DETECTING AND DEFENDING WORMHOLE ATTACKS USING LOCALIZATION SCHEME IN WIRELESS SENSOR NETWORKS

A PROJECT REPORT

Submitted by

AJAY S

Register No: 14MCO002

in partial fulfillment for the requirement of award

of the degree of

MASTER OF ENGINEERING

in

COMMUNICATION SYSTEMS

Department of Electronics and Communication Engineering

KUMARAGURU COLLEGE OF TECHNOLOGY

(An autonomous institution affiliated to Anna University, Chennai)

COIMBATORE - 641 049

ANNA UNIVERSITY: CHENNAI 600 025

APRIL-2016

BONAFIDE CERTIFICATE

Certified that this project report titled **"DETECTING AND DEFENDING WORMHOLE ATTACKS USING LOCALIZATION SCHEME IN WIRELESS SENSOR NETWORKS"** is the bonafide work of **AJAY S [Reg. No. 14MCO002]** who carried out the research under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other project or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE

Ms. S.UMAMAHESWARI

ASSOCIATE PROFESSOR

Department of ECE

Kumaraguru College of Technology

Coimbatore-641 049

SIGNATURE

Dr. A.VASUKI

HEAD OF THE DEPARTMENT

Department of ECE

Kumaraguru College of Technology

Coimbatore-641 049

The Candidate with university **Register No. 14MCO002** was examined by us in the project viva –voice examination held on.....

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

First, I would like to express my praise and gratitude to the Lord, who has showered his grace and blessings enabling me to complete this project in an excellent manner.

I express my sincere thanks to the management of Kumaraguru College of Technology and Joint Correspondent **Shri Shankar Vanavarayar** for his kind support and for providing necessary facilities to carry out the work.

I would like to express my sincere thanks to our beloved Principal **Dr.R.S.Kumar Ph.D.,** Kumaraguru College of Technology, who encouraged me with his valuable thoughts.

I would like to thank **Dr.A.Vasuki Ph.D.,** Head of the Department, Electronics and Communication Engineering, for her kind support and for providing necessary facilities to carry out the project work.

In particular, I wish to thank with everlasting gratitude to the project coordinator **Dr.M.Alagumeenaakshi Ph.D.,** Asst. Professor(SRG), Department of Electronics and Communication Engineering, throughout the course of this project work.

I am greatly privileged to express my heartfelt thanks to my project guide **Ms.S.Umamaheswari M.E., (Ph.D.),** Associate Professor, Department of Electronics and Communication Engineering, for her expert counselling and guidance to make this project to a great deal of success and I wish to convey my deep sense of gratitude to all teaching and non-teaching staff of ECE Department for their help and cooperation.

Finally, I thank my parents and my family members for giving me the moral support and abundant blessings in all of my activities and my dear friends who helped me to endure my difficult times with their unfailing support and warm wishes.

ABSTRACT

Node localization becomes an important issue in the wireless sensor network as its wide applications in environment monitoring, emergency rescue and battlefield surveillance, etc. Basically, the DV-Hop localization scheme can work well with the assistance of beacon nodes that have the capability of self-positioning. The distance-vector propagation phase during the DV-Hop localization can even aggravate the positioning error, compared to the localization schemes without wormhole attacks. However, if the network is invaded by a wormhole attack, the attacker can tunnel the packets via the wormhole link to severely disrupt the DV-Hop localization process. In this paper, we focus on defending against the wormhole attack in the DV-Hop localization process, i.e., eliminating the impacts of the wormhole attack on the DV-Hop localization process. A wormhole resistant scheme for each node to determine their pseudo neighbours is introduced to forbid the communication link between them so as to achieve secure localization.Further, this work aims to improve the effectiveness of secure localization scheme in terms of packet delivery ratio, delay and throughput.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

WSN	Wireless Sensor Network
BPSK	Binary Phase Shift Keying
MEMS	Micro Electro Mechanical System
DV-Hop localization	Distance Vector Hop localization
WEP	Wired Equivalent Privacy
DoS	Denial of Service
TOA	Time of Arrival
TDOA	Time Difference of Arrival
AOA	Angle of Arrival
PDR	Packet Delivery Ratio
QoS	Quality of Service

CHAPTER 1

INTRODUCTION

1.1 Wireless Sensor Network

The objective of Wireless Sensor Network is to sense and collect data from a target domain, process the data, and transmit the information back to specific destination. WSNs are versatile and can be deployed to support a wide variety of applications. They are composed of using large number of wireless sensor nodes. These sensors are deployed depends on the nature of the application. Once deployed, sensor nodes self-organize themselves into an autonomous wireless network, which requires very little or no maintenance. It collaborates to carry out the specific application after deployment.

WSNs are based on emerging technologies such as wireless communication technologies, information technology, semiconductors, MEMS, micro systems technology and embedded micro-sensors. WSNs have the potential to revolutionize telecommunications in a way similar to what we call the internet of things by offering a wide range of different applications some of which remain to be discovered.

1.1.1 Sensor Node

The WSN is built of "nodes" - from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

A wireless sensor node is composed of four basic components: a sensing unit, a processing unit (microcontroller), a transceiver unit and a power unit. In addition to the above units, a wireless sensor node may include a number of application-specific components, for example a location detection system or mobiliser; for this reason, many commercial sensor node products include expansion slots and support serial wired communication.

Wireless Sensor Network Channels and Nodes

Network Channels: User nodes or gateways and onward transmission to other network.
Sensor Channels: Communicates among sensor nodes and targets.

Sensor Network has three types of Nodes. They are,

Sensor Nodes: Monitor immediate environment.
Target Nodes: Generates various stimuli for sensor nodes.
User Nodes: Client and Administration of Sensor Networks.

1.1.2 Deployment and Design Issue

WSNs are meant to be deployed in large numbers in various environments, including remote and hostile regions, where ad-hoc communications are a key component. For this reason, algorithms and protocols need to address the following issues:

- Lifetime maximization
- Robustness and fault tolerance
- Self-configuration

Deployment of a wireless sensor network is a critical issue because of the various characteristics of the sensing nodes:

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment Ability to withstand harsh environmental conditions
- Ease of use
- Power consumption

At the network layer, the intention is to find ways for energy efficient route setup and reliable relaying of data from the sensor nodes to the sink, in order to maximize the lifetime of the network. The major differences between the wireless sensor network and the traditional wireless network sensors are very sensitive to energy consumption. Moreover, the performance of the sensor network applications highly depends on the lifetime of the network.

1.2 Localization

The goal of localization is to determine the physical coordinates of a group of sensor nodes. These coordinates can be global, meaning they are aligned with some externally meaningful system like GPS, or relative, meaning that they are an arbitrary "rigid transformation" (rotation, reflection, translation) away from the global coordinate system. Beacon nodes (also frequently called anchor nodes) are a necessary prerequisite to localize a network in a global coordinate system. Beacon nodes are simply ordinary sensor nodes that know their global coordinates a priori. This knowledge could be hard coded, or acquired through some additional hardware like a GPS receiver. At a minimum, three non-collinear beacon nodes are required to define a global coordinate system in two dimensions. If three dimensional coordinates are required, then at least four non-coplanar beacons must be present. The advantage of using beacons is obvious: the presence of several pre-localized nodes can greatly simplify the task of assigning coordinates to ordinary nodes. However, beacon nodes have inherent disadvantages. GPS receivers are expensive. They also cannot typically be used indoors, and can also be confused by tall buildings or other environmental obstacles. GPS receivers also consume significant battery power, which can be a problem for power-constrained sensor nodes. The alternative to GPS is pre-programming nodes with their locations, which can be impractical (for instance when deploying 10,000 nodes with 500 beacons) or even impossible (for instance when deploying nodes from an aircraft).In short, beacons are necessary for localization, but their use does not come without cost.

1.3 Range-Based Localization Schemes

Time of Arrival (TOA) technology is commonly used as a means of obtaining range information via signal propagation time. The most basic localization system to use TOA techniques is GPS. These systems require expensive and energy-consuming electronics to precisely synchronize with a satellite's clock. With hardware limitations and the inherent energy constraints of sensor network devices, GPS and other TOA technology present a costly solution for localization in wireless sensor networks. The Time Difference of Arrival (TDOA) technique for ranging (estimating the distance between two communicating nodes) has been widely proposed as a necessary ingredient in localization solutions for wireless sensor networks. Like TOA technology, TDOA also relies on extensive hardware that is expensive and energy consuming, making it less suitable or low-power sensor network devices. In addition, TDOA techniques using ultrasound require dense deployment (numerous anchors distributed uniformly) as ultrasound signals usually only propagate 20-30 feet. To augment and complement TDOA and TOA technologies, an Angle of Arrival (AOA) technique has been proposed that allows nodes to estimate and map relative angles between neighbours. Similar to TOA and TDOA, AOA estimates require additional hardware too expensive to be used in large scale sensor networks.

1.4 Range-Free Localization Schemes

In sensor networks and other distributed systems, errors can often be masked through fault tolerance, redundancy, aggregation, or by other means. Depending on the behavior and requirements of protocols using location information, varying granularities of error may be appropriate from system to system. Acknowledging that the cost of hardware required by range-based solutions may be inappropriate in relation to the required location precision, researchers have sought alternate range-free solutions to the localization problem in sensor networks. In a heterogeneous network containing powerful nodes with established location information is considered. In this work, anchors beacon their position to neighbours that keep an account of all received beacons. Using this proximity information, a simple centroid model is applied to estimate the listening nodes' location. An alternate solution,

DV-HOP assumes a heterogeneous network consisting of sensing nodes and anchors. Instead of single hop broadcasts, anchors flood their location throughout the network maintaining a running hop-count at each node along the way. Nodes calculate their position based on the received anchor locations, the hop-count from the corresponding anchor, and the average-distance per hop; a value obtained through anchor communication. Like DV-Hop, an Amorphous Positioning algorithm uses offline hop-distance estimations, improving location estimates through neighbour information exchange.

