Comparative Analysis of WSN MAC Protocols and Node Clone Attack

A Dissertation Submitted in Partial Fulfillment of the Requirement for the Degree of

Master of Technology

In

Computer Science & Engineering

Under the Supervision of

Dr. Yashwant Singh

By

Balmukund Mishra (132218)

Jaypee University of Information Technology
Waknaghat, Solan – 173234, Himachal Pradesh

May, 2015

Certificate

This is to certify that dissertation entitled "**Comparative Analysis of WSN MAC Protocols and Node Clone Attack**", submitted by "Balmukund Mishra" in partial fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor: ……..

Name of Supervisor: **Dr. Yashwant Singh**

Designation: **Assistant Professor**

Date: ……

Acknowledgement

Foremost, I would like to express my sincere gratitude to my advisor **Dr. Yashwant Singh** for the continuous support and guidance for my project work, for his patience, motivation, enthusiasm, and immense knowledge. His guidance has helped me at all times of my research and writing of this thesis. I could not have imagined having a better advisor and mentor for my thesis study.

I would like to thank my advisor Dr. Yashwant Singh for sharing his vast expanse of knowledge guiding me with the correct books, research issues to study without which I wouldn't have been able to proceed so much further in my topic ofComparative Analysis of WSN MAC Protocols and Node Clone Attack. He always spared his valuable time and helped in striving to move forward to this point.

Secondly, I would like to thanks **my Parents** who have always been with me for inspiring me and thirdly, I would like to thanks **God** for keeping me energetic, healthy and enthusiastic.

Signature of the student ……..

Name of Student: Balmukund Mishra

Date ……..

TABLE OF CONTENTS

List of Figures

List of Tables

Abstract

Wireless Sensor Networks (WSN) are practiced in many real life applications such as military, weather forecasting, medical, target spotting and tracking, etc. The sensor nodes are spread over the target area for the accumulation of data. The collected data further transmitted from one sensor node to other sensor node. WSN nodes have limited resources like energy, memory and processing capabilities. Efficient utilization of these resources is challenging task in WSN. MAC layer of wireless sensor nodes plays a vital role in WSN because most of the power is depleted at this layer due to collision in medium access and node synchronization.

We have given a comparative analysis of all the existing WSN MAC protocol. The comparison is done on the basis of various parameters such as energy consumption, end to end latency, scalability, security from the outside attacker. Analysis of these MAC protocols will serve us in selection of a MAC protocol for a particular WSN application. As well as second part of my project is node clone detection. Node clone in wireless sensor network is very dangerous issue because nodes are deployed in hostile environment where it is not possible to physically go and protect the system and node. So nodes deployed in hostile environment can easily captured and compromised by intruders and all the confidential and personal data been extracted from node. However, they require too strong assumptions to be practical for large-scale, randomly deployed sensor networks. In this project work we will give a novel approach for node clone detection that will takes very less communication messages for detection of node clone and revocation.

CHAPTER-1
INTRODUCTION

1.1 Introduction

Wireless sensor networks (WSN) are a kind of ad hoc networks where large numbers of tiny sensor nodes are deployed in remote, hostile environment. Due to the wireless communication and the node structure, WSN suffer from many issues that affect its performance. Energy consumption is one of the main issues in wireless sensor networks because replacement of power source in a short interval is not possible. Wireless sensor networks has an infrastructure less architecture, i.e. in WSN every node, equipped with smart sensor, can communicate with each other without any fixed architecture. The term “wireless” has become a generic and all-encompassing word used to describe communication in which electromagnetic waves carries a signal over part or whole communication path. WSN technology is able to reach virtually every location on the surface because of wireless communication medium.

The major component of a sensor node is sensing module, processing module, transceiver, storage module and a power source. In addition a mobilizer service is also implemented. All these modules must be fitted into small sized node. The life time of sensor node depends on the power supply unit of sensors. Different node has their different transmission range and reliability,which varies according to time, and application. Transmission range of a node also affects the lifetime of sensor nodes because higher transmission range require more energy to transmit. Therefore, it is necessary to check the accuracy of transceivers by comparing the reading with those of a standard [1].

WSN have thousands of applications in human life with various challenges. For example in military application the size of sensor node is very small such that one can’t easily anticipate the location of sensor node. Wireless sensor node should be able to identify their neighbours, so getting the location of neighbour is a basic challenge of WSN. Other challenges of the WSN are data type and data rates. In mission critical WSN application, it should be ensured that the data transmitted is

delivered correctly to the end user or not. Data should be received in a secured manner without tampering or eavesdropping [2].

Hardware and software used in wireless sensor networks impose a lot of design issues that must be addressed while designing to achieve efficient and effective operations in WSN [3]. In WSN many researchers worked earlier to improve the performance, accuracy and adoptability.

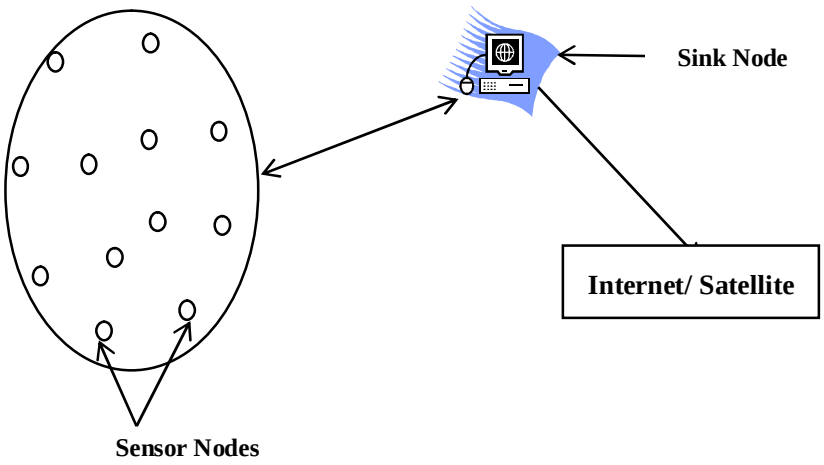

Fig-1.1 Architecture of WSN

A major part of power is consumed in radio (transmitter and receiver), which is controlled by the MAC protocol. So the energy efficient MAC protocol will increase the lifetime of sensor networks up to a certain level. MAC is a sub layer of data link layer, where MAC protocols are used to arbitrate the access of communication channel. Since a common communication channel is used, collision and traffic control is the main issued at MAC sub layer. Many MAC layer attacks depend only on increasing the traffic on the networks, which is converted in DOS attack after some time. The purpose of DOS attack is to waste the resources of WSN such that the networks cannot perform their function normally. So efficiently utilising our resources and controlling these attacks should be basic properties of MAC layer's protocols.

In any type of networks it is not possible to leave the security aspect because data travels into the networks must be protected. In sensor networks protection of data in the nodes is also very important because nodes are deployed in remote and hostile environment. Another important challenge in designing security mechanisms of

wireless sensor networks, cryptographic algorithm requires complex processing which takes much time and power which is not feasible in wireless sensor networks.Security at Mac layer is another important concern because by attacking at a node, an attacker can waste the WSN node energy unnecessarily, steal, and interrupt data transmission. Node clone attack is one of the major concerned attacks in WSN. In node clone attack, attacker initially captures the nodes, deployed in remote, hostile environment and then places its replica into different part of the networks [4].

1.2 Problem Statement

WSN is a collection of large number of small sensor nodes deployed in hostile environment. Nodes in WSN have limited amount of resources in terms of energy, memory and computation capability. So efficient utilisation of resources should be the key feature of current protocols developed and used in WSN.MAC protocols main feature is to arbitrate the access of communication medium. Most of the power in a node is consumed by the transmitter and receiver unit, which is controlled by MAC protocols. For the application of WSN which protocols should be used is a main problem. Another issue is security of WSN from the attacks,one of the attack is node clone, which makes the replica of compromised node. Node clone attack can generate many attacks in networks. Few problems which may come across in WSN are:

1. All existing MAC protocols are either involved in collisions (Contention Based) or have latency (Schedule Based) that will cause problems for WSN in the terms of energy inefficiency and throughput.
2. The second main problem with the WSN is their vulnerability to different attacks because of resource limitation, sensor node deployments in a hostile ad unrestricted environments.

1.3 Objectives

Selecting MAC protocols for specific application is a main problem in wireless sensor networks. Another issue is security in WSN. Many algorithms have been proposed so far for detecting node clones in wireless sensor networks. On the basis of various problems is WSN, our objectives are:

1. To present a Comparative Analysis of existing energy efficient MAC Protocols for WSN.

2. To develop a novel approach for detecting node clones in wireless sensor networks.

1.4 Methodology

We have selected two problems for our dissertation; first one is comparative analysis of WSN MAC protocols. For this we have compared all the existing MAC protocols on the basis of WSN parameters like energy, latency, end-to-end delay and throughput etc. and based upon the comparison result, we have concluded by application specific usage of MAC layer protocols in wireless sensor networks.

For the second problem which is node clone detection in wireless sensor networks, we have compared all the existing protocol in witness based node clone detection category and proposed a novel approach for witness based node clone detection. For the simulation, we have used a java simulator and implemented two latest protocols in the literature, and compared our proposed result with the other two protocols.

1.5 Contributions

To achieve our objectives, we have made comparative analysis on various MAC layer protocols and we have proposed an approach for node clone detection Following are the publications:

Paper-1 Balmukund Mishra, Vandana Mohindru, Yashwant Singh "Comparative Analysis WSN MAC protocol" JBAER October 2014 Volume 1 Number 6.Pg: 15-23 ISSN: 2350-0077.

Paper-2 Balmukund Mishra, Yashwant Singh "An approach towards the witness based node clone detection in WSN" Third International Symposium on security in computing and communication SCMS ALUVA, KOCHI, KERLA, INDIA, March 2015, SPRINGER, SCOPUS (Communicated).

1.6 Thesis Organisation

This dissertation includes five different chapters. First chapter gives the organisation of the dissertation that is Introduction, problem statement and motivation followed by the chapter wise organisation of the thesis.

Chapter 2 gives a detailed study of wireless sensor networks its requirements, assumptions and the existing problems. In chapter 2 we have provided the protocol stack, applications areas and security requirements of the wireless sensor networks. This chapter also includes the complete literature survey of our dissertation. For both of our objective, we have discussed all the related works that is necessary to explain.

In chapter-3 we have given the comparative analysis of all the WSN MAC protocols which has been presented in literature survey.

Chapter 4 is about the complete study of Node clone attack, our proposed method for node clone detection, demo of simulators and comparative analysis with previous existing protocols. On the basis of comparison done in this chapter we have given an analysis of the node clone detection methods.

Finally chapter five presents the conclusion and future work.

CHAPTER 2
LITERATURE SURVEY

2.1 Introduction

Wireless Sensor Networks (WSN) is networks that composed of many sensor nodes. The number of sensors varies depend on the scope of the networks. The nodes of the WSN may be used in various environmental conditions, such as under the sea, battle or in a furnace. Sensor networks can be used for target tracking, system control and chemical and biological detection. In military applications sensor networks can enable soldiers to see around corners and to detect chemical and biological weapons long before they get close enough to cause harm them. Civilian uses this network for environmental monitoring, traffic control and providing health care monitoring for the elderly while allowing them more freedom to move around. These smart sensor nodes have constraints on their power and memory. Generally WSNs work with the battery power. In addition, nodes may use other energy resources, such as solar energy or use vibration of their surroundings to become part of the required energy. However, the major problem with WSNs is limited energy [5].

Sensor networks have resource constraints in energy, memory, storage space and computing power. These constraints cause many challenges for WSNs designers and developers. The designers must design networks that are designed highly distributed, fault-tolerant, secure, and efficient in energy consumption. For many sensor networks applications, security requirements are very critical issue. Some of these applications are in the military field and must protect their important and critical data against attacks. Another major issue in these applications is data integrity and authentication [6]. Apart from military applications, there are applications that authentication and integrity protection are more important than confidentiality in these networks. In many applications, these networks are used in hostile and inaccessible environments. Due to cost constraints, resistant and secure hardware using for all nodes is not possible. Therefore, the attacker can access any node and read nodes information that this information can include encryption keys. However in the WSNs Nodes coordinate is important to carry out their duties, in the event of loss any node.

Figure 2.1 shows the WSN node architecture. The concept of wireless sensor networks is based on simply combining these for separate module into a unit and connecting it via wireless ad hoc networks for communication. In this initially Sensing unit will start functioning and in a very short time interval it will sense the medium and collects the data. This data will go to the memory and then processor for further processing, after this processed data will go to the transceiver\Receiver unit [7].

2.1.1 Sensing Unit

Sensing unit has actual sensors which capture the information from the environment and stores it in its memory for some time.

2.1.2 Computation Unit or Processor

Locally stored information is then goes to the processor and different kind of operation can be performed on this data to reduce the data size and getting actual data.

2.1.3 Transceiver

Transmitter and Receiver is the most important part of a sensor node because most of the power in sensor node is consumed in this module. Transceiver and receiver are used to transmit data and receiver is for receiving data from the networks. All the energy efficient protocol will turn off the transceiver/receiver unit into sleep mode whenever a node will not have any data to send or receive.

