Object-Oriented Tool Command Language. C++ defines all the internal functioning of objects for simulation, on other hand, OTCL develop simulation through object assembling and configurations with scheduling of discrete events. C++ and OTCL is linked with each other through TCLCL.

The reason for using 2 languages is that OTCL creates and configures network, and C++ runs simulation and do the compiling and linking so as to create executable files. OTCL is in use for configuration purpose fro simulation, setup the simulation, or for 1 time simulation and for running simulation with the existing modules of the NS2 library. It does not include complexity, but is very limited in functionality, hence cannot be a choice for researchers but only for new learners. C++ is used when we deal with packets or when we require to recreate or update existing module of NS2 library. Once the simulation is over/complete we are left with two files one is trace file and other is nam file. Nam file is for animation and trace file is for results. NS2 can be installed on windows using Cygwin. Cygwin provides Linux environment under windows. Or we can use a virtual platform to install NS2 like VMWARE and install Linux in it and then NS2.

- **4.3.2.1.2 Advantages of NS2:** There are certain advantages of NS2 over other software exists in market today and are the reason why to choose NS:

    1. NS2 is very cheap as compared to other software.
    2. In NS2, we can simulate and test even the complex scenarios very easily.
    3. The results can be obtained readily and with high reliability.
    4. As processing is fast more scenarios can be tested and simulated over a small time sequence.
    5. It provide support to almost every protocol and platform.
    6. NS2 also supports the concept of modularity through which it provide the ability of independence.
    7. NS2 is also very popular in market due to its high advantages than disadvantages.

These are some of the advantages of NS2 which let us decide to choose NS2 for our simulation purposes.

- **4.3.2.1.3 Disadvantages of NS2:** The NS2 also have some disadvantages with all the advantages, but are less in number than advantages, which also give a reason to prefer NS2 for our simulation purpose. These are as follows:

    1. The NS2 is very complex to model as the internal structure is very complicated.
    2. There might exists some bugs which will make it less reliable.
    3. It does not provide any interface or GUI to interact to, but for visualization of simulation it provides Network Animator.
    4. The documentation capabilities in NS2 is also not that good.

But these disadvantages are not that serious that will be a reason for not choosing NS2. These disadvantages can be overlooked without any serious penalties.

4.3.2.2 Introduction to VMWARE: It is Virtual Machine Ware which provide the power of virtualization. By virtualization we means to the ability of making a software-only schema of anything than a physical presence. The process of virtualization can be implemented for applications, servers, databases and network infrastructure so as to reduce the overall load and the expenses of IT in an industry and providing the high efficiency and agility all every business.

- **4.3.2.2.1 Properties of VMWARE:** the key features or characteristics of VMWARE are as follows:

    1. **Partitioning:** It means that we can run number of operating systems on a single physically present system with dividing different resources in between the created virtual machines which are present only in the logical context not physically.
    2. **Isolation:** This provide the ability of fault isolation and security isolation on the physical or hardware level and providing high level modernized

resource management to preserve the performance. This will also help in fault tolerance and security exploits/ threats.

3. **Encapsulation:** This property will provide the capability to save the current state into a form of files like other application interface provides and with the ability of moving and copying these saved files in the schema like other software application files. It provide independence from software point of view and provide mobility for saved files.

4. **Hardware Independence:** This means that it will give the service of migration of so as to migrate the virtual system between different physically existing system without any loss of integrity and reliability.

- **4.3.2.2.2 Benefits of VMWARE:** The VMWARE provides us with huge range of benefits with less of penalties. These benefits are:

1. It cut down on the operational costs of an organization's IT structure.

2. Reduce the downtime for high efficiency.

3. Boosting the productivity and interactive responses.

4. The resources and applications provisioned quickly.

5. Prove to be a great help in case if disaster recovery and for continuity in work.

6. The database is easy to manage and is simplified.

7. Create a true software centric database management.

We use the VMWare workstation for installing the Fedora Linux operating system in it in accordance to run the NS2 on windows platform. It provides us with the capability of letting us installing and running number of instances of same or different operating systems on a single physically present computer machine/system.