1.5 Types of Routing Protocols

In order to maximize the lifetime of WSN, Energy Efficient Routing Protocols should be employed. Types of routing protocols are,

Node-Centric Routing: In WSNs, node centric communication is not a commonly expected communication type. Therefore, routing protocols designed for WSNs are more data-centric or geocentric.

Data-Centric, or Location-Aware Routing: In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute based naming is necessary to specify the properties of data. Here data is usually transmitted from every sensor node within the deployment region with significant redundancy. In location aware routing nodes know where they are in a geographical region. Location information can be used to improve the performance of routing and to provide new types of services.

QoS based Routing: In QoS based routing protocols data delivery ratio, latency and energy consumption are mainly considered. To get a good QoS (Quality of Service), the routing protocols must possess more data delivery ratio, less latency and less energy consumption.

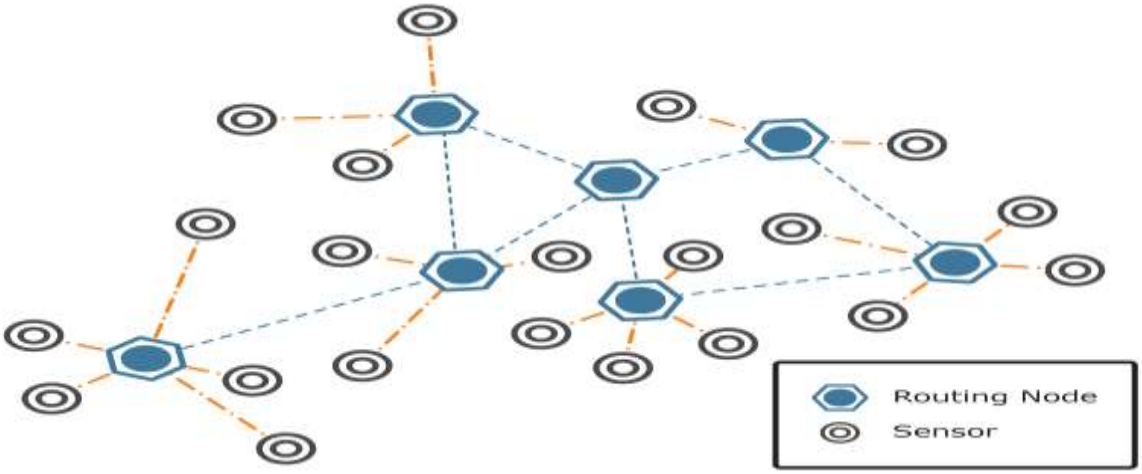

Figure.1.1 Node Deployment

1.6 Applications of WSN:

Wireless sensor networks have the potential to revolutionize telecommunications in a way similar to what we call the internet of things by offering a wide range of different applications some of which remain to be discovered. Sensor networks have a huge potential for applications in various fields, including:

- Environment and health: ocean temperature, collecting information on patients' conditions
- Management of critical industrial areas: monitoring of oil containers, checking the concentration of chemicals and gases
- Warehouse management and supply chain monitoring and historical states of the goods with the conditions of critical conservation
- Military applications: surveillance and recognition.

CHAPTER 2
LITERATURE REVIEW

Zhiwei Li,DiPu, Weichao Wang, Alex Wyglinski (2011) Previous research on security of network coding focused on the protection of data dissemination procedures and the detection of malicious activities such as pollution attacks. The capabilities of network coding to detect other attacks have not been fully explored. In this paper, we propose a new mechanism based on physical layer network coding to detect wormhole attacks. When two signal sequences collide at the receiver, the starting point of the collision is determined by the distances between the receiver and the senders. Therefore, by comparing the starting points of the collisions at two receivers, we can estimate the distance between them and detect fake neighbour connections via wormholes. While the basic idea is clear, we have proposed several schemes at both physical and network layers to transform the idea into a practical approach. Simulations using BPSK modulation at the physical layer show that the wireless nodes can effectively detect fake neighbour connections without the adoption of special hardware or time synchronization.

Guiyi Wei, Xueli Wang and Yuxin Mao (2010) With the emergence of wireless sensor networks in military surveillance, environmental monitoring and other fields, security has become an important issue. Wormhole attack can destabilize or disable a wireless sensor network. Intypical wormhole attack, the attacker receives packets in the network, forward them through a wired or wireless link with high-bandwidth low-latency links than the network links, relay them to another point in the network. In this paper, we propose to use the key techniques and probabilistic multi-path redundancy transmission (PMRT) to detect wormhole attacks. Id-based key management scheme is used for wireless sensor networks to build security link and detect wormhole attack. Compared with existing methods, the proposed approach not only reduces the communication overhead, but also saves node energy.

Fan-rui KONG,Chun-wen LI, Qing-qing Ding, Guang-zhao CUI, Bing-yi CUI (2009) As the applications of wireless sensor networks (WSNs) diversify, providing secure communication is emerging as a critical requirement. In this paper, we investigate the detection of wormhole attack, a serious security issue for WSNs. Wormhole attack is difficult to detect and prevent, as it can work without compromising sensor nodes or breaching the encryption key. We present a wormhole attack detection approach based on the probability distribution of the neighbouring-node-number, WAPN, which helps the sensor nodes to judge distributively whether a wormhole attack is taking place and whether they are in the influencing area of the attack. WAPN can be easily implemented in resource-constrained WSNs without any additional requirements, such as node localization, tight synchronization, or directional antennas. WAPN uses the neighbouring-node-number as the judging criterion, since a wormhole usually results in a significant increase of the neighbouring-node-number due to the extra attacking link. We model the distribution of the neighbouring-node-number in the form of a Bernoulli distribution. Then the model is simplified to meet the sensor nodes' constraints in computing and memory capacity. Finally, we propose a simple method to obtain the threshold number, which is used to detect the existence of a wormhole. Simulation results show that WAPN is effective under the conditions of different network topologies and wormhole parameters.

Hao-Ting Pai, Fan Wu A number of studies have made progress towards satisfying the vital security requirements of mobile commerce, including identifying and resolving most of the possible flaws. However, recent studies have asserted that a particular attack, called the wormhole attack, can seriously impair the routing protocol. This vulnerability exists in a wireless system and may also exist in ad hoc commerce systems. Although many attempts have been made to confront wormhole attacks in the field of wireless communications, the available solutions are still inadequate and need to be improved. For example, Ariadne-based methods have been confronted with the new insider attacks, but to date the vulnerability has not been fixed. Moreover, those

solutions are not tailor-made for a mobile commerce environment. This paper identifies a possible new threat from wormhole attacks in an ad hoc mobile commerce environment and proposes an approach for handling this type of attacks in a way that is not impacted by the new problems facing Ariadne and endairA. Based on cryptographic theory, the proposed method that we discuss can nullify wormhole attacks coming from both the outside involving non-authorized and non-authenticated identities, and the inside for authorized and authenticated identities. The main features of our solution are: in the routing request process, heavy computation can be parallelized among powerful servers; and in the routing reply process, not every source node decrypts all the ciphertext transmitted by intermediate nodes and not every intermediate node needs to execute cryptographic computations. Through theoretical analysis, our approach is shown to be suitable for the mobile commerce environment, and more efficient and robust than Ariadne.

Nabila Labraoui and Mourad Gueroui (2011) Localization in wireless sensor networks (WSNs) has drawn growing attention from the researchers and a number of localization schemes have been proposed to discover the locations of regular sensors based on a few beacon nodes, which are assumed to know their locations through GPS or manual configuration. However, the localization process is vulnerable to malicious attacks aimed at interrupting the functionality of location-aware applications. The wormhole attack is a particularly challenging one since the external adversary which acts in passive mode, does not need to compromise any nodes or have access to any cryptographic keys. In this paper, wormhole attack in DV-hop is discussed, and a Wormhole-free DV-hop Localization scheme (WFDV) is proposed to defend wormhole attack in proactive countermeasure. Using analysis and simulation, we show that our solution is effective in detecting and defending against wormhole attacks with a high detection rate.

Shiyu Ji, Tingting Chen, Sheng Zhong (2013) Network coding has been shown to be an effective approach to improve the wireless system performance. However, many security issues impede its wide deployment in practice.Besides the well-studied pollution attacks, there is another severe threat, that of wormhole attacks, which undermines the performance gain of network coding. Since the underlying characteristics of network coding systems are distinctly different from traditional wireless networks, the impact of wormhole attacks and countermeasures are generally unknown. In this paper, we quantify wormholes' devastating harmful impact on network coding system performance through experiments. We first propose a centralized algorithm to detect wormholes and show its correctness rigorously. For the distributed wireless network, we propose DAWN, a Distributed detection Algorithm against Wormhole in wireless Network coding systems, by exploring the change of the flow directions of the innovative packets caused by wormholes. We rigorously prove that DAWN guarantees a good lower bound of successful detection rate. We perform analysis on the resistance of DAWN against collusion attacks. We find that the robustness depends on the node density in the network, and prove a necessary condition to achieve collusion-resistance. DAWN does not rely on any location information, global synchronization assumptions or special hardware/middleware. It is only based on the local information that can be obtained from regular network coding protocols, and thus the overhead of our algorithms is tolerable. Extensive experimental results have verified the effectiveness and the efficiency of DAWN.