2.1.4 Battery

All the operations performed inside the sensor node will require power and it is a limited source in WSN nodes. A power source in wireless sensor networks is a very important factor and nowadays every application of WSN application ad protocols are designed energy efficient that shows the importance of energy constraints in WSN. Another aspect is according to Moore’s laws the number of transistors increases every year in same cost and the same area so in near future we can afford more power in same cost and the same area that will be very beneficial for WSN application durability.

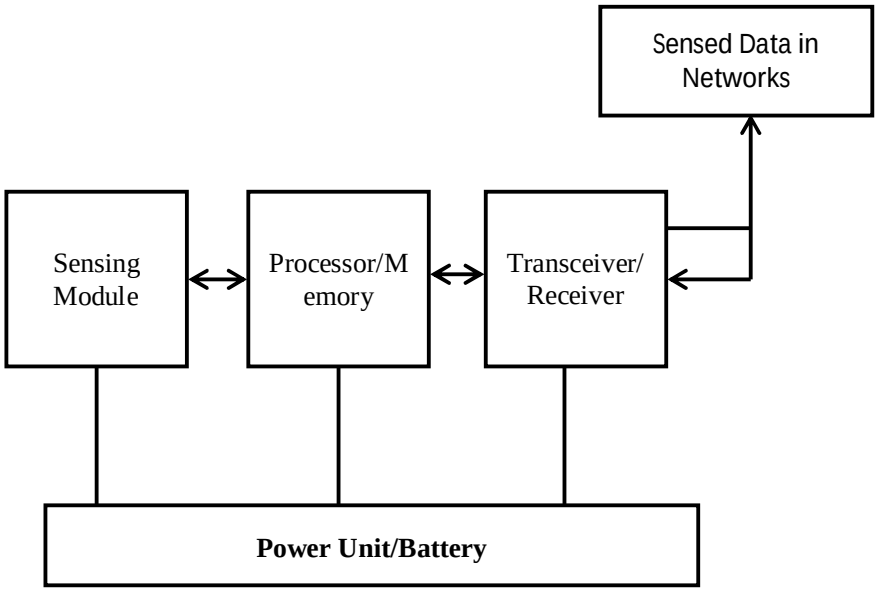

Fig-2.1 Node Architecture of WSN

2.1.5 Protocol stack of Wireless Sensor Networks

A simple protocol stack of WSN is shown in Fig-2.2. We will consider 4 main layers of the networks. Application layer defines a standard set of services and interface primitives available to a programmer independently on their implementation on every kind of platform. An example is the so called sensor networks services platform (SNSP).Second layer from the top is transport layer. Transport layer helps to maintain the flow of data if the sensor networks application requires it. Transport layer is especially needed when the system is planned to be accessed through the Internet or other external networks. Unlike protocols such as TCP, the end-to-end communication schemes in sensor networks are not based on global addressing. Therefore, new schemes that split the end-to-end communication probably at the sinks may be needed.Third layer is Networks layer in any layered architecture. Networks Layer takes care of routing the data, directing the process of selecting paths along which to send data in the networks [8].

Data link Layerprovides the multiplexing of data streams, data frame detection and medium access control (MAC).In the end Physical Layer is responsible for frequency and power selection, modulation, and data encryption.

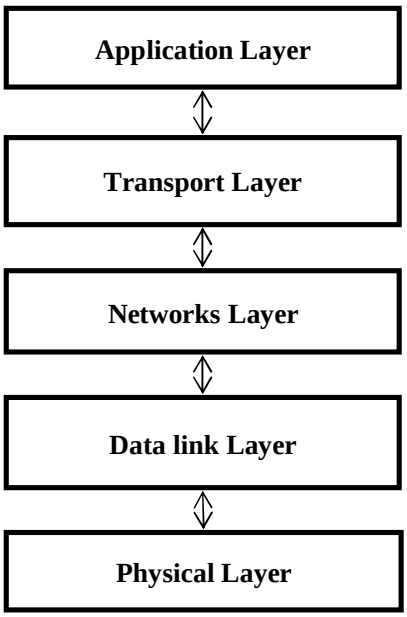

Fig-2.2 Layered Architecture of WSN

2.1.6 MAC (Media Access Control)

Media access is very critical issue in design of the wireless sensor networks. Collision of data from two are more than two sender in the medium is a big concern in WSN because it will unnecessarily consumed two much energy of wireless sensor networks nodes [9]. To solve this problem different kind of MC protocols are devised by various researchers which we will present in this section. However from different perspective the MAC protocols can be classified in different categories for example centralised and distributed, single channel based and multiple channel based, contention based and contention free and etc .This layer has as a primary responsibility to provide error-free transmission of data between two remote hosts (computers). At the source machine it receives the data from the Networks Layer, groups them into frames and from there are sent to the destination machine. From that point the data are received from the Data Layer at the destination, a checksum is computed there to make sure that the frames sent are identical with those received and eventually the data are passed to the Networks Layer. The **M**edia **A**ccess **C**ontrol **L**ayer is one of two sub layers that make up the Data Link Layer of the OSI model [10]. The MAC layer is responsible for moving data packets to and from one Networks Interface Card (NIC) to another across a shared channel. While MAC layer

for WSN is designed specifically such that all the major source of energy depletion should be as low as possible. There are three basic services that Data Link Layer commonly provides [11]:

1) Unacknowledged connectionless service.
2) Acknowledged connectionless service.
3) Acknowledged connection oriented service

In the first case frames are sent independently to destination without the destination machine acknowledge them. In case of a frame is lost no attempt is made by the Data Link Layer to recover it. Unacknowledged connectionless service is useful when the error rate is very small and the recovery of the frame is made by higher layers in the Networks hierarchy. Also LANs find this service appropriate for real-time traffic such as speech, in which late data are worse than dad data. Maybe you have personally experienced this case, where delay of data occurs in a computer to computer conversation. Imagine maintaining a computer to computer conversation with another person. It would be much better if the data were sent and received on time (as if the dialog was carried out via a normal telephone line) but a bit distorted instead of data received after 2sec delay and in better quality.

The second case is a more reliable service in which every single frame, as soon as it arrives to destination machine is individually acknowledged. In this way the sender knows whether or not the frame arrived safely to the destination. Acknowledged connectionless service is useful in unreliable channels such as wireless systems. Finally we have acknowledged connection oriented service. The source and destination machines establish a connection before any data are transferred. Each frame sent is number, as if it has a specific "ID", and the data link layer guarantees that each frame sent is indeed received by the other end exactly once and in the right order. This service is said to be the most sophisticated service the data link layer can provide to Networks layer.

2.1.6.1 MAC Protocol Design Challenges

MAC protocols are very important for successful networks operations. MAC protocols main objective is to arbitrate access to a shared medium or channel to reduce the collision rate of the networks and also it fairly distribute the networks bandwidth between different nodes of the wireless sensor networks.. Use of energy efficient, secure MAC protocol provides reliability and efficiency to the WSN.MAC is responsible for medium access, scheduling, buffer management and error control. In WSNs the first and matter issue is the lifetime of networks and nodes. For this reason MAC protocols must provide Energy efficiency in WSNs. On the other hand, MAC protocol designer must consider networks development, new nodes adding, multiplicity of nodes, the networks topology changes and such topics. Other important issues related to MAC protocols are fairness, delay, throughput and bandwidth. Also all of these topics are important for the WSNs, but the most important thing is the lifetime of networks nodes [12].

2.1.7 Node Clone Attack

Wireless sensor networks are subject to attacks such as node capture and cloning, where an attacker physically captures sensor nodes, replicates the nodes, which are deployed into the networks, and proceeds to take over the networks. Among many physical attacks to sensor networks, the node clone attack can create more damage in the networks. Because of production expense limitation, sensor nodes are generally short of tamper-resistance hardware components. Thus an adversary can capture a few nodes, extract code and all secret credentials and use those materials to clone many nodes out of of-the-shelf sensor hardware. Many detection algorithms for node capture and cloning attacks use distributed protocols that rely on collisions of messages containing node id and locations [13].

2.1.7.1 Security challenges of Wireless Sensor Networks

In the sensor networks, nodes should not disclose any data to neighbours. In many applications, nodes transmit very critical data, so create a secure communication channel in wireless sensor networks is very important. General information about the sensor, such as sensor identities and public keys, should be encrypted to be protected against traffic analysis attack. With data confidentiality, the adversary will not be able to steal information, but it does not mean that the data are

secure. An adversary can alter the data, and cause irregularity in the networks. Integrity ensures that the data that received during transmission is not changed by the malicious node. In the otherwise, even in the absence of malicious nodes, data can be modified, while is exchanges between nodes, so MAC using is necessary for providing data integrity [14].

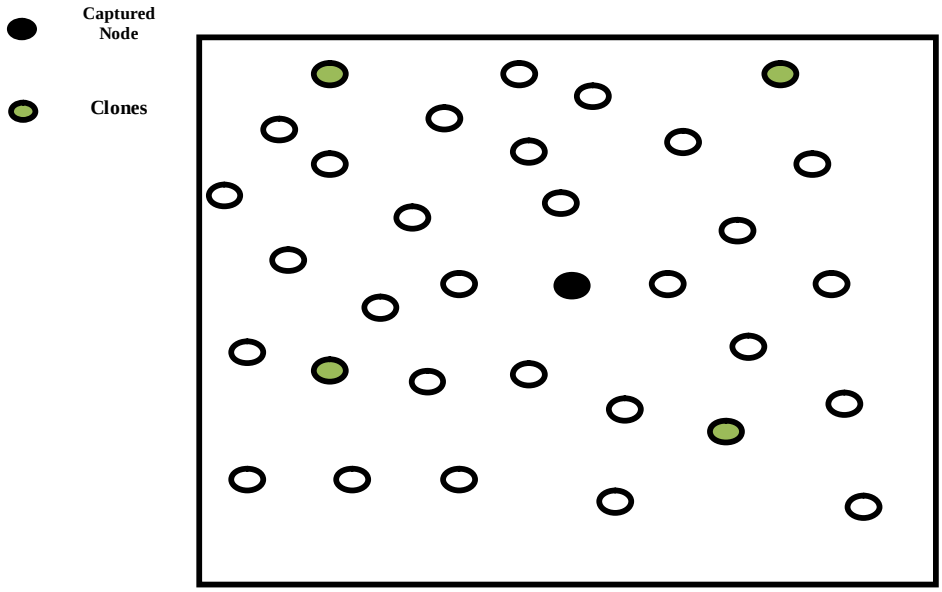

Fig-2.3 Example of Node Clone in WSN

Fig-2.3 shows the concept of node clone attack. In this figure number of sensor nodes is deployed in a rectangular region. Where black circles represents the attacked node. There may be more than one attacker can work in a region. Attacker initially captures the node, and makes replicas of the node by stealing the information present inside the node. Capturing of node is easy in wireless sensor networks because they are deployed in a remote region. In this diagram green circle represents the clones of the compromised node. Once the attacker places the replica of a node inside the region, it is difficult for networks administrator to discriminate between the original node and replica. However it can be identified that the copies of certain node ids is made, and can revoke all that kind of malicious node with that original node.

Due to the WSNs use wireless environment for data exchange, the networks must have mechanism to specify source and destination identity. Otherwise, a malicious node can receive and send information to other nodes. Data authentication allows the receiver to be sure that the data send from a valid sender that is a member of WSN. In the two-way communication, authentication can be obtained through a

symmetric mechanism. Transceiver shares a secret key to compute message authentication code (MAC) for all data.Even if the confidentiality and integrity of data is provided, the freshness of each message must to be provided. Simply, data freshness implies that the data is not old. This requirement is more important when we use shared key strategies for the networks. Although a shared key distribution in the networks is time consuming, but shared keys need to be changed. Also, if the sensor is aware of the key change time, it is easy to take down the sensor normal job. To solve this problem, we can add a time sequence number of packets to ensure data freshness.Accessibilityis another very important challenge in WSN. Accessibility refers to providing WSNs service delivery at Denial of Service (DOS) attacks. DOS Attacks Can targets all layers of WSN and disables their Nodes. By DOS attack batteries or other power resources consume will be higher and much faster and causes failure in the nodes and networks. Usually for providing accessibility in WSN, the redundancy of sensor nodes is used [15].

2.2 MAC Protocols

MAC protocols main function is to arbitrate access of the communication medium and other resources of the networks. MAC protocol is a part of data link layers sub layer MAC layer. Number of protocols has been proposed so far by many researchers of the efficient utilisation of WSN resources. In next section we will give the classification and functioning of every protocol in brief.

2.2.1 CLASSIFICATION OF MAC PROTOCOLS FOR WSN

MAC protocols presented in the literature can be classified in two groups according to the approach used to manage medium access contention based and schedule based and a secure MAC protocol specifically designed to provide security at MAC layer protocols. Before discussing energy efficient MAC protocols that are specifically designed for WSN, some Traditional MAC protocols like ALOHA, CSMA, and CSMA/CD are there in which it is important to understand the mechanism of CSMA here and the reason why it cannot be used directly in WSN. Medium access control has been extensively studied for traditional wireless networks. A variety of MAC protocols have been proposed to address differentnetworks scenarios. From different perspectives, MAC protocols can be classified into different

categories, for example, centralized and distributed, single – channel based and multiple - channel based, contention based and contention free, and so on. Time division multiple access (TDMA), frequency division multiple access (FDMA), code division multiple access (CDMA), and carrier sense multiple access (CSMA) are typical MAC protocols that have been widely used in traditional wireless networks. However, these protocols do not take into account the unique characteristics of sensor networks, for example, denser levels of node deployment, higher unreliability of sensor nodes, and severe power, computation, and memory constraints. For this reason, traditional MAC protocols cannot be applied directly to sensor networks without modification. To design an efficient MAC protocol for sensor networks, the unique characteristics of sensor networks, in particular, energy efficiency and networks scalability must be taken into account. Moreover, delivery latency, networks throughput, bandwidth utilization, and fairness, which are the primary concerns in traditional wireless networks, should also be considered, but are of secondary importance in sensor networks [16].