These tools took a great part in our research study, without these tools we would not be able to simulate our work and would not be able to come to conclusion about the effectiveness of our proposed algorithm.

NS2 provide us the base for all our simulations to implement and run on. VMware fives us the platform of installing Linux based operating system onto windows and also to install the NS2 in it. These tools help us through our research cases.

CHAPTER 5
RESULTS AND DISCUSSIONS

The results are obtained to check for the effectiveness of our approach. Following are the experimental results with possible discussion over it. Also a brief comparison is done with the existing scheme and new proposed scheme.

5.1 Experimental Results

For the collection of results and proves for effectiveness of our proposed approach, we use simulator called Network Simulator version 2, because of its high clarity of modeling networking concepts.

5.1.1 Simulation Parameters: For the simulation purpose we use some set of simulation parameters. These are:

- **Simulation area:** The area boundary in which the nodes are deployed and simulation is conducted. We use an area of 500 X 500.
- **Routing protocol:** The ZRP that is Zone Routing Protocol is used for routing the message between nodes for communication.
- **Number of nodes:** The total number of node deployed for running simulation are 8, a fairly small network of nodes.
- **Antenna model:** The antennas are used for sending and receiving signals. Weuse Omni antenna.
- **Interface queue type:** The queue for message receiving and sending in nodes are used as priority queues. High priority packets will be processed first than low priority.

- **Network interface type:** The interface used to connect to the network is Wireless Phy.

- **Radio propagation model:** The radio propagation used is two-ray ground model.

- **Channel type:** The channel is wireless for communication between nodes.

Simulation Area	500 X 500
Routing Protocol	ZRP
Number of nodes	8
Antenna Model	Omni Antenna
Interface Queue Type	Priority Queue
Network Interface Type	Wireless Phy
Radio Propagation Model	Two Ray Ground
Channel Type	Wireless Channel

Table 5.1: Simulation Parameters

5.1.2 Performance Parameters: We set three parameters to testify the efficacy of our proposed algorithm as these ra the most affected parameters under wormhole attack. These are:

- **Delay:** The delay will show the total delay encountered by the nodes under the wormhole attack in seconds. To find delay, we use formula:

  $D = P_d + Q_d + T_d$

  Where, P_d is processing delay that is time a node takes to process a packet, Q_d is the queuing delay that is the time a packet spent in the network queues and T_d is the transmission delay that is the time a packet take to transmit from source to destination.

- **Throughput:** The throughput refers to the maximum performance a node is capable of giving. The processing time without any faults are at a node will show its throughput. To show network throughput, we can take average of all node's throughput present in the network.

  T = number of processed packets/ latency for processing each packet

- **Packet loss ratio:** The packet loss ratio is the probability that how many packets get lost in the network under wormhole attack.

  PLR = number of packets lost / total number of packet received

5.1.3 Simulation Setup: For performing simulation we set up the simulation environment. In simulation environment we use an area of 500 X 500 and use ZRP protocol for routing decisions, as it will maintain the desired distributed nature of proposed scheme. We use three different radio ranges that is 5tr, 10tr and 15tr. The results are obtained based on these radio ranges and scenario under wormhole attack.

In results, the yellow wave will show the performance under wormhole existence. The red wave will show the performance at 15 tr, the green wave will show the performance at 10 tr and blue wave will show the performance at 5 tr.

5.1.4 Results: After simulation we are having our results in X-Graph on the three performance parameters that is delay, throughput and packet loss ratio.

- **Case I: Packet loss ratio**

  The packet loss ratio is high with low radio range and low with medium radio range. But no significant changes in results of high radio range and wormhole affected scenario.