CHAPTER 3

METHODOLOGY

3.1 Attacks on Wireless Sensor Networks

As the use of wireless sensor networks becomes increasingly more common, especially in data-sensitive environments, routing security is emerging as a primary concern. Many sensor networks have proposed sensor network routing protocols but few consider or implement security goals.

We, the authors, researched the uses of wireless sensor networks last semester and our research focused on their use in Mass Causality Events (MCE). In these events, motes are attached to a patient's wrist and are tasked with transmitting vital information about the patient's condition, medical history, and personal data to emergency personnel. The transmitting of personal data over wireless communication became an

Many protocols are currently insecure and can become secure simply by incorporating existing security mechanisms into their design. With the assertion that wireless sensor network protocols must be proposed with security as a priority to achieve secure routing, this describes an effective solution.

This document presents the background of the existing problem in wireless sensor networks coupled with what is required for secure routing protocols. Additionally, it presents various attacks and security analysis on current protocol designs as well as countermeasures and security services available to defend those attacks.

Wireless sensor networks are very susceptible to attacks due to the nature and simplicity of their protocol design. Most of the network layer attacks against sensor networks fall into one of the following categories described below.

3.2 Altered routing information

The first of the five types of attacks is altered routing information, the most common attack on sensor networks. This attack on the routing protocol targets the routing information exchanged between two nodes and is the most direct of all five of the attacks. Intruders are able to lengthen or shorten source routes, create routing loops, repel and/or attract network traffic, or generate false error messages by altering routing information.

3.3 Selective Forwarding

An essential function of a multi-hop network is that the member nodes forward and receive messages. An intruder initiates a selective forwarding attack by inserting malicious nodes into the network. These nodes will refuse to send or will drop certain messages. This type of attack has two extremes; a node can act like a black-hole and drop every received packet or a node can selectively drop and forward packets as controlled by the intruder[3]. The former is much more obvious and more easily be detected by both the other nodes and the network administrator. The later is much less obvious and is more effective.

These mechanics of the selective forwarding attack can be tricky, potentially impossible. This technique is considered more effective when the intruder is included in the path of data flow.

3.4 Sinkhole Attacks

Sinkholes are a multifunctional attack. Not only can they be a standalone attack but they can cause a domino effect and initiate other types of attacks as well. Sensor networks are especially susceptible to these attacks due to the configuration of their communication patterns.

In a standalone sinkhole attack, adversaries try to lure nearly all the traffic from an area in the network through a centralized node which they have compromised. These attacks tend to work because the compromised node makes itself look like an attractive path through the routing algorithm. They do this by processing a high

quality route and use as much power as they can to transmit the data from the node to the base station in one hop. Thus, it is likely that all other nodes will transmit there data destined for the base station through the adversary.

Mounting a sinkhole attack makes selective forwarding trivial. The compromised node, if operating accordingly, will have control of all data headed for the base station. It can then selectively suppress or modify packets that came from any node in the area.

3.5 The Sybil Attack

The Sybil attack is most effective in geographic routing protocols. Such protocols often process communication between nodes by passing a pair of coordinates to their neighbours. Essentially, with the Sybil attack a node adversary can "be in more than one place at once."

3.6 Wormholes

The underlying purpose of a wormhole is to replay messages in a network. An adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. Packets transmitted via the wormhole have a lower latency than those traveling between those same nodes over the normal network. Wormholes have a conniving way about them. They have the ability to convince those nodes located multi-hops away from a base station that they are only a single hop away if they go through the wormhole. Again, this can cause a domino effect of attacks. If there is a sinkhole on the other side of the wormhole, nodes will send packets directly through the wormhole to the sinkhole for the most direct one hop route to the base station, tricky.

3.7 Authentication Broadcasts

One of the most important requirements for a secure network protocol was for the base stations to be trustworthy. It is assumed that they are and thus the concern is that adversaries mustn't be able to spoof broadcasts of flooded messages from any of those base stations.

Authenticated broadcasts are useful for localized node interactions. This would require nodes in the protocol to broadcast a HELLO message to announce themselves to their neighbours. These HELLO messages must be authenticated and spoof proof.

A proposed protocol is one that uses only symmetric key cryptography and requires minimal packet overhead. It achieves the asymmetry necessary for authenticated broadcast and flooding by using delayed key disclosure and one-way key chains. Replay is thus prevented because messages authenticated with previously disclosed keys are ignored.

Table 3.1 Security attacks on each Layer of the Internet Model

Layer	Attacks
Application Layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding,resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

3.8 Wormhole attack model and its impacts on DV-Hop localization:

We consider a hostile environment where the DV-Hop localization procedure of sensors may be disrupted by wormhole attack. In the wormhole attack, one attacker sniffs packets at one point of the network, tunnels them via the wormhole link to the other attacker which locates at the other point of the network, then the attacker broadcasts the received packets to its neighbours. We assume that the wormhole link is bi-directional and symmetrical so that the packets could be transmitted via either direction. The communication between each pair of colluding wormhole attackers is not

limited to R since they can communicate with each other using certain communication technique, i.e., the wormhole link, which may be implemented with wired communication. Considering that if the length of the wormhole link is less than R, both attackers are within each other's transmission range such that the packets transmitted by one attacker can be received and retransmitted by the other attacker, resulting in endless packet transmission loop. To exclude this exceptional case, we simply assume that the length of the wormhole link is larger than R, in which case, two colluding wormhole attackers can still communicate with each other via the wormhole link.

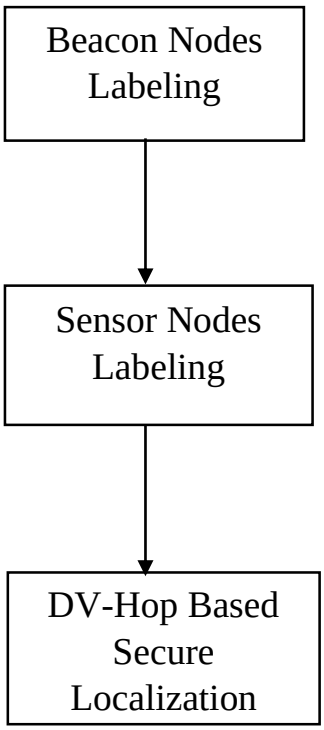

Figure 3.2. The flowchart of the label-based DV-Hop secure localization scheme

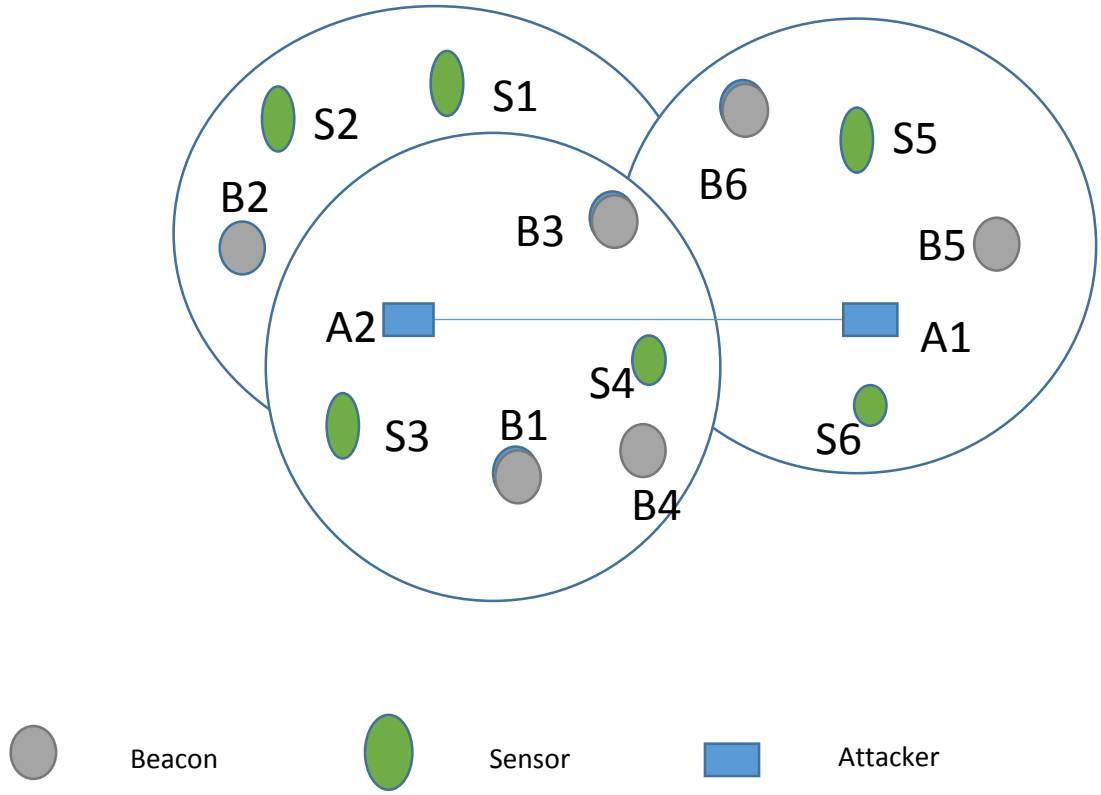

Figure 3.3. The wormhole attack in a WSN

3.8.1 Beacon nodes labelling

Before localization, all nodes in the network, including both beacons and sensors, periodically broadcast Hello messages to its neighbours, then each node can build a neighbour list after receiving the Hello messages from its neighbours. The Hello message includes the node's type (i.e., beacon or sensor), ID, and coordinate if it is a beacon. When building the neighbour lists, the beacon nodes may detect some abnormalities caused by the wormhole attack. By analysing these abnormalities, the beacon nodes can be classified and labelled into three categories: under the duplex wormhole attack, under the simplex wormhole attack, and without the wormhole attack. As shown in Figure. 3.3, beacon nodes in DR(A1) ∩ DR(A2), i.e., B3, are under the duplex wormhole attack, beacon nodes in DR(A1) \ DR(A2) and DR(A2) \ DR(A1), i.e., B1, B2, B4, B5 and B6, are under the simplex wormhole attack, and beacon nodes

outside DR(A1) ∪ DR(A2) are without the wormhole attack. The classification of the beacon nodes can be based on the following three properties:

3.8.1.1 Self-exclusion property: A node normally cannot receive a message sent from itself in a loop-free path. For each beacon node under the duplex wormhole attack (i.e., B3 as shown in Figure. 2), the Hello message it sends will be relayed by attacker A1 via wormhole link to attacker A2 and then received by itself; similarly, the Hello message will also be transmitted from A2 to A1 via wormhole link and then received by itself. However, without the wormhole attack, a node cannot receive a message sent from itself. Therefore, the beacons under the duplex wormhole attack can be identified using the self-exclusion property.