2.2.1.1 CSMA Mechanism

Medium access control is critical for enabling successful networks operation in all shared - medium networks. The primary task of a MAC protocol is to arbitrate access to a shared medium or channel in order to avoid collision and at the same time to fairly and efficiently share the bandwidth resources among multiple nodes. Instead of using directly CSMA mechanism because of their disadvantage, high rate of collision, it is used in both contention based and schedule based protocols. In contention based protocol CSMA is used in basic data communication. Similarly in reservation based protocol slot requests are generally performed through CSMA.CSMA is a listen for transmit method. The functionality of CSMA is [17]. The node first listens to the channel for a specific time (IFS, inter frame space) and then work as follows

1. If the channel is idle the duration of IFS, the node may transmit the data.
2. If the channel becomes by during the IFS, the node defers the transmission and continues to monitor the channel until the transmission is over

2.2.1.2 Contention Based WSN MAC Protocol

Contention based medium access relies on controlled connection between nodes to set up communication links. It does not require any infrastructure. Each node tries to access the channel independently based on the carrier sense mechanism. But the problem with contention based MAC Protocol is collision probability increases with the increase in node density. In contention - based MAC, all nodes share a common medium and contend for the medium for transmission. Thus, collision may occur during the contention process. To avoid collision, a MAC protocol can be used to arbitrate access to the shared channel through some probabilistic coordination. Both ALOHA (Additive Link On - Line Hawaii System) and CSMA are the most typical examples of contention - based MAC protocols. In pure ALOHA, a node simply transmits whenever it has a packet to send. In the event of a collision, the collided packet is discarded. The sender just waits a random period of time and then transmits the packet again. In slotted ALOHA, time is divided into discrete timeslots. Each node is allocated a timeslot. A node is not allowed to transmit until the beginning of the next timeslot. Pure ALOHA is easy to implement. However, its problem is that the channel efficiency is only ~ 10% [18]. Compared with pure ALOHA, slotted ALOHA can double the channel efficiency. However, it requires global time synchronization, which complicates the system implementation. Some important contention based MAC protocols are.

2.2.1.2.1 TRAMA (Traffic-Adaptive MAC protocol)

TRAMA is a schedule based energy efficient collision free protocol. It is based on time slot structure and uses distributed election scheme. The pair wise communication between neighbours is performed to schedule transmission slots. TRAMA consists of four main phases. Neighbourhood discovery through NP (neighbourhood protocol), Traffic information exchange through SEP and AEA (Schedule exchange protocol and adaptive election algorithms), and data transmission [19].

TRAMA increases the energy efficiency by increasing the time spent in the sleep mode. In addition TRAMA decreases the collision rate. However significant amount of end to end delay is occurred. Frame length is directly proportional to end to end delay, so by optimizing frame size end to end delay can be reduced. Still collision

is possible, since TRAMA uses only information on one hop neighbours, hidden terminal problem can cause collisions in the networks.

2.2.1.2.2 PAMAS (Pattern Based MAC)

Pattern based MAC is enhancement of TRAMA, a schedule based protocol. In this protocol schedule is determined on the basis of global information exchange. The collision probability of data is zero in this protocol that increases the energy efficiency in the low traffic networks. Still collision of schedule reservation message packets is possible, and exchange of global messages for schedule reservation will incur heavy traffic the networks. Another kind of reservation based protocol that is classified under the TDMA based protocol which uses TDMA as the schedule reservation method [20].

2.2.1.2.3 Energy Aware TDMA based MAC protocol

Energy aware TDMA based MAC protocol is based on the formation of clusters and gateways. In this protocol, cluster head is elected based on the power level and range of the node. Gateway performs all the tasks. Gateway collects the data and send to another node within the cluster. Gateway is also responsible for slot assignment. The protocol operates in four phases IE data transfer, refresh, event based rerouting, and refresh based rerouting. For the slot assignment two techniques breadth first and depth first is used. Energy consumption in Energy Aware TDMA based protocol is reduced up to a certain level, but the problem arises due to clustering mechanism latency is increased and hence throughput of the networks decreases [21]. BMA MAC is the advancement of this protocol. Which works in two phases 1st is a cluster setup phase and 2nd steady state phase. In cluster setup phase cluster head (CH) is selected based upon available energy of nodes [22].

Steady state phase is used in each cluster. In which data period is split into two parts that is a data transmission period (fixed duration) and idle period. Slots are assigned here on demand. Whenever a node has to send data it will make a request to the CH by 1bit message. And after assignment of slot to the node, it will send the data in its own slot. We have categorized another kind of MAC protocol that is secure MAC protocol. In this category many protocols have been proposed so far. Our focus is to handle the node cloning attack. Here we will compare the protocol which is only related to node capturing attack [31].

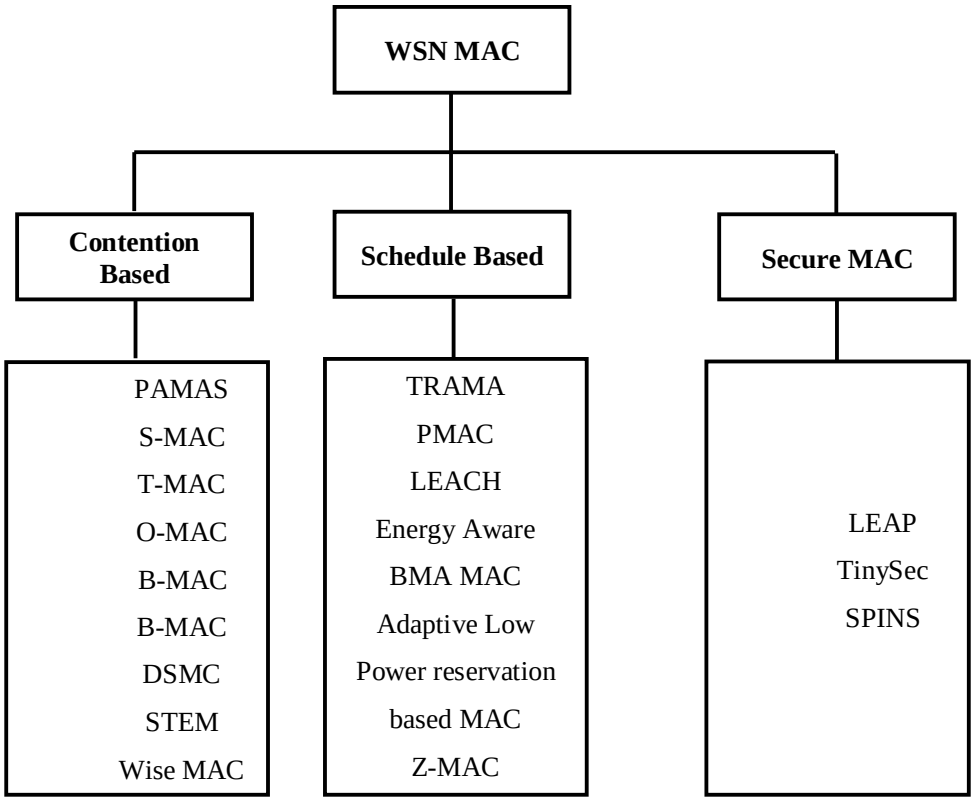

Fig-2.4 Classification of WSN MAC protocols

2.2.1.3 Schedule Based MAC Protocol

Protocol arbitrates medium access by finding a schedule to transmit, receive or active inactive. In a schedule based model of MAC protocols, energy wastage due to collision is reduced up to a certain level, but the disadvantage of schedule based protocol is the latency that occurred due to the synchronization of schedule. Much of the schedule based protocol uses local schedule synchronization which incurs the increase in delay of sending a frame. Some important schedule based protocol will be discussed ere and will be compared with their category of protocols on different parameters.

2.2.1.3.1 PAMAS (Power aware Multi-Access signalling)

PAMAS is a contention based MAC protocol. It is designed with the main objective energy efficiency. It works on two different channels for data and control packets, which makes it more costly and complex in design. In this protocol node goes to sleep mode which are neither transmitting nor receiving the data [23].

2.2.1.3.2 S-MAC (Sensor MAC)

Figure-2.5 shows the operation of S-MAC protocol. Sensor MAC is a contention based MAC Protocol in which a Sensor node periodically goes to a fixed listen/sleep duty cycle. For example in Fig-2.5 Node-1 wants to send data to node2.for that it firstly exchange control packets to all the Neighbouring nodes. And then send data to specific node, in the meantime other neighbour nodes goes to sleep mode.

Still a lot of energy is wasted due unnecessarily exchange control messages and idle listening to all the neighbouring nodes. Many protocols have been proposed to improve the energy inefficiency of S-MAC protocol such as T-MAC (Timeout MAC), Optimized MAC. Optimized MAC gives better performance in terms of energy efficiency in which duty cycle varies according to the traffic on the networks, and the networks load is identified by the number of messages in a queue pending at a particular node [24].

2.2.1.3.3 T MAC(Timeout MAC)

Fig-2.6 shows the operation of T-MAC protocol. T MAC protocol also known as timeout MAC protocol is based on S- MAC protocol. In T-MAC protocol, Sensor nodes go to sleep mode if no events (sending or receiving) has occurred from Ta amount of time as shown in Fig-3.4. The time Ta is a minimal idle listening time, it is also called timeout of T-MAC protocol. Ta>Tci + Trt + Tta + Tct, where Tci is length of contention interval, Trt is the length of RTS packet, Tta is Turnaround time, and Tct is the length of CTS packet. The comparison done between S-MAC and T-Mac protocol is based on two important parameters first is the average energy consumption and secon is the average latency of a packet sent.

Average energy consumed in T-MAC protocol is less than the S-MAC protocol because in T-MAC protocol nodes are idly active for short interval of time as compared to S-MAC protocol. The latency in T-MAC protocol is higher than the S-MAC protocol, this is an overhead of T-MAC protocol [25].

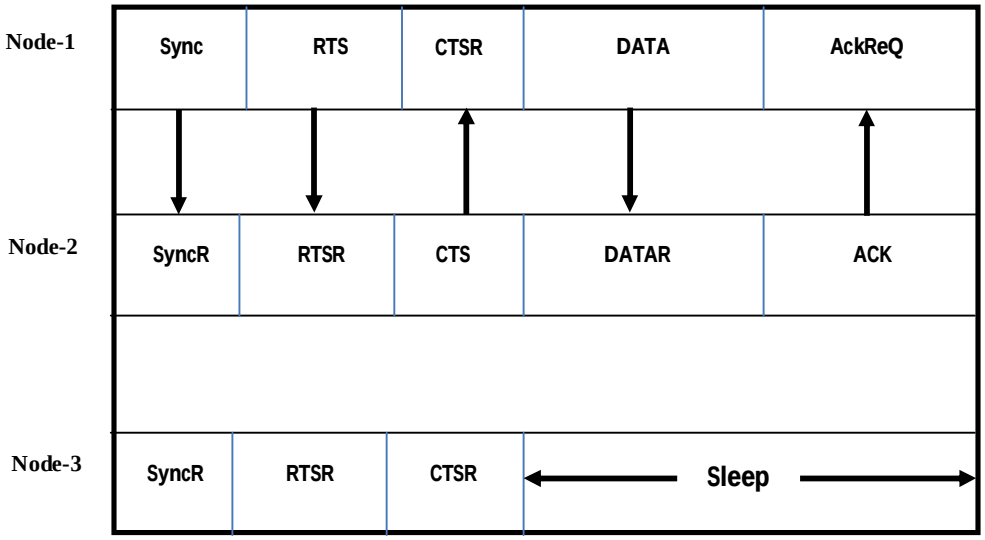

Fig-2.5 Working of S-MAC Protocol

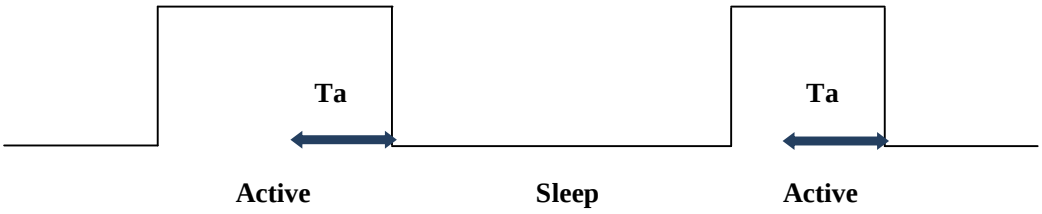

Fig-2.6 Working of T-MAC protocol

2.2.1.3.4 Optimized MAC

In the Optimized MAC protocol [5], the sensors duty cycle is changed based on the networks load. If the traffic is more than the duty cycle will be more and for low traffic the duty cycle will be less. The networks load is identified based on the number of messages in the queue pending at a particular sensor. The control packet overhead is minimized by reducing the number and size of the control packets as compared to those used in the S-MAC protocol. This protocol may be suited for applications in which apart from energy efficiency there is need for low latency [26].