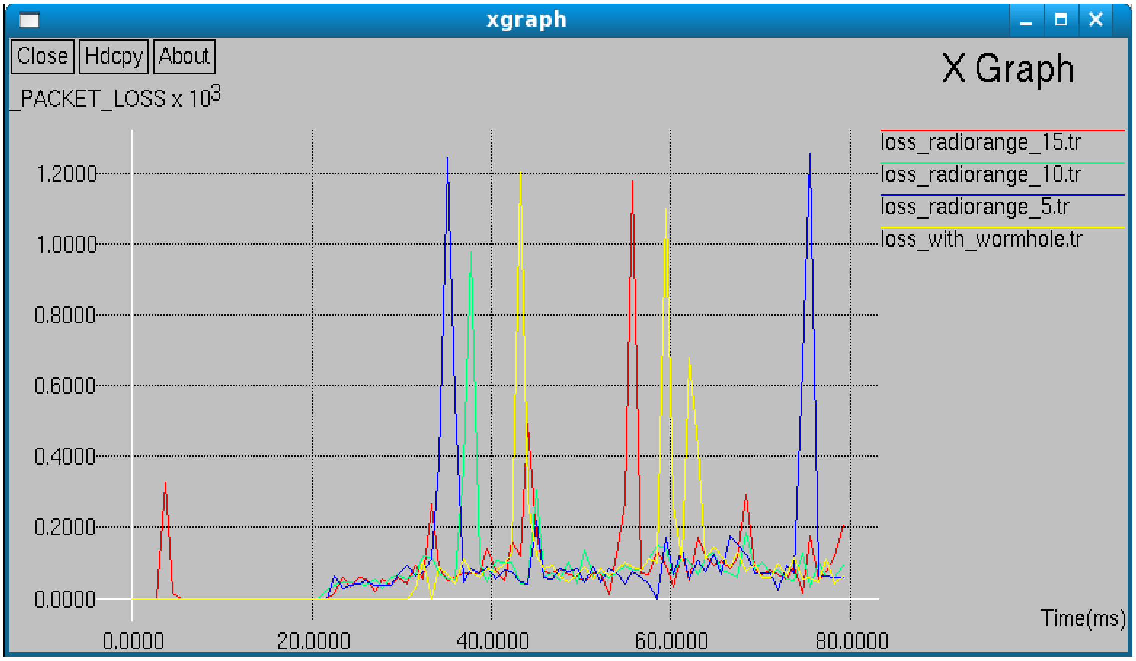


Figure 5.1: Packet loss ratio

- **Case II: Delay**

When the radio range is less or is 5tr then the delay is very high. Under wormhole attack the delay is almost equal to the delay at 5 tr. The delay for 10 tr shows quite less delay. The delay at 15 tr is also burdensome.