Beacon labelling scheme BL1: Every beacon node checks whether it violates the self-exclusion property when building
its neighbour list. The beacon node which violates the self-exclusion property can determine that it is under the duplex
wormhole attack.

3.8.1.2 Packet uniqueness property: A node normally cannot receive more than one copy of the same message from any of its neighbours.

As shown in Figure. 3.3, beacon node B4 lies in the common transmission region of attacker A1 and beacon B1, i.e., DR(A1) ∩ DR(B1). B1 can receive Hello message from B4 twice: one directly from B2 and the other from A2 (B4 → A1 →A2 → B1). Thus, if a beacon node receives the same message more than once from a neighbouring node, it is under a wormhole attack.

Beacon labelling scheme BL2: Every beacon node checks whether it violates the packet uniqueness property. If it does, i.e., it receives more than one copy of the same message from one of its neighbours, it can determine that it is under a wormhole attack (either a duplex or simplex wormhole attack).

3.8.1.3 Transmission constraint property: A node normally cannot communicate with nodes outside its transmission range.

As shown in Figure. 3.3, beacon node B5 lies outside the transmission region of beacon node B1. However, the Hello message transmitted by B5 can be received by attacker A1, after that A1 will relay it through the wormhole link to A2 which will further relay it to B1. When receiving the Hello message from B5, B1 can calculate the distance between them as the coordinate of B5 is included in the Hello message. B1 can observe that it receives a message from a node which is outside its transmission range. Thus, it can determine that it is under a wormhole attack.

Beacon labelling scheme BL3: Every beacon node checks whether it violates the transmission constraint property when building its neighbour list. If the transmission constraint property is broken, it determines that it is under a wormhole attack.

3.8.2 Sensor nodes labelling

In the previous section, we have just labelled the beacon nodes in the network with D, S1, S2 or N. This is not adequate for the localization procedure to defend against the wormhole attack. Therefore, we will further label the sensor nodes in the network. Similar to the beacon nodes, if sensor nodes lie in region DR(A1)∪DR(A2) (as shown in Figure. 3.3), they are attacked by the wormhole attack; if sensors lie outside the above region, they are not attacked by the wormhole attack. Each attacked beacon node broadcasts an Alert message if it is being labelled with S1, S2 or D. The Alert message includes its label, the attacked beacon set and its members' labels. For each beacon node with a label D, its attacked beacon set will include all the beacons in region DR(A1) ∪ DR(A2). Initially, each sensor node will label itself with N. After receiving an Alert message from any of its neighbouring beacons, the sensor node can then relabel itself with U to indicate that the sensor node's self-localization may be affected by the wormhole attack and its final label is still uncertain. For each sensor node labelled with U, it will further conduct the following labelling schemes. Similar to the beacon labelling scheme BL1, sensor labelling scheme SL1 is used to detect the duplex wormhole attack.

Sensor labelling scheme SL1: Each sensor node labelled with U checks whether it violates the self-exclusion property. If yes, it determines that it is under the duplex wormhole attack. The sensor node will mark itself with label D. Sensor nodes can use the following schemes to label themselves if they are under the simplex wormhole attack.

Sensor labelling scheme SL2: For a sensor node labelled with U but not D, if it receives two copies of the same message from its neighbouring node, it can conclude that it is under the simplex wormhole attack and label itself with S.

Sensor labelling scheme SL3: For a sensor node labelled with U but not D, if it receives messages from two beacon nodes, it can calculate the distance between these two beacon nodes since their coordinates can be obtained from the messages. If the distance is larger than 2R, the sensor node can conclude that it is under the simplex wormhole attack and label itself with S. If the sensor is not under the wormhole attack, it can use the next sensor labeling scheme to determine its label.

3.8.3 Wormhole attack detection schemes

The wormhole attack detection schemes and the wormhole attack resistant localization schemes are discussed.

Wormhole attack detection schemes: The packet leashes mechanism uses geographical and temporal to detect whether or not the packets are attacked by wormhole attacks. Wang and Bhargava proposed a scheme to detect the wormhole by visualizing the anamolies introduced by the attack which needs all the distance messages between each pair of nodes. A wormhole attack detection mechanism is proposed which uses geographic information to detect anamolies in neighbour relations and node movements.

Wormhole attack resistant localization schemes: As the localization process is greatly affected by the wormhole attack, some secure localization approaches have been proposed. The schemes can be applied into the localization against wormhole attacks, but it does not suit for the scenario when large percentage of locators are attacked. Inter-node messaging properties are used to detect the abnormality of the network when the

wormhole attack exists. A so-called conflicting set is built to detect the wormhole attack and to further resist against the impact of the attack on the localization.

In this section, we will describe the network model, localization approach, attack model and then analyse the impacts on the localization process.

Network model

We assume that there are three types of nodes in a wireless sensor network : beacons (or anchors),sensors and attackers. Beacons are location-fixed nodes with their positions known in advance (by GPS device or manual configuration) they will keep stationary after deployment. The sensors, either moving around or staying at a place, are position-unknown nodes that need to locate with assistance of beacons. The system can conduct the localization procedure periodically for the sensor nodes to update their current locations since they may be mobile.

DV-Hop localization approach

In the first phase, a typical distance vector routing mechanism is employed: each beacon initiates a flooding, which includes location information, ID and the hop-count of 1, throughout the network; each node that relays the flooding message will increase the hop-count by one and add its own ID onto the flooding message as the sender; after the flooding procedure, every node can obtain the minimum hop-count to each of the beacons. ID and the hop-count of 1, throughout the network; each node that relays the flooding message will increase the hop-count by one and add its own ID onto the flooding message as the sender; after the flooding procedure, every node can obtain the minimum hop-count to each of the beacons.

In the second phase, each beacon, after obtaining the position and hop-count information to all the other beacons, estimates the average distance per hop in the network.

In the last phase, each sensor can estimate its distance to each beacon based on its hop-count to this beacon and the average hop-size. For example, sensor k can estimate the distance d_{kj} (the distance from sensor k to beacon j) using $d_{kj} = h_j \times HS_j$.

After obtaining the distance information to all the beacons, each sensor can conduct the triangulation or maximum likelihood estimation scheme to estimate its own location.

Wormhole attack model

We consider a hostile environment where the DV-Hop localization procedure of sensors may be disrupted by wormhole attack. In the wormhole attack, one attacker sniffs packets at one point of the network, tunnels them via the wormhole link to the other attacker which locates at the other point of the network, then the attacker broadcasts the received packets to its neighbours. We assume that the wormhole link is bi-directional and symmetrical so that the packets could be transmitted via either direction. The communication between each pair of colluding wormhole attackers is not limited to R since they can communicate with each other using certain communication technique, i.e., the wormhole link, which may be implemented with wired communication. Considering that if the length of the wormhole link is less than R, both attackers are within each other's transmission range such that the packets transmitted by one attacker can be received and retransmitted by the other attacker, resulting in endless packet transmission loop. To exclude this exceptional case, we simply assume that the length of the wormhole link is larger than R, in which case, two colluding wormhole attackers can still communicate with each other via the wormhole link.

All nodes are deployed randomly and are stationary. Our proposed technique uses two prover nodes and a verifier node. Prover node collects the information about the location of neighbour nodes and delivers it to the verifier node. It then evaluates each node independently to idendify wormhole attackers.,i.e if the node at a particular location acts in other end location of the network. If the malicious nodes are found, the verifier node will inform the prover nodes about the attacker nodes and immediately those wormhole links are removed from the network.

Let Ps denote the theoretical probability that beacon nodes successfully detect the wormhole attack, while Pf denotes the probability that the beacon nodes fail to detect the wormhole attack. Hence we have: $P_s = 1 - P_f$ .The wormhole attack cannot be

detected only under the following two scenarios: (1) there is no beacon node in D_R (A1); and (2) there is no beacon node in D_R(A2).