2.2.1.3.5 B-MAC (Berkley-MAC)

B-MAC is advancement of S-MAC. In this protocol overhead of sending 4 control messages before sending every data packet is reduced by sending a preamble. B-MAC is a good protocol for low traffic networks. But if traffic on the networks increases, sending preamble before every message transmission is an overhead. And thus preamble may be involved in a collision that may cause energy wastage [27].

CCA mechanism in B-MAC is used to reduce the interference and noise from the medium. It is more energy efficient for the duration of no traffic. The preamble sampling technique may be more costly than sleep\active schedule protocol for high traffic networks [28]. Another protocol is CC-MAC which is based on removal of spatial correlation. Removal of spatial correlation will reduce the overhead of sending the same data by many sensor nodes. DSMAC is another Schedule based protocol which works on packet loss due to long queues and congestion control [29]. The main motive of the DSMAC protocol is to minimize the medium Access delay that may occur due to high traffic rate.

2.2.1.3.6 STEM (Sparse topology and energy management)

A problem with basic preamble sampling technique is node has to mind the whole preamble even if he fires up-up in the centre, or at the starting of preamble. Stem requires two radio channels. A separate channel for wakeup packet. In this protocol, instead of sending long preamble, a node sends a small wakeup packet. Recipient node of wakeup packet listens and replied with the small wakeup packet. After packet exchange transmitter will start sending data. If we denote the preamble length Tp, using the basic preamble sampling mechanism a transmitter node will take Tp time before sending every data packet. Wake up a time in STEM reduces this time to Tp/2 [30].

2.2.1.3.7 Wise MAC

Wise MAC solves the problem of energy wastage due to unnecessary sending the preamble and loosing energy wile every de ha affixed wakeup schedule. This scheme schedules the start of preamble packet, and saves [31]. The WiseMAC medium access control protocol was developed for the “WiseNET” wireless sensor networks. This protocol is similar to Spatial TDMA and CSMA with Preamble Sampling protocol [32] where all the sensor nodes have two communication channels. TDMA is used for accessing data channel and CSMA is used for accessing control

channel. However, WiseMAC needs only one channel and uses non-persistent CSMA with preamble sampling technique to reduce power consumption during idle listening. This protocol uses the preamble of minimum size based on the information of the sampling schedule of its direct neighbours. The sleep schedules of the neighbouring nodes are updated by the acknowledgement message (ACK) during every data transfer. WiseMAC is adaptive to the traffic loads and provides low power consumption during low traffic and high energy efficiency during high traffic. The simulation results show that Wise MAC performs better than S-MAC protocol.

2.2.1.4 Secure MAC protocol

For many sensor networks, security is a big issue like military applications of WSN need high level of security, in which the biggest IE is node capturing attack. Nodes are deployed in hostile environment, so if a node is captured, by using the information contained in that node, all types attack possible in WSN are now becoming easier for an attacker, and is called node cloning attack. One of the protocols that take care about the node capturing is LEAP.

2.2.1.4.1 Localized Encryption and Authentication protocol

In this protocol each sensor uses four different keys. Individual key is a shared key between base station and sensor. Group key is shared between all the sensor and base station. Pair wise key is shared between two sensors. Cluster key is shared between neighbours of the sensor. Leap protocol uses a multi-broadcast authentication protocol like μ**TESLA.** It has loose synchronization and delayed authentication problem. LEAP is used to defend against node capture attack as well as it is protects from the intrusion in the networks [33].

Comparative analysis of energy efficient MAC protocols is given by the Table - 1 in which comparison is done on the basis of various parameters like collision, latency, scalability, networks throughput, etc.

2.3 Types of Attacks in Wireless Sensor Networks

A Wireless sensor networks is a collection of a large number of sensor nodes which have limited amount of resources. Nodes in Wireless sensor networks have limited power source, memory and computation capability. These limitations are due to limited energy and physical size of the sensor nodes. Due to these constraints, it is

hard to directly use the conventional security mechanisms in WSNs.In order to optimize the conventional security algorithms for WSNs, it is necessary to be mindful about the constraints of sensor nodes [34].

The major constraints of WSN are

- WSN has limited amount of power sources so, we cannot deploy complex security mechanism as used in other networks for higher level of security.
- Sensor nodes are a small device, which has a very less memory. Sensor networkscant not hold the memory requirements for setup of higher level security model for networks. In the SmartDust project, for example, TinyOS consumes about 4K bytes of instructions, leaving only 4500 bytes for security and applications (Hill et al., 2000). A common sensor type- TelosB- has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage. The current security algorithms are therefore, infeasible in these sensors [35].
- Unreliable communication is another serious issue for wirless sensor networks security. WSN uses broadcast\ multicast mechanism for communication inside a networks that is very easy for eavesdropping and modification of data.

2.3.1 Physical layer attacks of WSN

Since the use of technology of wireless communication in WSN, it is easily to incur jamming attack from attackers in physical layer. Moreover, physical access to the sensor node is possible because of the placement of sensor nodes in an unguarded environment. Therefore, an intruder may be able to tamperor damage with the sensor devices.

2.3.1.1 Jamming

As a well-known attack to wireless communications, jamming is one of many exploits used compromise the wireless environment. Jamming can be a huge problem for wireless networks, since radio frequency (RF) is essentially an open medium. Jamming can disrupt wireless transmission. And it can occur either unintentionally in the form of interference, noise or collision at the receiver side or in the context of an attack. Even sporadic jamming can be sufficient to cause disruption because the communication data carried by the networks may be available for only a short time [36]. This attack is very effective for single frequency networks. Adversaries can

disrupt the networks through launch radio waves near the frequency point, as long as they get the centre frequency of communication frequency. Conventional defence techniques against physical layer jamming rely on spread spectrum, which can be too energy consuming to be widely deployed in resource constrained sensors.

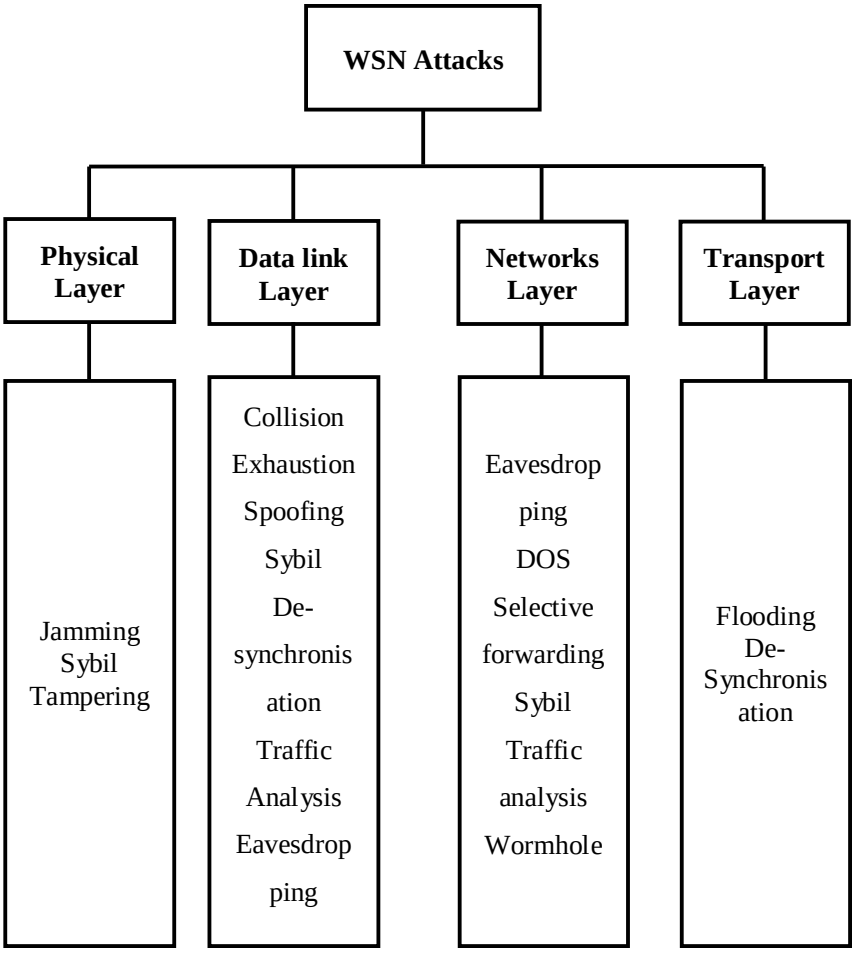

Fig-2.7 Classification of WSN security Attacks

Mobile-phone networks generally use code spreading as a defence against jamming. In addition, when jamming is intermittent, nodes may be able to report the attack to the base station by sending a few high-power and high-priority messages. In order to maximize the probability of successfully delivering such messages, nodes should cooperate with each other, for example, switching to a prioritized transmission scheme that minimizes collisions. Nodes can also buffer high-priority messages indefinitely so as to relay them once a gap in the jamming occurs.

2.3.1.2 Tampering

An adversary can tamper with nodes physically, and interrogate and compromise them, which aggravates the threats of large-scale sensor networks. However, it is unpractical to control access to hundreds of nodes spread over several kilometres. Furthermore, an attacker may be able to destroy or replace the sensor and computational hardware, even extract sensitive materials such as encryption keys to get unlimited access to higher levels of communication. Therefore, such networks can fall prey to true brute-forcedestruction. Focused on the dangers discussed above, one countermeasure called tamper proofing is presented. Tamper-proofing is a method used to hinder, deter or detect unauthorized access to a device or circumvention of a security system. When possible, the node should respond to tampering in a fail-complete manner. For example, it could cryptographic or erase program memory. There also are many other traditional physical defences such as camouflaging, hiding nodes and so on [37].

2.3.2 Data link Layer attacks of WSN

The link or Media Access Control (MAC) layer provides channel arbitration for neighbour-to-neighbour communication. Cooperative schemes that depend on carrier sense, which let nodes detect if other nodes are transmitting, are particularly vulnerable to all kinds of attacks. For example, collisions and unfairness at the link layer may be able to delay the packet transmission or cause the packet to be corrupted [38].

2.3.2.1 Collision

Collision is a kind of attack which can be easily launched by a compromised (or hostile) sensor node. In a collision attack, an attacker node does not follow the medium access control protocol and cause collisions with neighbour node's transmissions by sending a short noise packet. This attack does not consume much energy of the attacker but can cause a lot of disruptions to the networks operation. It is not trivial to identify the attacker due to the wireless broadcast nature. Adversaries may be able to disrupt an entire packet only need to induce a collision in one octet of a transmission. These malicious collisions which create a kind of link-layer jamming

can be identified by the networks to use collision detection. However, this approach cannot completely effective defence this attack. Proper transmission still requires cooperation among nodes, which is expected to escape corruption of others' packet. A subverted node could repeatedly and intentionally deny access to the channel, expending much less energy than in full-time jamming [39].

2.3.2.2 Unfairness

This threat may not entirely prevent legitimate access to the channel and the use of small frames means that the channel is only captured for a small amount of time. However, the adversary could cheat by quickly responding when needing access while other nodes delay, for example, causing users of a real-time MAC protocol to miss their deadlines. One method of defending against this threat is to use small frames so as to an individual node can only capture the channel for a short time. Nevertheless, this approach increases framing overhead if the networks typically transmits long messages. Furthermore, when vying for access, an attacker can defeat this defence by cheating, such as by responding quickly while others delay randomly [40].

2.3.2.3 Exhaustion

Exhaustion attempts retransmission repeatedly, even when attracted by an unusually late collision, such as a collision induced near the end of the frame. In nearby nodes, this threat could culminate when the battery resources was exhausted. A self-sacrificing node could develop the interactive nature of most MAC-layer protocols in an interrogation attack. For example, IEEE 802.11 which based MAC protocols uses request-to-send (RTS), clear-to-send (CTS), and Data/ACK messages to transmit data and reserve channel access. The node could elicit a CTS response from the targeted neighbour and repeatedly request channel access. Constant transmission would finally exhaust the energy resources of both nodes. One countermeasure to prevent this attack is to makes the MAC admission control rate limiting, so that the networks can ignore excessive requests without sending expensive radio transmissions. Nonetheless, this limit cannot drop below the expected maximum data rate the networks supports. One design-time strategy for protection against battery-exhaustion attacks limits the extraneous responses the protocol

requires. Designers usually code this capability into the system for general efficiency, but coding to handle possible attacks may require additional logic [41].

2.3.3 Networks Layer attacks of WSN

Networks layer attacks are a significant and credible threat to wireless sensor networks. This layer provides a critical service. Before reaching their destination, messages may pass through a lot of hops in a large-scale deployment. Unfortunately, as the aggregate networks cost of relaying a packet increases, the probability of the dropping or misdirecting packet along the way in the networks increases as well [42].