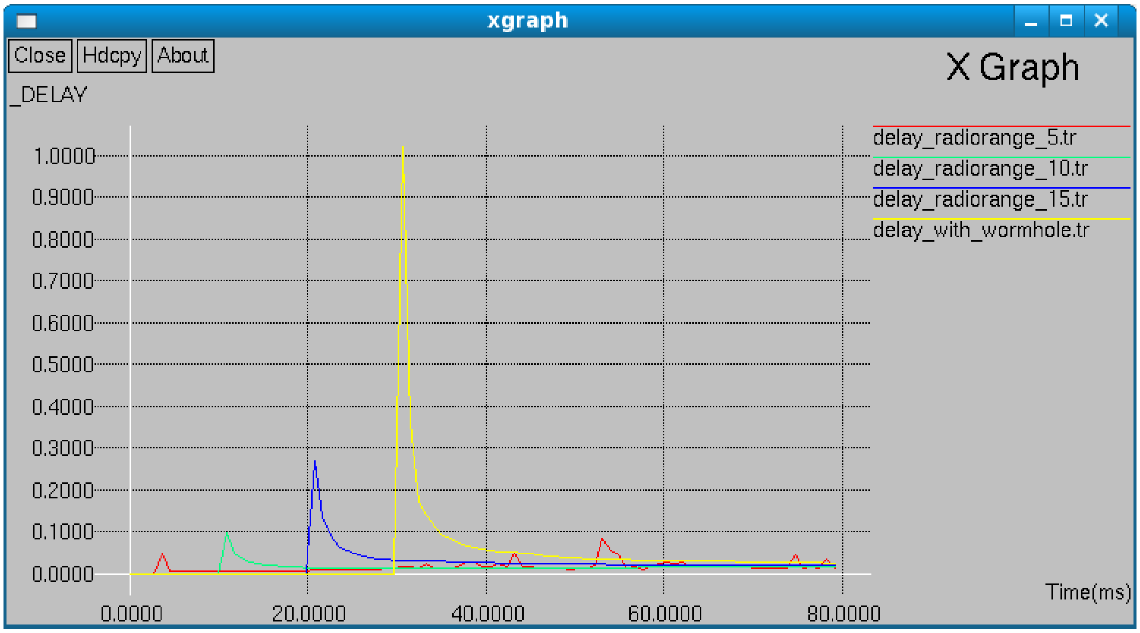


Figure 5.2: Delay

- **CASE III: Throughput**

  In case of high radio range throughput is high, then inline is medium radio range followed by low radio range and in wormhole the throughput affects the most.

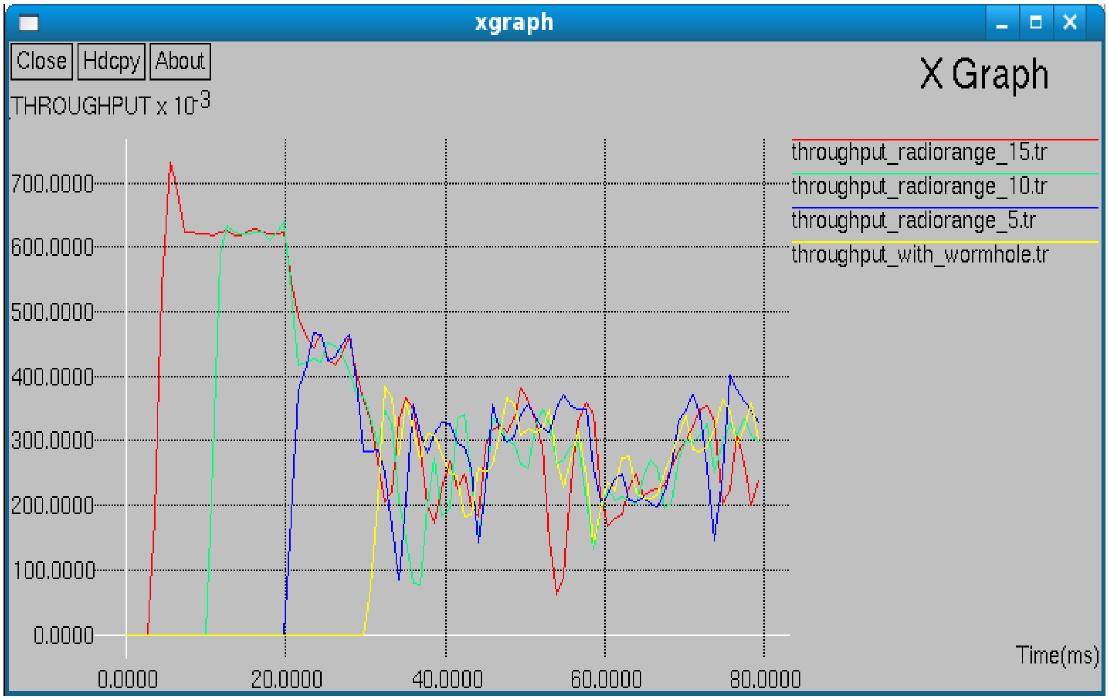


Figure 5: Throughput

So here are the obtained results for our proposed scheme. The delay in wormhole is large, the throughput affected badly and packet loss ratio obviously increased. These set of parameters will help us tell the wormhole existence in network.