As the beacon nodes are randomly deployed in the network with density ρ_b, the probability that there is no beacon node in D_R (A1) is $P(A) = e^{-\rho b D_R(A1)}$. Similarly, the probability that there is no beacon node in D_R (A2) is $P(B) = e^{-\rho b D_R(A2)}$. Thus, we can get:

$$Pf = P(A \cup B) = P(A) + P(B) - P(AB)$$
$$= 2e^{-\rho b \pi R2} - e^{-\rho_b D_R(A1) \cap D_R(A2)}. \quad (3.1)$$

Therefore, the probability of the wormhole attack detection is:

$$Ps = 1 - P_f$$
$$= 1 - 2e^{-\rho_b \pi R2} + e^{-\rho_b D_R(A1) \cap D_R(A2)} \quad (3.2)$$

3.8.4 WSNs with a static sink

In the early days, a typical WSN was composed of static sensor nodes and a static sink placed inside the observed region. In such a setup, the major energy consumer is the communication module of each node. In practice, multi-hop communication is required for sending data from sources to sink nodes. Consequently, the energy consumption depends on the communication distance. One way to reduce the communication distance is to deploy multiple static sinks and to program each sensor node such that it routes data to the closest sink. This reduces the average path length from source to sink and hence results in smaller E_{bar} compared to the case of single static sink. On the other hand, reduction in E_{max} is also observed because routing load on the nodes located in the vicinity of a single sink also gets distributed among all the nodes located in the vicinity of multiple static sinks. These static sinks partition the WSN into small sub-fields each with one static sink. By simulation it was shown that the proposed scheme leads to energy efficiency and better data delivery ratio compared to schemes based on a single sink. However, a major problem with multiple static sinks is that one has to decide where to deploy them inside the monitored region so that the data relaying load can be balanced amongst the nodes. This problem is considered as an

instance of the well-known ‘‘facility location problem’’ where for a given number of facilities and customers the optimal position for the placement of the facilities has to be identified so that all facilities are evenly burdened. If the positions of the static sinks are given, then the solution of this problem can be used for finding the optimal partitioning of the field. However, even if we assume location-optimal deployment of static sinks, the nodes close to a sink will deplete their energy rather rapidly. Adding some mobile sinks to a set of static sinks has been shown to improve the data delivery rate and to reduce energy dissipation of the sensor nodes.

3.8.5 WSNs with a mobile sink

Another approach for extending the lifetime of the nodes close to the sink is the utilization of a mobile sink. In some aspects, this is similar to using several static sinks – however, using several static sinks requires additional global communication for collecting all data at a single final point. In order to overcome the shortcomings observed for a static sink, the use of a mobile sink has been proposed. A mobile sink can follow different types of mobility patterns in the sensor field, such as random mobility, predictable/fixed path mobility, or controlled mobility, which has consequences with respect to energy efficiency and data collection strategies. In the following we summarize some proposed solutions for each type of mobility.

Random mobility: In this class, the sink follows a random path in the sensor field and important questions relate to the data collection strategy. Usually, the sink uses a pull strategy for collecting data from the sensor nodes. In a pull strategy, a node forwards its data only when the sink initiates a request for it, whereas in a push strategy a node proactively sends its data towards the sink. The random sink mobility can be used to reduce E_{max} and E_{bar} compared to the case of a static sink. Single hop data collection leads to the strongest reduction of energy consumption, because no data relaying load on the sensor nodes exists. However, it can also result in incomplete data collection from the WSN, because with a random mobility pattern there is no guarantee that the sink will reach all nodes in the sensor field or it might take too much time to do so.If the time required for complete coverage of the field has to be even lower, then the sink can be programmed to collect data from all nodes which are within a maximum

number of hops larger than one. This results in increased relaying load on the sensor nodes, and hence increases E_{max} and E_{bar} compared to the case of single hop data collection.

Obviously, there is an important trade-off between coverage time of the WSN and energy dissipation. The coverage time can be further reduced if multiple mobile sinks move randomly in the sensor field in an efficient way. The path coordination of the mobile sinks in the sense that each sink leaves a trail on its mobility path is introduced. When other sinks encounter this trail they change their mobility direction, which improves the coverage of the sensor field. However, the extra coordination effort needed for these strategies results in additional overhead and additional energy dissipation from the nodes.

If the data collection is not triggered by the sink, but follows a push strategy, another major overhead in the case of random sink mobility occurs because of the difficulty of tracking the current position of the sink and adapting the routing paths to the sink in the case of multi-hop communications, which leads to increased energy dissipation. In order to address this issue, the overhearing feature of the wireless networks is to track the position of the randomly moving sink. The mobile sink periodically transmit a beacon message containing its position. Whenever a neighbouring node of the sink hears this message, it updates the sink location in subsequently transmitted packets accordingly. Every node that overhears the packet from neighbouring nodes of the sink will also update the location coordinates of the sink thus eventually all nodes will have updated the location coordinates of the sink for geographic routing. A multi agent based data routing and mobile sink tracking scheme is proposed. It selects multiple intermediate nodes between a source node and the sink, which are called agents. These agents (especially the one closest to the sink) are responsible of tracking the location of the mobile sink thus minimizing the path updating cost that eventually reduces the overhead in tracking the location of the randomly moving sink. A mobile sink based data collection scheme is introduced for delay tolerant networks by formulating an optimization problem that maximizes the lifetime of the WSN given delay and flow conservation constraints. The formulated

model enables the node to identify the best time to route data to the sink so that all constraints regarding energy and delay can be met.

Fixed mobility: In this class of schemes the sink is programmed to follow a fixed path in a round robin fashion. This fixed path is predetermined and is not influenced by the behavior of the WSN at runtime. Coverage of the sensor field has to be guaranteed by an appropriate strategy for determining the routing paths for the data packets. An important distinction is whether the sink can predict its future positions or not. Moreover, sink mobility is planned such that the complete sensor field can be traversed in minimum possible time. As a result, energy dissipation (E_{max} and E_{bar}) can be very low. In case the sink is able to predict its future positions it can communicate this information to a node located in the vicinity of its future position. This node is responsible for collecting the sensor data in its vicinity so that when the sink actually arrives at this position, it should not have to wait for the data. This idea for a sink with directional antenna, claiming that their scheme results in increased packet delivery rate and reduced energy dissipation of the nodes.

The problem of finding the optimum fixed path in terms of network lifetime has been investigated theoretically. For a simple network model they showed that if nodes in a WSN are programmed to report data towards the sink within a certain fixed time interval, then minimum E_{max} can only be achieved if the mobility trajectory of the sink is set close to the periphery of the sensor field. The authors noted that due to the simplified system model their results may be misleading. A practical routing protocol is designed that not only balances the energy dissipation of the nodes but also tries to reduce data losses. Based on simulations, they illustrate the advantages of a mobile sink over a static one. Their scheme is based on discrete mobility of the sink, where the sink sojourn time at predetermined locations is greater than its mobility time (total time that the sink spends in motion) which helps to avoid frequent route updates in the WSN, hence leading to energy efficiency both in terms of E_{max} and E_{bar} compared to other mobile sink based routing schemes.

So far, it was assumed that the data rate is identical for all sensor nodes. In the case of varying data rates across sensors, energy dissipation can be balanced by

partitioning the nodes in groups (clusters) such that each group has approximately the same total data rate. Based on this assumption, the sensor field in small portions equal to the number of available data collector nodes is divided, which they call ‘‘gateway nodes’’. The gateway nodes have similar duties as the cluster heads mentioned earlier. The heuristic algorithms for the selection of packet nodes and assigning them to gateway nodes is introduced. This way, each portion of the field has a set of packet nodes that route their data to the corresponding gateway node. Then the trajectory of the sink is fixed and it is defined such that in each cycle it must pass by each gateway for data collection. It denote the cluster heads as ‘‘sub sinks’’, which are deployed in the sensor field. Each sensor node is then associated with one of the sub sinks. The association criterion is based on how much time the sink spends with each sub sink. If a sub sink has the mobile sink in its vicinity for a longer time, then more sensor nodes are associated with it and vice versa, which improves the throughput of the sensor field.

Controlled mobility refers to schemes where sink mobility is controlled or guided based on a parameter of interest, such as residual energy of the nodes, or on a predefined objective function, or on predefined observable events.

The performance of a routing protocol in a WSN strongly depends on the network and energy model considered.

Mobility model

Two basic types of state-of-the-art routing protocols are:

(i) the SS protocol for a WSN based on a static sink placed at the center of the sensor field and on shortest path routing of data from the nodes towards the sink and

(ii) the MS protocol for a WSN based on a mobile sink which moves along a fixed concentric circle around the center of the WSN in a stop-and-go fashion and on shortest path routing of data from the nodes towards the current location of the sink. During the early days of WSNs only static sinks were used and it was recognized that the strategically best position for a static sink in a WSN is the center of the field, as this leads to minimum E_{bar}.

CHAPTER 4

Network Simulator 2 (NS2)

NS2 is an open- source simulation tool that runs on Linux. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP over wired and wireless (local and satellite) networks. It has many advantages that make it useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS2 supports several algorithms in routing and queuing. Queuing algorithms include fair queuing, deficit round-robin and FIFO. REAL is a network simulator originally intended for studying the dynamic behavior of flow and congestion control schemes in packet switched data network. NS2 is available on several platforms such as FreeBSD, Linux, Sim OS and Solaris. NS2 also builds and runs under Windows.

Simulation has been carried out using Network Simulator (NS2). Totally 20 nodes are deployed for simulation scenario. Some of the nodes are fixed and some are movable. The nodes act as gateways for sensor network in every cell. Each cell is provided with a Base Station Controller to control and resolve dynamic routing strategies for the gateways and sensor nodes. There is a network monitor deployed per every three cell to monitor the communication.