2.3.3.1 Homing

In the majority of sensor networks applications, some nodes will have special responsibilities, for example, they are elected the leader of a local group for coordination. More powerful nodes might serve as cryptographic key managers, monitoring access points or query, or networks uplinks. Because these nodes provide critical services to the networks, they often attract an adversary's interest. Location-based networks protocols that rely on geographic forwarding expose the networks to homing attacks. Here, a passive adversary learns the presence and location of critical resources by observing traffic. Once found, its collaborators or mobile adversaries can attack these nodes by using other active means. One effective approach to hiding significant nodes provides confidentiality for both message headers and their content. The networks can encrypt the headers at each hop supposing that all neighbours share cryptographic keys. This would prevent a passive adversary from easily learning about the source or destination of overheard messages, if a node has not been subverted and remains in possession of valid decryption keys.

2.3.3.2 Neglect and greed

This threat is a simple form of attack arbitrarily neglects to route some messages to attacks the node-as-router vulnerability. In this kind of attack, the subverted or malicious node can still take part in lower-level protocols, and may even acknowledge reception of data to the sender, but it may refuse to forward packets or drop them on a random or arbitrary basis. Also, it can forward to packet to wrong receiver and gives undue and high priority to its own messages, so as to destroy the networks communication rule. Furthermore, the dynamic source routing (DSR) protocol [43] is susceptible to this attack. Communications from a region may all use the same route

to a destination as the networks caches routes. If a node along that route is greedy, it may consistently degrade or block traffic from the region to a base station. Multipath routing can be used to counter this type of attack. Messages routed over *n* paths whose nodes are completely disjoint are completely protected against neglect and greed attacks involving at most *n* compromised nodes and still offer some probabilistic protection when over *n* nodes are compromised. The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information. Allowing nodes to dynamically choose next hop from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow. Sending redundant messages is effective countermeasure. It is difficult to distinguish a greedy node from a failed node, however, so prevention is safer than relying on detection.

2.3.3.3 Misdirection

Misdirection is based upon changing, spoofing, or replaying the routing information. By forwarding the message along with the wrong path or by sending false routing updates can lead to this kind of attack. This attack targets the sender and diverts traffic away from its intended destination. Moreover, by misdirecting many traffic flows in one direction, this attack can target an arbitrary victim. In one variant of misdirection, Internet smurf attacks, the attacker forges the victim's address as the source of many broadcast Internet control-message-protocol echoes and directs all echo replies back to the victim, flooding its networks link. A sensor networks that based on a hierarchical routing mechanism can use a method similar to the egress filtering in Internet gateways, which can help prevent smurf attacks. By verifying the source addresses, parent routers can verify that all routed packets from below could have been originated legitimately by their children.

2.3.3.4 Black Holes

Distance-vector-based protocols [44] provide another easy avenue for an even more effective attack. Nodes advertise zero-cost routes to every other node, forming routing black holes within the networks. As their advertisement propagates, the networks routes more traffic in their direction. In addition to disrupting message delivery, this causes intense resource contention around the malicious node as

neighbours compete for limited bandwidth. Theseneighbours may themselves be exhausted pre-maturely, causing a hole or partition in the networks [45].

2.3.4 Transport Layer Attack of WSN

Transport layer manages end-to-end connections and this layer is needed when the sensor networks intends to be accessed through the Internet. The service the layer provides can be as simple as an unreliable area-to-area any cast, or as complex and costly as a reliable sequenced-multicast byte stream. Sensor networks tend to use simple protocols to minimize the communication overhead of acknowledgments and retransmissions. The transport layer can be attacked via flooding or DE synchronization [46].

2.3.4.1 Flooding

The aim of flooding attacks is to exhaust memory resources of a victim system. Similar to TCP SYN flood, the attacker sends many connection establishment requests, forcing the victim to allocate memory in order to maintain the state for each connection. Limiting the number of connections prevents complete depletion of resources, which would interfere with all other processes of the victims. However, because the queues and the tables fill with abandoned connections, this method prevents legitimate clients from connecting to the victim as well. Connectionless protocols can naturally resist this type of attack a little, but they may not provide adequate transport-level services for the networks.

Client puzzles are a typical way of reducing the severity of flooding attacks by asking all client nodes to demonstrate their commitment to the resources they require. The server can easily create and verify the puzzles. While clients are solving the puzzles, the storage of client-specific information is not required. Servers distribute the puzzle, and clients solve and present them. If the clients hope to connect, they must solve and present the puzzle to the server before receiving a connection. Therefore, an attacker mustbe able to take more calculated resources per unit time to flood the server with effective connections. Under heavy load, the server measure the puzzles, and learn need work of potential clients. This solution is most suitable for combating adversaries that possess the same limitations as sensor nodes. The downside is that legitimate nodes now have to expend extra resources to get connected, but it is less costly than wasting radio transmissions by flooding.

2.3.4.2 DE synchronization

DE synchronization can disrupt an existing connection between two end points. In this attack, the adversary forges messages between endpoints. These messages carry sequence numbers or control flags that lead to the end points request retransmission of missed frames. If the adversary can maintain proper timing, it can hinder the end points from exchanging messages as they will be continually requesting retransmission of previous erroneous messages. Also, this attack leads to an infinite cycle that wastes energy. This threat is typically countered by authenticating all packets exchanged, including all control fields in the transport protocol header. And then the endpoints can detect and ignore the malicious packets, assuming the adversary fails to forge the authentication mechanism.

We have considered our problem statement for the detection of node clone attack. Node clone is not any type of specific layered attack. Because it is a kind of physical layer attack in which attacker initially captures the nodes, and steal the data inside the node. By using that stolen data of authenticated node, attacker makes fake replicas of that node and deploys in the target region. Now that fake node will start working as authenticated node because it has all the original data inside the node. As this fake node is in control of attacker, he can deploy any type of attack inside the networks. So detecting these kinds of fake nodes, also called clone detection is a very critical issue in wireless sensor networks [47].

2.4 Classification of Node clone Detection Algorithms

A wireless sensor networks is a group of nodes organized in to a wireless networks. Such networks are prone tomultiple attacks due to poor security. One of the attacks is node clone attack in which adversary or attacker captures somenodes from networks and replicates them including the cryptographic in formation and deploys them in the networks. Previousworks against node clone attacks suffer from either a high communication or storage overhead or poor detection accuracy. Insection, we classify the types of algorithms have been proposed so far for the detection of node clones in wireless sensor networks. Several algorithms are developed to detect the node-clone attacks, in static WSNs and mobile WSNs. Each one has it’s their advantages anddisadvantages [48].

2.4.1 Centralized Techniques

We have classified the node clone detection techniques broadly into two categories that is centralised and distributed. Centralized clone detection is the most straightforward and simple detection technique. In centralized techniques the detection process every node in the networks sends its location claim to sink node through its neighbouring nodes. Receiving the entire location claims, the sink node checks the node Ids along their location, and if it finds two other locations with the same ID, it raises a replica node. The sink node is considered to be a powerful central which is responsible for information convergence and decision making. Although this approach is very simple, it suffers from several drawbacks that are associated with the centralized system. In centralized system sink node becomes the single point of failure. Any compromise of the sink nodes or the communication medium near the sink node will render this protocol inadequate. Another problem with the centralised technique is, the node closest to the sink node will receive burnt amount of routing traffic and becomes the primary and easy target for the attacker. Total delay in centralized technique will always be greater than the distributed techniques because the base station will wait for all the location claim coming from the WSN nodes deployed in a region. A distributed or local protocol could revoke the replicated node more quickly than the centralized techniques. Many networks do not have as much capable sink nodes which can analyse the data at a time, coming from all the nodes inside the region.

In terms of security, or detection level of the protocol, protocols based on centralised technique will achieve 100% detection level of all replicated nodes, assuming all the messages successfully reach the base station. Efficiency of these protocols is measured theoretically in terms of number of communication required which is $n\sqrt{n}$in centralised protocols.

2.4.1.1 Random key pre distribution

Random key pre distribution security schemes are well suited for use in sensor networks because of their low storage overhead. However, the security of networks using pre-distributed keys can be compromised by cloning attacks. Cloning gives the adversary an easy way to build an army of replica nodes that can cripple the sensor networks. Brooks proposed an algorithm that a sensor networks can use to detect the

existence of clones .Random Keys that are present on the cloned nodes are detected by looking at how often they are used to authenticate nodes in the networks.[49]

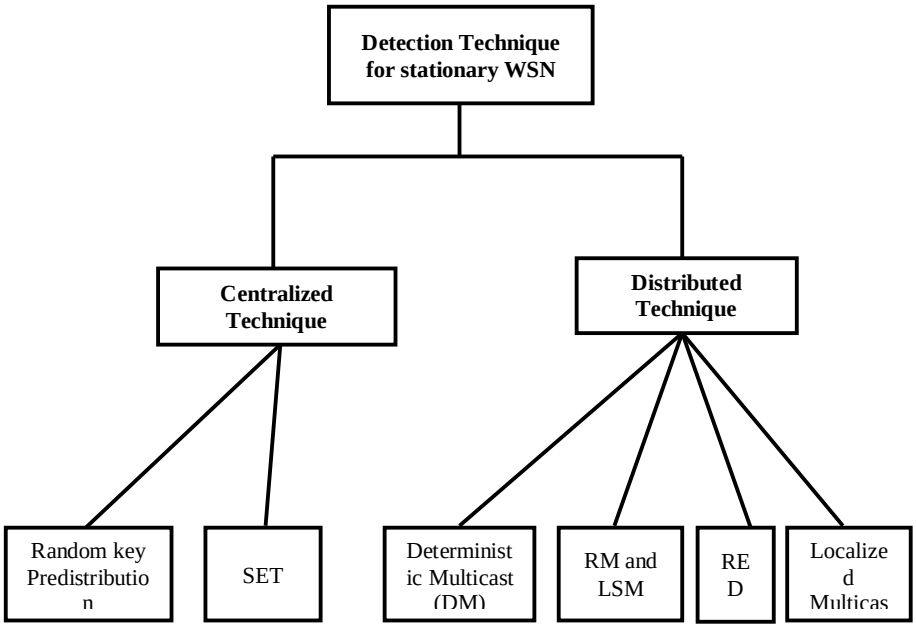

Fig-2.8 Categorization of Node Clone Detection Approaches

2.4.1.2 SET

SET is used to detect replicas by computing set operations of exclusive subsets in the networks, using localized voting mechanism, a set of neighbour nodes can agree on the duplication of a given node that has been replicated within the neighbourhood. This method fails to detect duplication nodes that are not within the same neighbourhood. This algorithm is used to reduce the communication cost of the preceding approach by computing set operations of exclusive subsets in the networks. SET then employs a tree structure to compute non overlapped set operations and integrates interleaved authentication to prevent unauthorized falsification of subset information during forwarding [50]. First, SET launches an Exclusive subset maximal independent set (ESMIS) algorithm which forms exclusive unit subsets among one-hop neighbours in an only one disjointed subset which are controlled by a head.

2.4.2 Distributed Techniques

To avoid the single source of failure in centralised techniques, we could rely on the local detection of clones in WSN. Using a voting mechanism, the neighbours can reach consensus on the legitimacy of a given node. While this type of local detection

will fails when we apply it in a distributed fashion for clone detection. As long as the replicated node is not at two hops away from each other, the local detection protocol cannot detect the replica. There is no essential rule exists, in distributed techniques and special detection mechanism called claimer reporter-witness frame work. Claimer reporter-witness frame work is provided in which the detection is performed by locally distributed node sending the location claim not to the sink node but to a randomly selected node called witness node.

2.4.2.1 Node to networksbroadcasting

This approach simply utilise the broadcast protocol for clone detection. Each node in the networks uses the authenticated broadcast protocol for the network's local information distribution. Each node stores the local information for its neighbour, and if it receives a conflict, revokes the offending node. This protocol has 100% detection level of all duplicate claims based upon the assumption that all the broadcasts reach every node. However this assumption could not be valid in many real life WSN applications. This protocol requires each node to store local information about its d neighbours. One location broadcast requires O(n) message. The total communication cost of this protocol is $O(n^2)$. After the analysis of this protocol it is verified by the author that it is justifiable for small networks, for large networks$O(n^2)$ factor is too high [51].

2.4.2.2 Deterministic Multicast (DM)

To improve the communication cost of previously proposed protocol, DM uses the technique of multicast instead of broadcast used in previous technique [52]. DM protocol is a claimer-reporter-witness framework. It is good example to explain claimer –report-witness frame work.. The claimer is a node which shares its location claim to its neighbour nodes, each neighbour node serving as a reporter. The reporter uses function to map the claimer ID to a witness node. Then the neighbour node forwards the claim to the witness. Witness will receive two different location claims for the same node ID if the adversary has replicated a node. There is a problem in Deterministic Multicast. If a replica knows the claimer's ID and function he/she will the witness's location. Then it compromises them before deploying his replication.

In this protocol, each node inside the networks, stores the average number of g location claims. At the time of communication suppose a number of neighbours do

not cooperate. Assuming an average networks path length of O($\sqrt{n}$) nodes, this results in O($\frac{g \ln g\sqrt{n}}{g}$) messages. This cost does not provide much security in WSN. Analysis of this protocol is, it is infeasible to spend so much of communication cost, without having a good security level [51].