5.2 Discussions

The proposed work produce better results than existing technique. The existing technique use time sequencing and round trip time, but in our approach we are using density as measuring function which introduces as a new approach. Our technique is novel as well as distributed. Many authors have worked time sequencing and round trip time management, but with the density very few work is present.

Our work can be correlated to existing technique in very few aspects. The routing is also happen in clustering, so a clustered routing algorithm must be used for best suitability, not some other protocols like AOMDV. But in our approach we use ZRP protocol to maintain the distributed nature of algorithm.

The major differences between our scheme and existing scheme is as follows:

- The use of cryptographic keys will help in attaining confidentiality, authentication and non-repudiation of the message transmission even if there is presence of the wormhole attack.
- The value for closeness function threshold will help in to calculating the whole probability for the very existence of a wormhole attack in the wireless sensor network.
- Message overhead is also less because the message length is kept as small as it can be.
- Base station are most privileged in comparison with privileged nodes and sensor nodes.
- Maximum tasks are performed by base station and privileged nodes to prolong the overall network lifetime.
- Make use of clustering technique for making it a distributed approach.
- Present a novel approach based on the density and closeness function of sensor nodes and privileged nodes.
- No special hardware or additional resources are required.

The proposed mechanism is stated under already presumed conditions or can say in a static network. But as most of the wireless sensor network present in static topology, so our approach will not be a big issue. But still we can use this algorithm to dynamic network topology for wireless sensor network and also can implement in other network structures than just only wireless sensor network. This could be the future scope of our study or proposed algorithm.

The authors in our base paper present a scheme based on timing of the messages sent and received, a slight mistake in calculation can pay for a big issue. But the computations are simple enough to run on any node of given network. Major issue in their work is that they present it as a centralized method but we are presenting distributed approach. The presented work by other authors take a stepping towards distributed approach. Some presented very good approaches, our approach can also be one of some approach.

As every work lack in some aspects, so as our also, but can be dealt with. The parameters for comparison in other technique are: throughput, delay and packet delivery fraction.

The previous scheme does not make use of cryptography but in our work we are presented the cryptography and cryptosystem that is public and private cryptosystem.

The previous scheme work well in dense network, but failed in dynamic network as the presented model in their work is stable and static. But there is scope to this limitation in our work.

The previous work is centralized but our method is distributed. In their approach, the source only can find the wormhole attack in network. But, in our approach the wormhole can be detected from any node.

For the wormhole to be found, we need to know the density of network nodes and closeness of theses nodes to each other. This is something novel which existing work does not have.

The base stations are declared as the most privileged nodes, but if the attacker ploy itself as base station then the sensor node might fall for the trap. But anyhow, in our assumed network the base station is most privileged nodes than other privileged node and sensor nodes.

Most of the computations involving in network is done by base station itself, so it helps sensor node to be free from all those bulky calculations and processing. Hence increasing the lifetime of the network.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

We already know about the widespan of the network covering every geographical region over the planet and beyond that. The security of the same is very important because of its awareness throughout the world. The attackers and malicious adversaries are always in high pace of attacking at communicating nodes in the network and exploits network properties. Due to these adversaries, the network is not reliable and not stable. To remove these adversaries from the network, one way is to defend them or other way is to prevent them from launching attacks in network. Both the methods are different in working. The defensive mechanism helps to defend from attacks once it is launched. But on the other hand, prevention mechanism helps to prevent from the attacks beforehand hence not making a chance of the attack being launched.

6.1 Conclusion

In the conclusion, we came to know that the proposed scheme or methodology is very effective in detecting the wormhole attack in wireless sensor networks. The proposed work follows a distributed approach as clustering is implemented. The schemes provide very less false positives and mostly truly find the real wormholes attack and not a false alarm. This scheme does not use any of the additional resources like highly synchronized clocks, location based hardware or software, high computational processors, etc. These are refrained to use in our proposed work. Also the processing of message packets involve little overhead. As the need of an hour for a distributed approach, our work fulfil the need. The cryptographic mechanism is used to prevent any malicious activity from wormhole attacker, for this, public and private cryptosystem concept is used. Our proposed algorithm provide the confidentiality, authenticity and non-repudiation of message transmission. The density function gives the base for detecting wormhole with some threshold value. Most of the work is performed by the base station as being the most privileged node from other nodes. Hence, enhancing the network lifetime as other nodes does not need to perform heavy and bulky calculations. Most of the presented work is using centralized approach, but in our work, we use a distributed approach. The results also show the upper-hand of our proposed algorithm on the already presented work. But still there is room for modification no matter how much we can achieve there will always be a space for further work.