4.1 Node Methods: Configuring the Node

Procedures to configure an individual node can be classified into:

1. Control functions
2. Address and Port number management, unicast routing functions
3. Agent management
4. Adding neighbours

4.1.1 Control functions

1. $node entry returns the entry point for a node. This is the first element which will handle packets arriving at that node. The Node instance variable, entry_, stores the reference this element. For multicast nodes, the entry point is the switch_ which looks

at the first bit to decide whether it should forward the packet to the unicast classifier, or the multicast classifier as appropriate.

2. $node reset will reset all agents at the node.

4.1.2 Address and port number management

1. The procedure **$node id** returns the node number of the node. This number is automatically incremented and assigned to each node at creation by class Simulator method, $ns node.

2. The procedure **$node agent <port>**returns the handle of the agent at the specified port. If no agent at the specified port number is available, the procedure returns the null string.

3. The procedure **alloc_ port** returns the next available port number. Is uses an instance variable, np_, to track the next unallocated port number.

4. The procedures, **add_ route** and add-routes, are used by unicast routing to add routes to populate the classifier.

4.1.3 Agent management

Given an <agent>, the procedure attach{} will add the agent to its list of agents_, assign a port number the agent and set its source address, set the target of the agent to be its (i.e., the node's) entry{}, and add a pointer to the port demultiplexer at the node (dmux_) to the agent at the corresponding slot in the dmux_ classifier. Conversely, detach{} will remove the agent from agents_, and points the agent's target, and the entry in the node dmux_ to mullagent.

4.1.4 Adding Neighbours

Each node keeps a list of its adjacent neighbours in its instance variable, neighbour. The procedure add neighbour {} adds a neighbour to the list. The procedure neighbours {} returns this list.

CHAPTER 5

SIMULATION SCENARIO AND RESULTS

5.1 SIMULATION SCENARIO

Simulation has been carried out using Network Simulator. Totally 20 nodes are deployed for simulation scenario. Some of the nodes are fixed and some are movable. The nodes act as gateways for sensor network in every cell. Each cell is provided with a Base Station Controller to control and resolve dynamic routing strategies for the gateways and sensor nodes. There is a network monitor deployed per every three cell to monitor the communication.

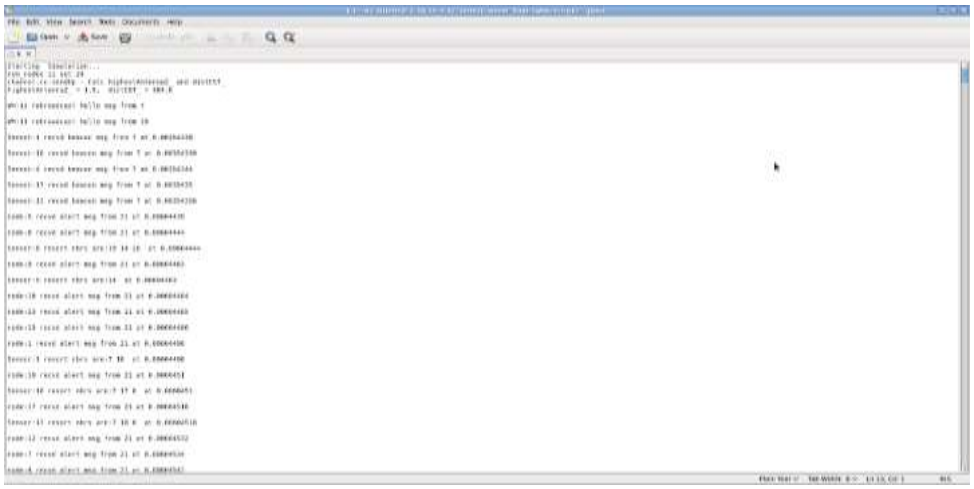

Figure.5.1 Simulation Output

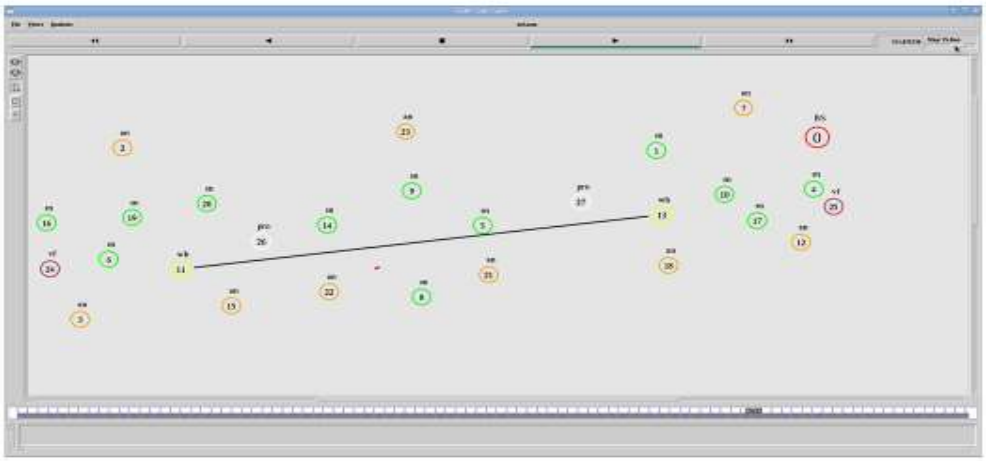

Figure.5.2 Simulation Step

5.2 PARAMETER INITIALIZATION

In order to analyze various parameters mainly packet delivery ratio, dropping ratio, delay and throughput, the following parameters are configured in the network simulator.

Routing Protocol	SWSN,MSWSN
Interface Queue	Droptail/PriQueue
Antenna	Omni directional Antenna
No. of nodes	25
No. of wormhole nodes	2
Energy of the node	1000 Joules

5.3 PACKET DELIVERY RATIO

Packet delivery ratio denotes the efficiency of a data transmission system. It is given by,

$$PDR(\%) = \frac{\text{Number of packets sent}}{\text{Number of packets received}} \times 100$$

The average packet delivery of every node for various network scenarios is plotted and shown in the Figure. PDR is one of the QoS parameters and it is closely related to throughput. It is shown that in existing system, the average packet delivery ratio is much less and it is enhanced by the implementation of flat converged proposal. Further in the enhanced proposal, the interference in the channel is avoided and this improves the delivery ratio to an optimized value.

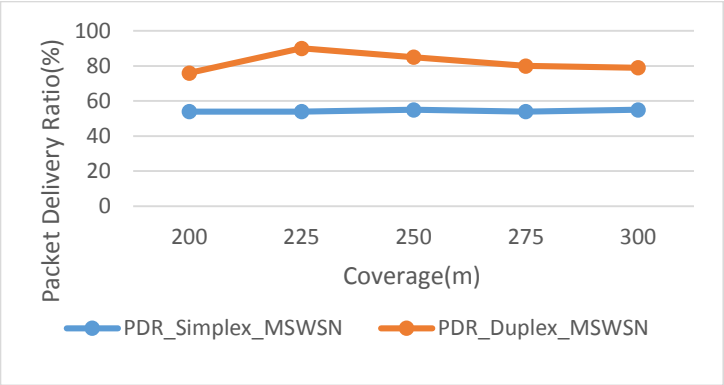

Figure. 5.3. Packet Delivery Ratio

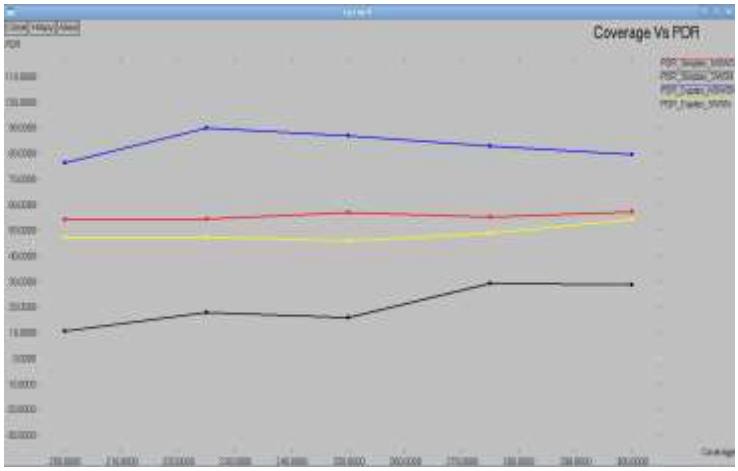

Figure. 5.3.1 Coverage Vs PDR

5.4 THROUGHPUT

To attain both high spectral efficiency and good coverage within sectors/beams, a scheme based on coordinated scheduling between sectors of the same site, and the employment of frequency reuse factor above 1 only in outer parts of the sector, is proposed and evaluated. The resulting sector throughput increases with the number of active users. As shown in the Figure.5.4.1, the enhanced proposal improves high yield in throughput as compared with the existing methods.