2.4.2.3 Randomized Multicast (RM)

Randomized Multicast (RM) is first efficient protocol under the category distributed node replica detection mechanism. To reduce the communication cost of deterministic multicast protocol discussed in previous section, RM is proposed. To overcome the resiliency problem of deterministic multicast protocol, it will select the witness of the node randomly [51]. Deterministic protocol for node clone detection perform better in other scenario, but it suffers from the resilience that means attacker can easily anticipate the position of the witness nodes if we will selects the fixed witness nodes. In RM, when a node announces it location claims, each of its neighbours sends location claims to the set of randomly selected witness nodes.

In networks of n nodes, if each location claim produces $\sqrt{n}$ witnesses, then the birthday paradox [52] predicts at least one collision with high probability that means at least one witness will receive a pair of conflicting location claim, and detects the node clones. This protocol assumes that each node knows its location. They also assumes that the networks utilizes an identity based public key system such that each node a deployed with a private key, K_a^{-1}, and any other node can calculate a's public key. At a higher level, in this protocol each node broadcast its location claims with a signature which is used for the authentication of location claim. After this each of the node's neighbour will probabilistically broadcast the claim to a randomly selected witness nodes. If any one of these witness nodes receives two different location claims of the same id, it will identify that and revoke the replicated node. Birthday paradox insures that this algorithm will detects the replication with high probability using a relatively limited number of witnesses. In this protocol each witness node that receive a location claim will firstly verify the signature. Then it checks the id against all of the location claims it has received so far. If it ever receives two different location claims for same node id, then it detects the replication, and the two claims will works as the evidence for the replication and revocation. Now for the future it blacklist the node a from further communication by flooding these two location claim

among the networks. Thus this protocol detects and defeats the node replication attack in fully distributed manner.

This protocol gives a detection level up to 93% in specific networks assumptions. Unlike the deterministic protocol, here no longer need to worry about the adversary using a limited number of captured nodes for the unlimited amount of replication. As for as the efficiency of this protocol, it still suffers from high storage cost which is not acceptable in most of the wireless sensor networks application. On an average each node will have to store p .d .g number of location claims. To ensure the collision more than 50 % of location claim for detection, p .d .g will have to be the order of O ($\sqrt{n}$). Enhancements have been done in this protocol to overcome this problem, but still storage cost is high. If we try to reduce the storage overhead that will affects the communication cost and average energy consumed by the sensor nodes, which is not acceptable in wireless sensor networks because of the availability of limited resources.

2.4.2.4 Line Selected Multicast (LSM)

The second protocol, Line-Selected Multicast (LSM), exploits the routing topology of the networks to select witnesses for a node location. It utilizes geometric probability to detect replicated nodes [53]. In RM, each node broadcasts a location claim to its one-hop neighbours. Then, each neighbour node chose randomly witness nodes within its communication range and forwards the location claim with a probability to the nodes nearest to selection locations by using geographic routing.In this protocol the location claim travel from one node to another node. If we compared with RM and LSM has a lower communication cost. It has a many drawbacks.

A different scheme for the detection of clone is been proposed in this protocol to reduce the communication cost of randomized multicast protocol. In a sensor networks a sensor node function as both a sensing unit as well as a router. For a location claim to reach node b from a, it must pass through several intermediate nodes. If these intermediate nodes also store the location claim, then it draws alne of witness nodes inside the networks. If a conflicting location claim ever crosses this line then these nodes will detect the replication and revoke the replicated node by blocking that node for further communication and flooding this message in the whole networks. Since the expected number of intersection e of x randomly drawn lines intersecting within the bound of the unit circle is given by.[53]

$$E(c) = x(x-1)(\frac{1}{6} + \frac{245}{144\pi^2})$$

Only it is required a few such lines to ensure the intersection. For example with only three such lines it is expected two collisions. This protocol modifies the randomized multicast protocol, so that it fix p .d .g as a small constant. When a's neighbour send the evidence of a's location claim to the constant number of witnesses, each of the nodes along the route stores the copy of the location claim. This protocol draws line segments instead of lines through the networks. The probability of intersecting two line segment is less thann the probability of intersecting two lines. The two line segment will only intersect if a fourth point outside the triangle made by three point falls inside a convex region. Thus the probability of intersection is given by.

$$E(c) = x(x-1)(\tfrac{1}{6} + \tfrac{245}{144\pi^2}) = .235$$

Since only a constant number of line segments are used in this protocol, the line selected multicast protocol has very reasonable performance characteristics. If we assume average length of line segment is O ($\sqrt{n}$), then this protocol only requires O (n $\sqrt{n}$) communication for the entire networks and each node stores O ($\sqrt{n}$) location claims [53].

2.4.2.5 Randomized, Efficient and Distributed Mechanism (RED)

It combines both characteristics of DM and RM, but this protocol uses the witness chosen by pseudo-randomly on a networks-wide seed to improve networks performance and a distributed protocol to detect the node replication attack. .This protocol consist of two steps: In first step, a random value, rand, is shared between all the nodes in the networks. In second step, is the detection phase, each node broadcasts its claim ID and location to its neighbouring nodes. Each and every neighbour node that hears a claim sends (with probability p) to a set of g pseudo randomly chosen networks places [54]. The pseudo random function takes as an input ID, random number, and g. Each node in the path (from claiming node to the witness destination) forwards the data to its neighbour closest to the destination. It protects the witness nodes. The replicated node will be detected in every detection phase.

They have defined their own threat model, they have assumed that before a round of the replica detection protocol is run the adversary can compromise a certain fixed number of nodes and can replicate one or more into multiple copies. They have

taken the adversary such that it requires some time to move from one point of the networks area to another, while during the same time interval the ubiquitous attacker can capture nodes regardless of their localization. The main problem in detection of node clone is to select the replica. If the adversary knew the future witness nodes, before detection protocol executes, he can subvert these nodes such that the attack would go undetected. Designing protocol for wireless sensor networks is a challenging task due to the resource constraint associated with it. All protocols are required to impose little overhead of energy, memory etc. it is possible that overall overhead of networks in not high but if the subset of nodes faces higher overhead and other nodes that is a serius issue in WSN , because higher overhead nodes will dead after some time that reduces the performance and lifetime of the networks. That means for a high performing and higher life of the WSN, the overall load should be distributed fairly among all the nodes in wireless sensor networks.

RED executes for the fixed interval of time. As discussed above, each run of this protocol consists of two steps. In the first step a random value is shared among all the nodes in the networks through centralised broadcasting scheme. In the second step each node digitally signs and broadcast its location claims that contains the id and geographic location. For each node, each of its d neighbours will forward this location claim with a probability p to a g number of pseudo randomly selected witness nodes. RED can easily be adopted to work in case an id is randomly chosen as the message destination. They have assumed that the routing will deliver a message sent to a networks location to the node closest to this location that the routing protocol will not fail. That message forwarding is not affected by dropping or wormhole attack of the networks. In this protocol the probability of detecting the clone attack is equal to the probability that at least one neighbour will send the location claim to the witness node for both the nodes (original and clone). If we assume average number of neighbouring node is d, then the probability that a claim message will be sent from a neighbourhood to the given location is $1- (1-p)^{d.}$ So the detection probability is $(1-(1-p)^{d})^{2}$. In this protocol the witness nodes are selected using the Pseudorandom function. This function takes the input as id of the node that is the first argument of claim message, current rand value and the number g of location claim that have to be generated. Pseudorandom function used in this protocol guarantees that, given a claim, the witness for this claim are unambiguously determined for a given protocol iteration.

So overall in this protocol they have introduced a new model of adversary. The main contribution of this protocol is randomized, comparatively efficient and distributed protocol that is able to detect node clones in wireless sensor networks. Through simulation they have compared the protocol performance with the line selected multicast protocol. They proved that their overhead of memory and energy as introduced in this protocol is low and almost evenly distributed among the nodes while these properties are not provided in line selected multicast protocols [54].

2.4.2.6 Localized Multicast

There are two distributed protocols for detecting node replication attacks called Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC). In both protocols, the overall Sensor networks are split into cells to form a geographic grid. In SDC, every node ID is exclusively mapped to one of the cells in the grid. When executing detection method, every node broadcasts a location claim to its neighbour's node. Then, every neighbour forwards the location claim with a probability to an exclusive cell by executing a geographic hash function with the input of node ID [55]. Once a location claim received by the destination cell by any node, the location claim is flooded by the entire cell. Since the location claims of clone nodes will be forwarded to the same cell, hence the clone nodes will be detected with certain probability. Like SDC, in the P-MPC algorithm, geographic hash function is employed to map node identity to the destination cells. However, instead of mapping to single deterministic cell, in P-MPC the location claim is mapped and forwarded to multiple deterministic cells with different probabilities. The rest of the process is similar to SDC [55].

In this protocol they have considered the detection algorithm only for static wireless sensor networks. And the literature of all the protocols under the detection of node clones in wireless sensor networks are discussed above. Here it is necessary to understand some of the protocols for clone detection in mobile wireless sensor networks also. The node replica detection techniques developed for static WSNs do not work when the nodes are expected to move as in mobile WSNs. As a result some techniques have also been proposed for mobile WSNs. These techniques are improved to detect the replica node. These techniques are characterized into two main classes as centralized and distributed techniques. Here we discuss only limited number of

protocols under both categories to understand the concept of detection applied in mobile sensor networks system.

2.4.2.7 Sequential Probability Ratio Test (SPRT)

In mobile sensor networks each and every time a mobile node moves one location to another location, each of its neighbours asks for a signed claim containing its location and time interval information .It decides probabilistically whether to forward the received claim to the sink node. The sink node computes the speed from every two successive claims of a mobile node and performs the SPRT by taking speed as an observed sample. Each time maximum speed is exceeded by the mobile node; it will promote the random cross the upper limit and thus edge to the sink node accepting the alternate hypothesis that the mobile node has been replicated [56]. On the other hand, each time the maximum speed of the mobile node is not reached; it will promote the random cross the lower limit. The sink node accepting the null hypothesis that mobile node has not been replicated [56].

2.4.2.8 eXtremely Efficient Detection (XED)

eXtremely Efficient Detection (XED), it's against the node replication attack in mobile sensor networks. The idea behind XED is motivated from the observation that for the networks without clones, if sensor node i meets another sensor node j at earlier time and i sends the random numbers to j , i and j meets again and again , i can assertion weather this is the node j met before requesting the random number r [57]. This techniques developed to, challenge-and-response and encounter-number, are fundamentally different from the others. The two sensor nodes i and j within the communication ranges of each other, first it will generate the random numbers and it will exchange their generated random numbers. The generated random numbers and received random number in their respective memory. To generate the random number they use the cryptographic hash function to store the node value. Here the replica does not possess the correct random number. This node can be attributed to the fact that each node detects the replica by itself and will detect the replica at different time period. The XED scheme is composed of two steps: online step and offline step. In offline step security parameter cryptographic hash functions stored in each node. In online step if one u encounter v for the first time, u node randomly generates $\propto$, computesh ($\propto$), sends h($\propto$)to v .

2.5 Conclusion

This chapter includes the literature survey of both topics we have selected for our thesis. In first potion of this chapter we have discussed the mac protocols classification and working. We have discussed all the three type of MAC protocols that is schedule based, contention based and secure MAC protocols. As it is clear from the literature that traditional MAC protocols cannot be used in wireless sensor networks because of their consumption, memory and collision overhead. So schedule based and contention based protocol are basically designed to arbitrate theaccess of the networks bandwidth and communication channel. While secure MAC protocols is basically for providing security at link layer by the intrusion, DOS and replay attacks. Final comparison of these MAC protocols and conclusion based upon their application specific usage is given in the next chapter. Next portion of this chapter includes the literature survey of node clone detection technique which includes the centralized and distributed techniques both. Distributed techniques of node clone detection drawn the attention of researcher for their advantages of arbitration of load between all the nodes that increase the life time of the networks. We have proposed a witness based technique for node clone detection which uses a fixed set of witnesses to detect the node clone. In chapter number five we have discussed all the details of our proposed methods for detecting node clone in wireless sensor networks.

CHAPTER 3
COMPARATIVE ANALYSIS OF MAC PROTOCOL

3.1 Introduction

Wireless sensor networks are practiced in many real life applications such as military, weather forecasting, medical, target spotting etc. The sensor nodes are spread over the target area for the accumulation of data. Collected data further transmitted from one sensor node to another sensor node towards the base station. Transmitted data involve texts, images and videos also, that creates huge traffic on the networks. If traffic increase into the networks, it will creates the problem of collision. Collision is the basic problem of networks that may be handled by the MAC protocols used at data link layer. Wireless sensor networks have limited amount of resources in terms of networks bandwidth, power, memory and computation capability. Efficient utilisation of these resources will increase the performance and lifetime of the wireless sensor networks, it can be practised by selecting best suitable MAC protocol for specific WSN application.

WSN has drawn so much attention of researcher from the last ten years because of their real life useful application in almost every field. And MAC layer is always a good idea to work for increasing the performance and durability of WSN. In this chapter we have included some secure MAC protocols of wireless sensor networks that provide protection against intrusion, node capturing and replay attacks. Energy efficient MAC protocols play a critical role in overall energy consumption of wireless sensor networks.