6.2 Future Scope

As for the future scope, there is scope for modification as the proposed work is considered and implemented in the static and stable network, but for future work we can try to implement the same approach to dynamic networks. As the current network backbone demands for high mobility and dynamic routing, we can reach out to perform the implementation to dynamic and highly unstable network. We can also try to use other feature than density feature for detection of wormhole attack in wireless sensor networks.

REFERENCES

[1] C. Networks, “Wireless sensor network survey,” no. August 2008, 2014.

[2] M. Sowmya and K. Srinivas, “Literature Survey on Wireless Sensor Networks,” vol. 3, no. 6, pp. 1093–1095, 2014.

[3] D. Carman, P. Kruus, and B. Matt, “Constraints and approaches for distributed sensor network security (final),” *DARPA Proj. Rep.*, pp. 1–139, 2000.

[4] A. Bagula, “APPLICATIONS OF WIRELESS SENSOR NETWORKS Why Use WSNs □ Classification □ Sensor Usage □ WSN Applications □ Future,” no. February, pp. 1–67, 2012.

[5] M. Messai, “Classification of Attacks in Wireless Sensor Networks,” *Icta*, no. April 2014, pp. 23–24, 2014.

[6] P. Maidamwar and N. Chavhan, “A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network,” *Int. J. Ad hoc Netw. Syst.*, vol. 2, no. 4, pp. 37–50, 2012.

[7] S. Ughade, R. K. Kapoor, and A. Pandey, “An Overview on Wormhole Attack in Wireless Sensor Network : Challenges , Impacts , and Detection Approach,” vol. 2, no. 4, pp. 105–110, 2014.

[8] R. Singh, “COUNTERMEASURES AGAINST WORMHOLE ATTACK IN WIRELESS SENSOR NETWORKS : A,” vol. 6, no. May, pp. 79–84, 2016.

[9] N. Jain, S. Gupta, and P. Sinha, “Clustering Protocols in Wireless Sensor Networks: A Survey,” *Int. J. Appl. Inf. Syst.*, vol. 5, no. 2, pp. 41–50, 2013.

[10] P. Boora and S. Malik, “Performance Analysis of AODV , DSDV and ZRP Routing Protocols in WSN using Qualnet,” vol. 4, no. 6, pp. 557–565, 2015.

[11] S. Kaur and S. Kaur, “Analysis of Zone Routing Protocol in MANET,” *Int. J. Res. Eng. Technol.*, vol. 2, no. 9, pp. 520–524, 2013.

[12] S. Chang, I. Member, and I. C. Context, “A Fault Tolerance Spider-Net Zone Routing Protocol for Mobile Sinks Wireless Sensor Networks,” vol. 3, no. 4, 2013.

[13] G. Padmavathi, P. Subashini, and M. Aruna, “ZRP with WTLS Key Management Technique to Secure Transport and Network Layers in Mobile Adhoc Networks,” *Int. J.*, vol. 4, no. 1, pp. 129–138, 2012.

[14] P. Amish and V. B. Vaghela, “Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol,” *Procedia Comput. Sci.*, vol. 79, pp. 700–707, 2016.

[15] N. N. Dangare and R. S. Mangrulkar, “Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad hoc Network,” *Procedia Comput. Sci.*, vol. 78, pp. 342–349, 2016.

[16] W. Wang and B. Bhargava, “Visualization of wormholes in sensor networks,” pp. 51–60, 2004.