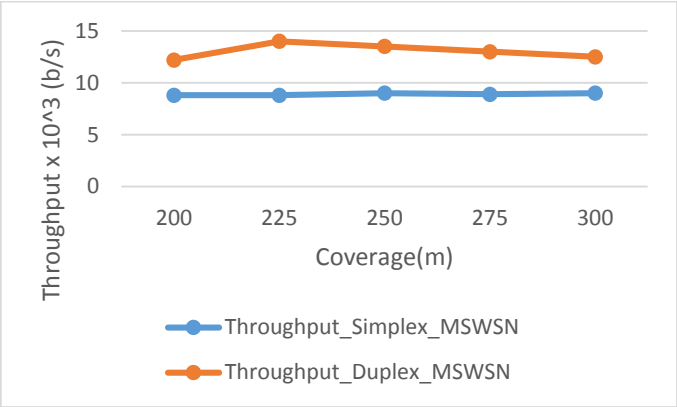

Figure.5.4. Throughput

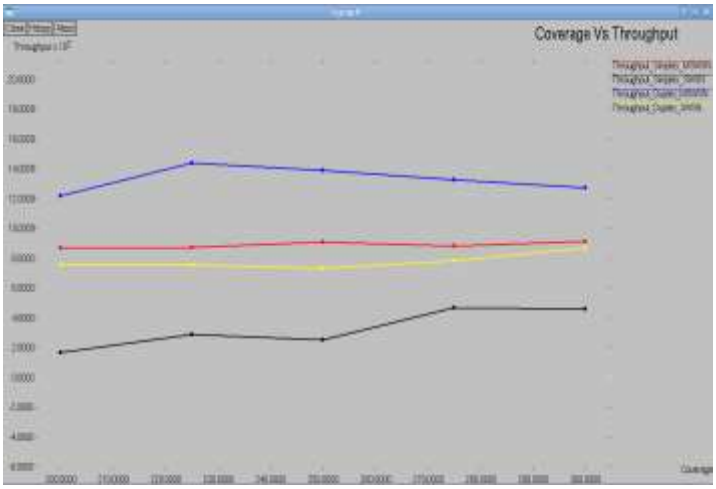

Figure.5.4.1 Coverage Vs Throughput

5.5 DELAY

The average end to end latency of every node for various network scenarios is plotted and shown in the Figure.5.5. It is defined as the inter arrival time between first packet time and second packet time divided over total packet delivery time. The increased latency in existing hierarchical architecture is overcome in the proposed converged system as shown in the Figure.5.5.1 and again the system is enhanced using interference avoidance algorithms as stated above. This provides additional reduction in latency and thereby improves the Qos.

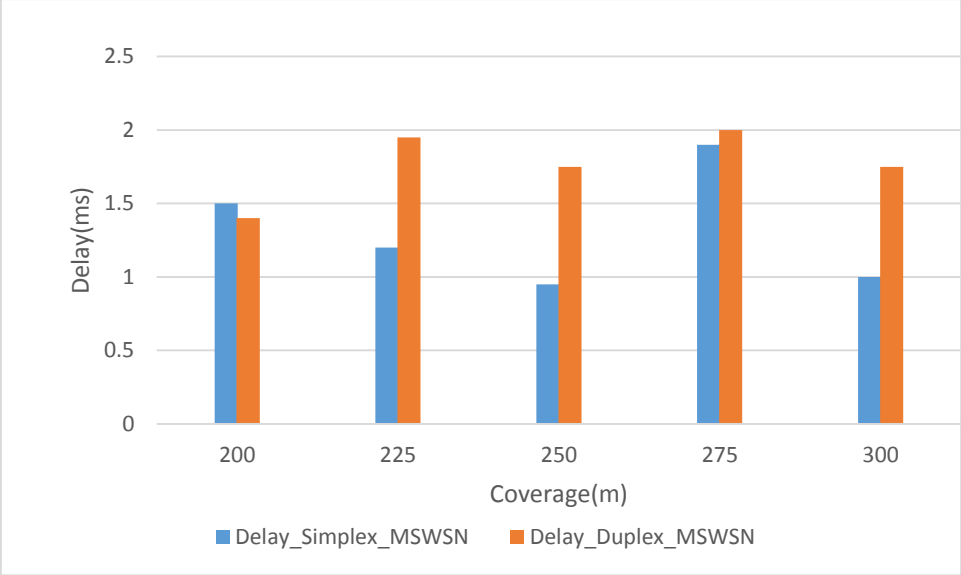

Figure.5.5 Delay

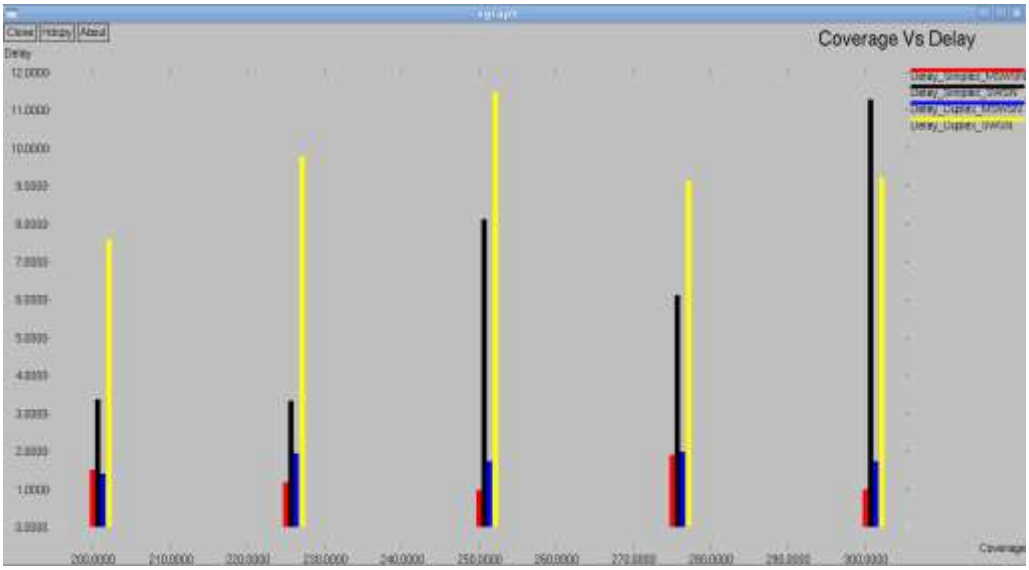

Figure.5.5.1 Coverage Vs Delay

5.6 DROPPING RATIO

Dropping Ratio denotes the number of packets of data travelling across the network fail to reach their destination. It is measured as a percentage of packets lost with respect to packets sent. The dropping ratio is estimated and plotted as shown in the Figure.5.6.

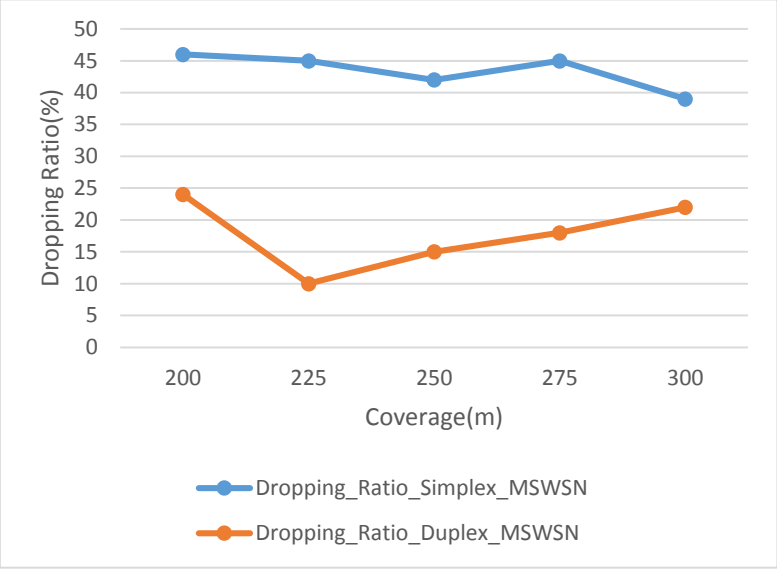

Figure.5.6 Dropping Ratio

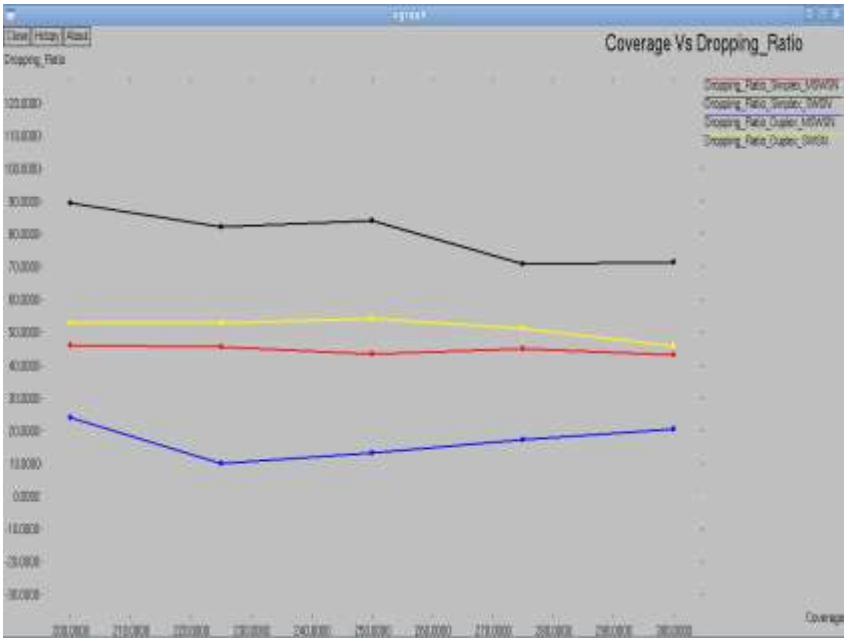

Figure.5.6.1 Coverage Vs Dropping Ratio

5.7 ENERGY CONSUMPTION

Energy consumption of a node is given by the formula,

$$\text{Energy Consumed} = \frac{\text{Average energy consumed in idle, sleep, txt and rxt mode}}{\text{Total energy consumed}}$$

The energy consumed per node for various network scenarios is plotted and shown in the Figure.5.7.