This chapter includes the basic challenges of MAC layer in wireless sensor networks. In first portion of this chapter we have explained the basic ideas and attributes required to consider for designing a good MAC protocol. Since power consumption is the basic and serious issue of wireless sensor networks that can be minimised by using better MAC protocols. In next section of this chapter we have discussed the major sources of energy wastage at data link layer of wireless sensor networks. Once we have designed the MAC layer protocol, we have to test this

protocol for the efficiency and unfair communication in wireless sensor networks. In following section of this chapter we have discussed the parameters on which we check the accuracy and adoptability MAC protocols. Last section of this chapter includes the comparison chart of all existing MAC protocol on the basis of parameters classification, collision, overhearing, idle listening, latency, scalability and throughput. In conclusion section we have concluded this chapter by comparing and analysis given on the basis of application specific usage of WSN MAC protocols.

3.2 Attributes of a Good MAC protocol

MAC protocols main objective is to achieve error-free communication in the networks. Errors at data link layer can be either caused by collision, or due to node failure in WSN. To design the good MAC protocol for WSN energy efficiency should be firs concern for the developer. Other main attributes of a good MAC protocols are latency, throughput fairness and security [59].

3.2.1 Energy efficiency

Usually in wireless sensor networks batteries are provided by button battery or dry battery. Wireless sensor networks are deployed in a hostile environment having limited source of energy. Many of WSN application battery is very critical for the continuous functioning of the networks because it cannot be renewed in a short interval. Even in some of the application it is impossible to change the battery so efficient utilization of power source should be primary concern in designing of wireless sensor networks protocols.

3.2.2 Latency

The second important parameter is latency. The networks performance basically depends upon the latency because of the fast processing requirements of the application. Real time application of wireless sensor networks needs to transfer the data in real time when collected towards the sink node. All the data collected at a node are sent to the sink node so that immediate action should be taken a sink. Latency basically depends upon the traffic in the networks, collision and bandwidth of the networks.

3.2.3 Throughput

Throughput requirement is also dependent upon the application. Some sensor application requires more data for that application throughput should be high. Throughput is an important parameter to analyse the performance of the networks. In most of the networks used for the networks data transfer if the throughput is high networks is assumed to be better. In Wireless sensor networks throughput requirement varies according to the application for example in some of the military application that are mission critical tasks, throughput should be high. Maintaining high throughput in the networks will affect the othe parameters of the nodes also, for example it will requires higher bandwidth, complex algorithm to secure the data from different attack. That will consumes more average energy per node.

3.2.4 Fairness

It is necessary to ensure that the sink node is receiving data from at the node fairly in low bandwidth WSN. Fairness can be important parameter to achieve the quality of service in the networks. For example in Military applications quality of service should be high so, fairness should also be high that means all nodes will share the bandwidth of the networks in a equally likely manner. If some of the nodes from critical area can't communicate very well to the sink node due to the unfair protocols used at MAC layer that will cause big problem for the networks. But in most of the WSN application energy efficiency and throughput are the major parameter to analyse the MAC protocols for WSN.

3.2.5 Security

WSN MAC protocol needs to secure for any application of WSN. Since the nodes are not so wealthy in terms of resources, therefore complex algorithms cannot be played over it. Security is the main preconcert to socialize this networks for common usage. For making the WSN secure, cryptography plays an important role. There are many algorithms proposed so far: symmetric, asymmetric and hybrid. But complex algorithms, which had been proposed for MANETs, are not successful over WSN. Unsecure MAC protocol can cause to energy wastage as well as many attacks that are possible into the WSN due to the vulnerability of attacks.

3.3 Major Sources of energy Wastage at MAC Layer

As mentioned earlier, energy efficiency is the primary concern of WSN design. In general energy consumption occurs in mainly three phases that is Data sensing, data processing and data communication. In other words, major sources of energy wastage in WSN are collision, exchange of control packets, Overhearing, and idle listening. For the WSN handling of idle listening is more important because nodes are kept alive even when the node has neither data to send or receive. When developing a new protocol we have kept in mind about all these sources of energy wastage as well as the security level of the protocol. The attacker can make the protocol more than worse if not secure, by simply DOS (jamming) attack. So in spite protocol being energy efficient it must be secure enough to WSN attacks [59].

3.3.1 Collision

At data link layer major source of energy wastage is collision. Collision occurs when two sensor nodes transmit their packets at the same time. As a result, the packets are corrupted and thus have to be discarded. Retransmissions of the packets increase both energy consumption and delivery latency. At data link layer major attack like denial of service and jamming attacks works on collision. Attacker creates too much traffic on the networks that keeps busy the networks resources all the time.

3.3.2 Overhearing

The second major source of energy wastage at data link layer is overhearing. Overhearing occurs when a sensor node receives packets that are destined for other nodes. Overhearing such packets results in unnecessary waste of energy and such waste can be very large when traffic load is heavy and node density is high.

3.3.3 Packet Overhead

The third source of energy wastage at data link layer is control packet overhead. A MAC protocol requires sending, receiving, and listening to a certain necessary control packets, which also consumes energy not for data communication.

3.3.4 Idle listening

The other source of energy wastage at data link layer is idle listening i.e., listening to receive possible traffic that is not sent. Idle listening occurs when a sensor

node is listening to the radio channel to receive possible data packets while there are actually no data packets sent in the networks. In this case, the node will stay in an idle state for a long time, which results in a large amount of energy waste. However, in many MAC protocols, for example, IEEE 802.11 ad hoc mode or CSMA, a node has to listen to the channel to receive possible data packets. There are reports that idle listening consumes 50 – 100% of the energy required for receiving data traffic. For example, Stemm and Katz [58] reported that the idle: receive: send ratios are 1 : 1.05 : 1.4, while in the Digital 2 - Mbps wireless LAN module (IEEE 802.11/2 Mbps) specification the ratios are 1 : 2 : 2.5.

3.4 MAC Performance Matrices

In order to evaluate and compare the performance of energy conscious MAC protocols, the following matrices are been used by many research groups [60].

3.4.1 Energy Consumption per Bit

The energy efficiency of the sensor nodes can be defined as the total energy consumed or total bits transmitted. Lesser the number, the better is the efficiency of protocol in transmission of the information of the networks. This performance matrix gets affected by all the major sources of energy wastage in wireless sensor networks such as idle listening, collision, control packet overhead and overhearing.

3.4.2 Average Delivery Ratio

Average packet delivery ratio shows the loss of data packets in the route. Collision is the main reason of the loss of average packet delivery ratio. The average packet delivery ratio is the number of packets received to the number of packets sent averaged over all the nodes. Large number of sensor node are deployed in a target region to gather the data in many cases there data are highly correlated. So up to a threshold level loss op packet delivery ratio will not affect the overall performance of the networks. In WSN mission critical application packet delivery ratio is very important parameter to analyse the performance of the WSN.

3.4.3 Average Packet Latency

The average packet latency is the average time taken by the packets to reach to the sink node. Average packet latency is a key parameter for performance analysis of

any networks. If a packet will takes more time to route it will take more number of hope and more bandwidth in the networks. Average packet latency will affects the networks in both ways quality of service as well as shortening of networks life time.

3.4.4 Networks Throughput

The networks throughput is defined as the total number of packets delivered at the sink node per unit time.

In Tabale-3.1 we have compared all the existing MAC protocols, i.e. schedule based, contention based and secure MAC on the basis of parameters, collision, overhearing, idle listening, latency, scalability, node lifetime and throughput. These parameters are very important to analyse the performance of MAC protocols. On the basis of these parameters comparison we will analyse the performance later.

Table-3.1 Comparison chart of WSN MAC Protocols

S-no	Protocols	Collision	Overhearing	Idle listening	Latency	Scalability	Node life-time	Networks throughput
1	CSMA	High	High	High	High	Not scalable for WSN	Less	Very Low
2	PAMAS	High	Low	Low	High	Very low	>CSMA	Low >CSMA
3	S-MAC	High	Low<PAMAS	Low	LOW	Very low	>PAMAS	Low
4	Optimized MAC	High	Very Low<<S-MAC	Very Less<<s-MAC	LOW	For latency is not a concern	>S-MAC	LOW
5	B-MAC	High	Very Low	Low	Yes(Low)	Scalable for WSN with Low traffic	Good	Good
6	CC MAC	High	Low	Low	Very low	Less for dense WSN	Good	Good
7	STEM	High	Low	Low	Low	High	Low	Good
8	Wise MAC	Very Low	Very Low	Yes(Less)	YES(Low)	High	High	Good
9	CSMA-MPS	Very Low	Overhearing of preamble is reduced	Yes (Less)	Low	high)	High	Good
10	TRAMA	Yes(Very Low)	Very Less	Very Less	High	High for low traffic WSN	High	High
11	PAMAC	Ultra Low	Very Less	Very Less	High	Worse for heavily loaded WSN	High	High

12	Energy aware TDMA based MAC protocol	Ultra Low	Very Less	Less	High	Low		Less
13	BMA MAC	Collision free inside cluster	Low	Less	High	Low	High	Low

3.6 Conclusion

On the basic of comparative study we have done so far we are now at conclusion that the traditional mac protocols are not suitable for directly use in wireless sensor networks applications. However conclusion on the basis of classification done above is all the contention based mac protocols have higher chance of collision but have less packet latency. While schedule based mac protocols have lower chance of collision but having higher packet latency. B-MAC works effectively in low networks traffic conditions since nodes will remain sleeping most of the time however at high and variable traffic condition, because of long preambles, throughput decreases also latency increases with increase in power consumption. All the Contention based S-MAC protocol, established a fixed duty cycle for radio transceiver to listen and sleep periodically for a fixed period of time. While a low duty cycle reduces idle listening time, it outcomes in high latency and low throughput in medium to high traffic conditions as only one data packet transmission can occur in each frame. On the other hand, if duty cycle is high, throughput and latency performance improves at the expense of reduced energy savings.

CHAPTER 4
NODE CLONE DETECTION

4.1 Introduction

WSN is a collection of a large number of tiny sensor nodes deployed in a robust environment. It is used for sensing various parameters like temperature, pressure, humidity etc. and has applications in the area of weather, health and military etc. Sensor nodes have limited resources in terms of energy, memory and computation capability. WSN is susceptible to various attacks like eavesdropping, denial of service, energy depletion due to the wireless communication medium. WSN is also vulnerable to node capturing attack which is very dangerous for the networks. Node capturing is also called node clone in which the attacker initially captures the node and steal all secret information contained in the node, then places the replica of that node in different part of the networks.

Various centralized schemes of node clone detection have been proposed in past. Centralized node clone detection has disadvantages like, single point of failure, and heavy traffic to the nearby nodes of the central server. Therefore the life time of the node nearby the detector node will be reduced. Distributed detection of node clone is another method for clone detection where each sensor node will send its unique id (Node id) and its location to some witness nodes where the actual detection is being performed.

The first part of this chapter presents a summary of distributed detection of node clone algorithms. The protocols proposed in literature review for distributed detection of node clone are focused on reducing the energy consumption of WSN node, but the detection level of these protocols is not very high. The second part of our paper revises a brief introduction about node replication attack and adversary model. Next section of our paper describes the proposed algorithm for node clone detection. At last experimental setup of our proposed algorithm is presented followed by comparison among LSM [53], RED [54] and proposed algorithm.

4.2 Notations

Following table specifies all the symbols that we are using in the paper here for the clarity of the reader

Table-4.1 Symbols and Function Table

N	Number of nodes in the networks
d	Average degree of the networks
p	Probability that a node will forward the location claim
g	Number of witness selected by each neighbour
l_a	Location of node a
H (M)	Hash of message M
K_a	a's Public Key
K^{-1}_a	a's private key
Send message ()	Function that will send message to the specified location
Forward message ()	Forward the received message to its original destination
Decode signature ()	Check the node clone by matching the ids and location
local ()	Return the neighbour ids of the global
global ()	Returns the global witness node id

4.3 Node clone detection Summary

The node clone detection methods of WSN are divided into centralized and distributed. In centralized approach clone detection is done at base station. All the detection procedure will be performed at the base station. Each node in WSN sends neighbours list (Node ids only of neighbours) to the base station and it will finds the clone by matching the neighbours list received from different nodes. This protocol has been modified by adding node location of neighbours to the neighbour list. Centralized approach has several drawbacks like single source of failure and heavy traffic to the nearby nodes of central base station. This will leads to the shortening of nodes lifetime. The centralized scheme has 100% detection level, assuming the entire neighbour data reached successfully to the base station.

Another solution is based on local detection that uses voting mechanism. However, using this kind of approach in distributed fashion will fails if the replica is not within the same neighbourhood. First protocol under distributed detection is simple broadcast [52] also known as Node to networks broadcast. Each node in the networks floods the authenticated broadcast message with the location claims. Each node stores the location of its neighbours and if any conflict occurs, it will revoke the clone and cloned node both. Another solution is deterministic multicast [52]. In deterministic multicast protocol the location claim will be forwarded to some deterministically selected witness nodes. This protocol may suffer from the resilience, that and adversary can predict the location of witnesses. Solution of resilience in deterministic multicast protocol is proposed as randomized multicast [52]. In randomized multicast protocol the random witness nodes are selected so that the adversary cannot anticipate their identities. If at least $\sqrt{n}$ neighbour forwards the location claim, then According to the Birthday paradox [54] at least one witness will detects the clone. The communication cost of this protocol is O (√n. p. g) messages per node. But this scheme have relatively high storage and communication cost. Each node have to store O (p. d. g) location claim. In order to reduce the communication cost of randomized multicast, Line selected multicast [53] is proposed, it uses the routing topology of the networks to detect the replica. The LSM protocol's behaviour is similar to randomized multicast, but slightly better detection probability. When a node in LSM protocol announces its location claim every node will check its signature and then forward the location claim with probability p. In LSM, a location claim will be routed from many intermediate nodes. On each node the location claim will be stored and checked with previous claims to detect the clone. LSM uses constant number of line segments. Line selected multicast will require average O (n√n) communication and O (√n) memory storage of location claim at each node.