[17] G. Akilarasu and S. M. Shalinie, “Wormhole-Free Routing and DoS Attack Defense in Wireless Mesh Networks,” *Wirel. Networks*, pp. 1–10, 2016.

[18] Y. Xu, Y. Ouyang, Z. Le, J. Ford, and F. Makedon, “Analysis of Range-Free Anchor-Free Localization in a WSN under Wormhole Attack,” *Work*, pp. 344–351, 2007.

[19] R. Matam and S. Tripathy, “Open Access WRSR : wormhole-resistant secure routing for wireless mesh networks,” *EURASIP J. onWireless Commun. Netw.*, no. 180, pp. 1–12, 2013.

[20] S. Gupte and M. Singhal, “Secure routing in mobile wireless ad hoc networks,” *Ad Hoc Networks*, vol. 1, no. 1, pp. 151–174, 2003.

[21] S. Banerjee and K. Majumder, “A comparative study on wormhole attack

prevention schemes in mobile ad-hoc network," *Commun. Comput. Inf. Sci.*, vol. 335 CCIS, pp. 372–384, 2012.

[22] F. Shi, W. Liu, D. Jin, and J. Song, "A countermeasure against wormhole attacks in MANETs using analytical hierarchy process methodology," *Electron. Commer. Res.*, vol. 13, no. 3, pp. 329–345, 2013.

[23] T. Hayajneh, P. Krishnamurthy, D. Tipper, and A. Le, "Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies," *Mob. Networks Appl.*, vol. 17, no. 3, pp. 415–430, 2012.

[24] T. Dimitriou and A. Giannetsos, "Wormholes no more? Localized wormhole detection and prevention in wireless networks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6131 LNCS, pp. 334–347, 2010.

[25] X. Ban, R. Sarkar, and J. Gao, "Local connectivity tests to identify wormholes in wireless networks," *Proc. Twelfth ACM Int. Symp. Mob. Ad Hoc Netw. Comput.*, p. 13:1--13:11, 2011.

[26] Y. Ravikumar and S. Chittamuru, "A Case Study on MANET Routing Protocols Performance over TCP and HTTP," *Sch. Eng. Blekinge …*, no. June, 2010.

[27] L. Qian, N. Song, and X. Li, "Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach," *J. Netw. Comput. Appl.*, vol. 30, no. 1, pp. 308–330, 2007.

[28] S. Madria and J. Yin, "SeRWA: A secure routing protocol against wormhole attacks in sensor networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1051–1063, 2009.

[29] J. Kim, D. Sterne, R. Hardy, R. K. Thomas, and L. Tong, "Timing-based localization of in-band wormhole tunnels in MANETs," *WiSec*, p. 1, 2010.

[30] K. Krentz and G. Wunder, "6LoWPAN Security: Avoiding HiddenWormholes using Channel Reciprocity," *Proc. 4th Int. Work. Trust. Embed. Devices - Trust.*

’14, pp. 13–22, 2014.

[31] H. Liang, H. Fan, and F. Cai, “Defending against wormhole attack in OLSR,” *Geo-spatial Inf. Sci.*, vol. 9, no. 3, pp. 229–233, 2006.

[32] Y. Xu, G. Chen, J. Ford, and F. Makedon, “Chapter 19 DETECTING WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS,” vol. 253, pp. 267–279, 2008.

[33] C. Security, “Wormhole Attack in Wireless Sensor Network,” vol. 2, no. 1, pp. 22–26, 2014.

[34] Z. Tun and A. H. Maw, “Wormhole Attack Detection in Wireless Sensor Networks,” pp. 545–550, 2008.

[35] M. Nurul, A. Shaon, and K. Ferens, “Wormhole Attack Detection in Wireless Sensor Network using Discrete Wavelet Transform,” pp. 29–35.

[36] K. Patel and T. Manoranjitham, “Detection of Wormhole Attack In Wireless Sensor Network,” vol. 2, no. 5, pp. 366–369, 2013.