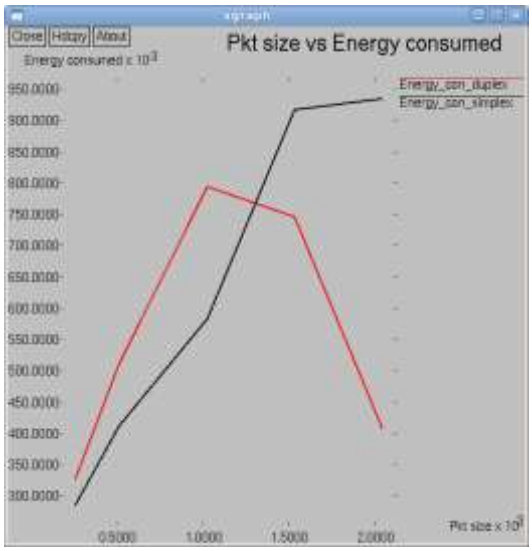

Figure.5.7 Energy consumed

5.8 NORMALIZE ROUTING OVERHEAD

Normalized routing load is computed as sent (and forwarded) dynamic source routing control packets divided by number of data packets received to the destination.

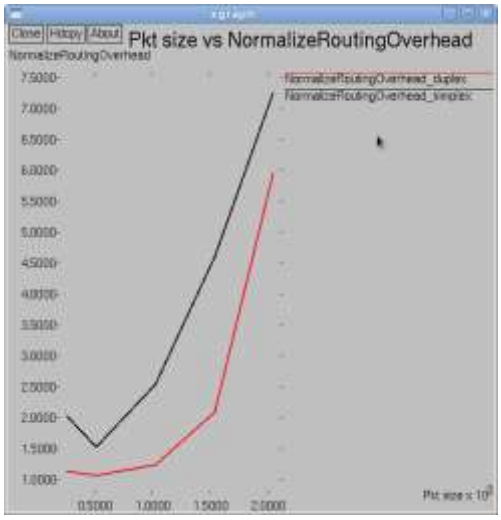

Figure.5.8 Normalize Routing Overhead

5.9 OVERHEAD

Overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal. It can be expressed as a percentage of non-application bytes (protocol and frame synchronization) divided by the total number of bytes in the message.

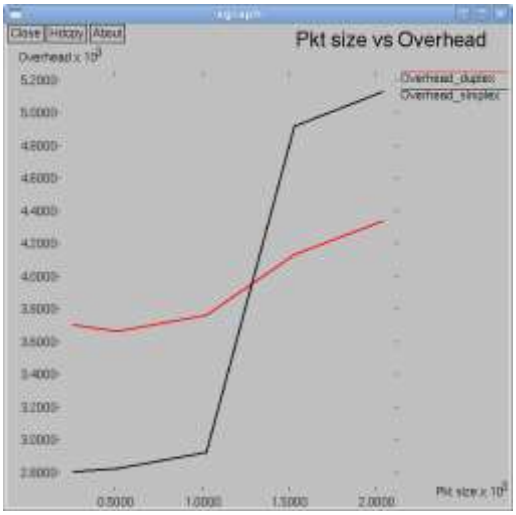

Figure.5.9 Overhead

CHAPTER 6

CONCLUSION AND FUTURE WORK

The severe impacts of the wormhole attack on the DV-Hop based localization in wireless sensor networks is analysed. The detection of wormhole attacks is analysed by packet size with the parameters such as Packet Delivery Ratio (PDR), Delay, Throughput, Dropping Ratio, Energy consumed, Normalized Routing Overhead and Overhead. In the proposed method, with the introduction of two prover nodes and a verifier node, the wormhole attack is detected effectively by reducing computational time, delay compared to the existing method of analysing each node separately by estimating its hop distance. Simulations are performed to demonstrate the effectiveness of our proposed scheme under different network parameters.

In our future work, we will extend our localization scheme to tolerate the packet loss. Also, we will consider the scenario when different types of nodes have different transmission radii to estimate probability of wormhole attack detection.

CHAPTER 7
REFERENCES

[1] Boukerche A, Oliveira H.A.B.F., Nakamura E.F., Loureiro A.A.F.,'Secure localization algorithms for wireless sensor networks', IEEE Commun. Mag. (2008)96–101.

[2] Bulusu N, Heidemann J, Estrin D(2000), 'GPS-less low cost outdoor localization for very small devices', IEEE Personal Communications, vol. 7,pp. 28–34.

[3] Capkun S, Cagalj M, Srivastava M, 'Secure localization with hidden and mobile base stations', in: Proc. of IEEE INFOCOM, 2006.

[4] Daisuke Takaishi (2014), 'Toward Energy Efficient Big Data Gathering in Densely Distributed Sensor Networks', IEEE transactions on emerging topics in computing, Vol.2, No.3, pp.388-397.

[5] Guiyi Wei et al., 'Detecting Wormhole Attacks Using Probabilistic Routing and Redundancy Transmission', International Conference on Multimedia Information Networking and Security,2010.

[6] Hao-Ting Pai (2011),'Prevention of wormhole attacks in mobile commerce based on non-infrastructure wireless networks', Electronic Commerce Research and Applications, pp.384-397.

[7] He T, Huang C, Blum B, Stankovic J.A.,Abdelzaher T, 'Range-free localization schemes for large scale sensor networks,, in: Proc. of ACM MOBICOM,2003, pp. 81–95.

[8] Honglong Chen,Wei Lou,Zhi Wang,Junfeng Wu,Zhibo Wang,Aihua Xia16 (2015), 'Securing DV-Hop localization against wormhole attacks in wireless sensor networks',Pervasive and Mobile Computing,pp.22–35.

[9] Jianqing Ma (2006), 'SeLoc: Secure Localization for Wireless Sensor and Actor Network, IEEE.

[10] Junfeng Wu et al.(2010),'Label-Based DV-Hop Localization Against Wormhole Attacks in Wireless Sensor Networks', Fifth IEEE International Conference on Networking, Architecture, and Storage.

[11] Liu D, Ning P, Du W, 'Attack-resistant location estimation in sensor networks', in: Proc. of IEEE IPSN, 2005.

[12] Loukas Lazos et al.,(2005),'ROPE: Robust Position Estimation in Wireless Sensor Networks',IEEE.

[13] Majid I. Khan et al. 36(2013), 'Static Vs mobile sink: The influence of basic parameters on energy efficiency in wireless sensor networks, Computer Communications', pp. 965-978.

[14] Ming-Yang Su (2010), 'WARP: A wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks, Computers and Security, pp.208-224.

[15] Nabila Labraoui, Mourad Gueroui(2011), 'Secure Range-free Localization Scheme in Wireless Sensor Networks',IEEE.

[16] Niculescu D, Nath B, 'Ad hoc positioning system (APS) using AOA', in: Proc. of IEEE INFOCOM, 2003.

[17] Phillip Lee (2014),'A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems',IEEE transactions on automatic control, Vol.59,No.12.

[18] Ram Ramanathan (2000),'Topology control of Multihop Wireless Networks using Transmit Power Adjustment', IEEE INFOCOM 2000, pp.404-413.

[19] Saurabh Gupta et al.**, '**Wormhole Attack Detection Protocol using Hound Packet', International conference on Innovations in Information Technology,2011.

[20] Shams Qazi (2013), 'Securing DSR against wormhole attacks in multirate adhoc networks', Journal of Network and Computer Applications, .582-592.

[21] Shiyu Ji, Tingting Chen, Sheng Zhong, 'Wormhole Attack Detection Algorithms in Wireless Network Coding Systems',2013.

[22] Thanassis Giannetsos et al. 80 (2014),'LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks', Journal of Computer and System Sciences,pp.618–643.

[23] Yih-Chun (2006),'Wormhole attacks in Wireless Networks', IEEE journal on selected areas in communications, Vol.24, No.2, pp.370-380.

[24] Zhiguo Shi et al. (2014), 'A wormhole attack resistant neighbhor discovery scheme with RDMA protocol for 60GHz directional network', IEEE transactions on emerging topics in computing, pp.341-352.

[25] Zhiwei Li, Di Pu et al(2011),'Forced Collision: Detecting Wormhole Attacks with Physical Layer Network Coding', Tsinghua Science and Technology, October 2011, 16(5),volume 16,pp.505-519.

CHAPTER 8
LIST OF PUBLICATIONS

- Presented a paper titled "Detecting and Defending Wormhole Attacks using Localization Scheme in Wireless Sensor Networks" in the TEQIP II sponsored National Conference on "Advanced Computing and Communication Systems" (NCACCS 2016) on 4th April 2016, at Government College of Technology, Coimbatore.

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

GOVERNMENT COLLEGE OF TECHNOLOGY

(An Autonomous Institution Affiliated to Anna University, Chennai)

Coimbatore - 641 013

National Conference

NCACCS 2016

Certificate

This is to certify that Dr./Mr./Ms. ATAV . S, of KUMARAGURU COLLEGE OF TECHNOLOGY, COVAI has presented a paper entitled DETECTING AND DEFENDING WORMHOLE ATTACKS USING LOCALIZATION SCHEME IN WIRELESS SENSOR N/WS. in the TEQIP II sponsored National Conference on "Advanced Computing and Communication Systems" (NCACCS 2016) on 4th April 2016, organised by the Department of Electronic & Communication Engineering.

ORGANIZING SECRETARY

CONVENER

PRINCIPAL