A new protocol for node replication detection is Randomized efficient and distributed protocol [54]. RED executes for fixed interval of time. In the first step of this protocol a random number is broadcasted in whole networks through a centralized broadcasting. In second step each node digitally signs and broadcasts it location claim (node id and location l_a). For each node its d number of neighbours will send its location claim with probability p to a set of g >=1 number of pseudo randomly selected networks locations. Assumptions of this protocol are routing will deliver a

message sent to a networks location to the node closest to it. For d neighbours, probability that a claim message will be sent from the neighbour to a given location is $1-(1-p)^{d}$, so the detection probability is $(1-(1-p)^{d})^{2}$. Another protocol in the distributed category is randomly distributed exploration (RDE) [49]. It is proposed for efficient communication performance with good detection probability. It uses the concept of line selected multicast with the addition of ttl concept. When a node gets a location claim with a ttl value, it will firstly check for clone and decrement the ttl (Time to live) value by one and forward it with probability p to the random neighbour. Other protocol is DHT based node clone detection [50] which is fully decentralized key based scheme. It is designed for high detection probability, designed on a distributed hash table frame networks.

4.4 Networks and Threat model

For the testing of our proposed approach we have considered a fixed type of unstructured networks which follows the multihop routing algorithm. Results of any algorithm in wireless sensor networks depend very much upon the type of networks and threat model we are selecting. For the adoptability of our proposed algorithm in real scenario, we have to test our algorithm in a complete random behaviour of the networks. So we have considered the networks and threat model of the system as given below.

4.4.1 Networks Model

Network is considered area with n number of randomly deployed tiny sensor nodes. Every sensor node knows its id, location, public and private key with some memory and processing capability. So a sensor node is represented by $\{A_{id}, l_a, K_a, k^{-1}_a, m_a, p_a\}$. Every node in sensor networks can transmit the data to any node in the networks or outside the networks. For that we used shortest path multihop routing using the Euclidean distance. Assumption for the networks is no traffic overload on the intermediate nodes used while routing.

4.4.2 Threat model

We considered a time dependent adversary who captures a node at any time and extracts all the data (node id, public and private keys, all sensed data). This adversary will deploy the clone of captured sensor node with that stolen information to different

location. And then adversary can deploy any type of attack in the networks. For implementing and testing our proposed approach we have taken a pseudo random function which will randomly copy any of the nodes which is called attacked node and places its replica to more than one place randomly.

4.5 Assumptions

We have proposed an approach for witness based node clone detection of wireless sensor networks, in which attacker deploys copy of node inside the target area. For the implementation of this protocol we have taken certain assumption for the simplicity which is already implemented by other researchers. Each and every assumption is a different issue of research in wireless sensor networks area.

1. Routing will deliver the message without delay to the destination without any interruption.
2. Routing will deliver a message sent to a networks location to the node closest to it.
3. Nodes are randomly deployed on a 500*500 area, we have chosen adversary that ra randomly deploys the different number of replicas to different locations every time we run the simulation.
4. Every nodes, know their neighbours id and location for creating the location claim of the nodes as it is very hot topic of research in WSN.

4.6 Proposed Approach

We have focused on improving the detection level of node clone detection at same cost (energy, computation and memory) while designing this protocol. In literature and REDare well known algorithms for node clone detection. Energy consumption in LSM and RED is less but their detection level is also low. In our proposed approach, whenever a node has to transmit a location claim, it will firstly check for clone and then, forwards the location claim to the node nearest to the global destination. In this approach all the intermediate nodes in route are start working as temporary witness node. In this way detection level will improve by increasing thewitness node. So basically in this approach we will select some random number of witness nodes by a pseudo random function. While sending location claim to the global witness, it will pass through the many intermediate nodes. These intermediate

nodes will now start working as temporary witness nodes. Pseudo code of our proposed algorithm is given here.

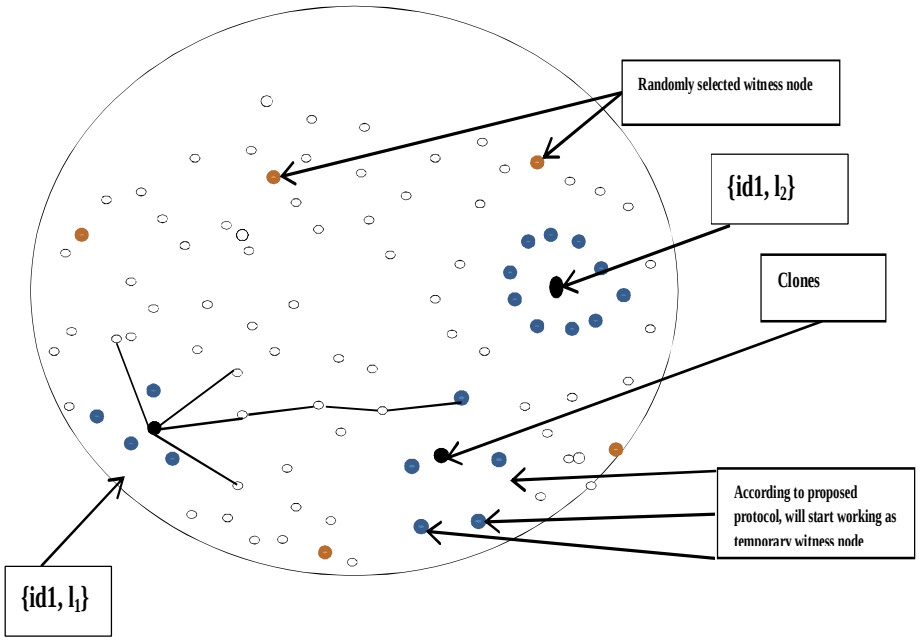

Fig-4.1 Proposed Approach working of node clone detection protocol

Figure 5.1 shows the working of proposed approach for witness based node clone detection in WSN. As we have mentioned earlier, node clone is a copy of authentic nodes which can deploy many types of attack in the networks. Our proposed approach detects the node clone by matching the node ids as well as node locations. A node is said to be clone of another if two node's id matches but their location did not match. For the efficiency of our protocol we cannot apply this match to every node, it will take too much amount of resources. We have randomly selected some witness nodes and send the location claim to those randomly selected witnesses. In between the route, since from source to destination it will takes number of hopes, in our proposed algorithm these intermediate nodes will also works as temporary witness node. Node clone detection is also performed at the temporary witness node as it is performed on the selected witness nodes. Security level of our proposed algorithm is approx. 95 to 97%, it is the highest detection level of all the witness based distributed node clone detection techniques present in literature. We have given the theoretical

proof of the detection level of our proposed algorithm in the following section of this chapter. We have taken a general scenario of wireless sensor networks which can be applied in any type of networks conditions. For this we have taken the random deployment of WSN nodes because at the time of deployment of sensor nodes, its location is not fixed. For the adversary, we does not know the type and thinking of attacker. So for that we have taken the random adversary which compromises the random nodes from all thedeployed nodes, and places the random number of replicas inside the target region. Our proposed algorithm as given below performed same as we discussed above.

Input: Set of randomly deoloyed nodes

Output: Node id of clones

1. Random gen=new Random();
2. Node →neighbours of (node): {Id_n, l_n, Is Loc-Claim, neighbours of(n), K_n ($H(Id_n, l_n)$)};
3. While (on Receive Message (M)) Begin
4. if (M.Type = Loc-Claim)
5. if(gen<Claim-forward-probability(p))
6. Decode-signature() //check for clone;
7. while(g!==number of forward) Begin
8. pos global = pos.predefined-witness-node(gen, id_n);
9. pos local = neighbours-of-global (global);
10. send message(m, local, global, sender info() , signature, type = controlmsg);
11. End
12. End if
13. else If (M.Type = control-msg)
14. If(id_n= Local Destination of(m))
15. Decode Signature(m);
16. forward Message(m);
17. Else Handle Exception (node not found, battery not avail...etc.)
18. End
19. End

Flow of our proposed algorithm is shown in Figure-4.2.When we start the clone detection algorithm in our wireless sensor networks, initially all nodes will requests for their locations to the neighbours. Then every node will create its location claim which consists of its own id, location with the complete list of their neighbour's id and location. Now randomly g number of witness nodes is selected to detect the node clone. Then every node multicasts their location claims to these randomly selected

witness nodes. These location claims will go through many intermediate nodes, on where detection will also be performed. This will increase the detection probability of the clone detection algorithms.

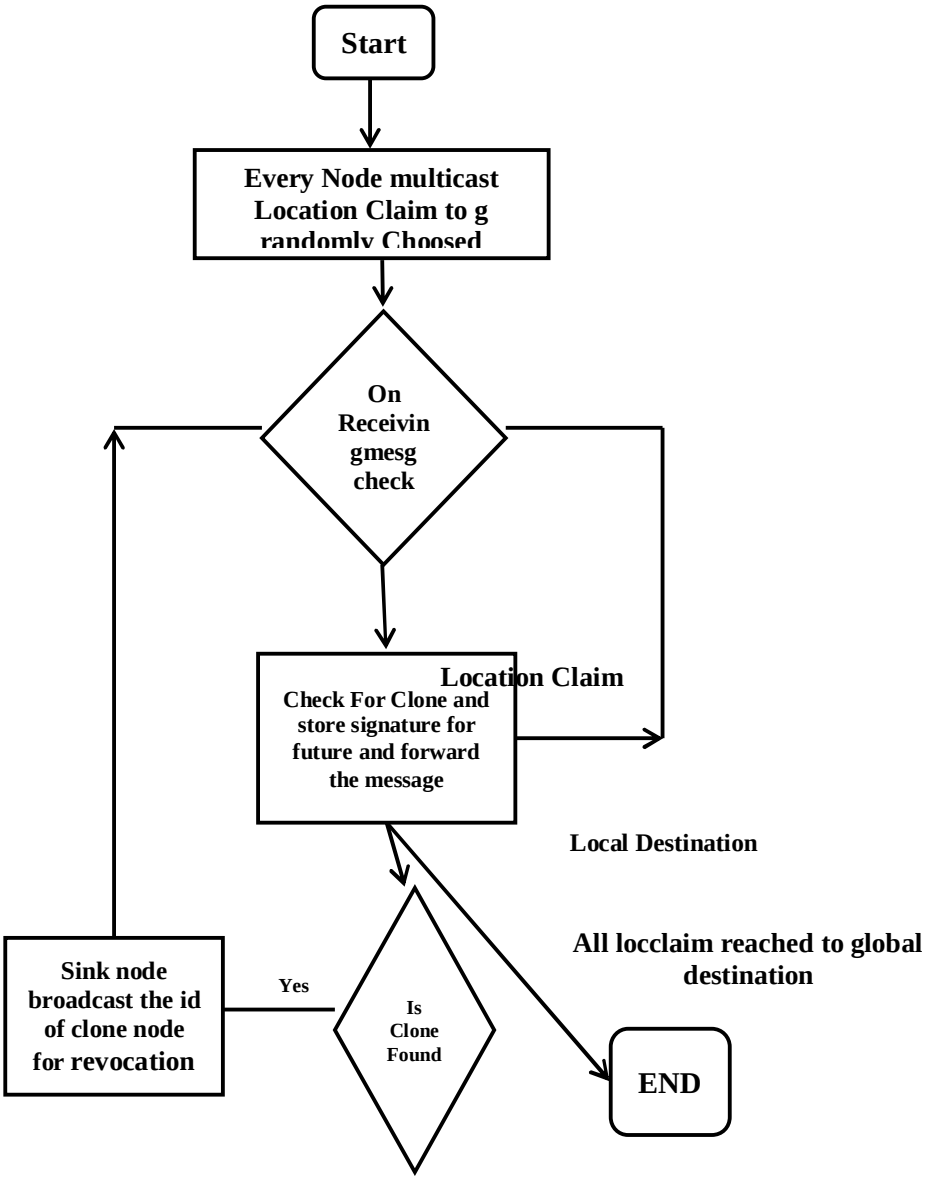

Fig-4.2 Flow Chart of Proposed Approach for node Clone detection

4.7 Security Analysis

Let node A is attacked node, who claims to be at L locations $\{l_1, l_2, \ldots. l_L\}$. d neighbours of each node will select randomly g number of witnesses. If the neighbours coordinated perfectly then probability (p_f) that a node fails to hear any of the g announcements from one neighbour is [6].

$$p_f = 1 - \frac{g}{n} \tag{1}$$

Approximately (p.d) number of neighbours will send the location claim. If $p_{none}$is the probability that node will not hear, so the probability that any node will not hear the location claim is

$$p_{none} = \left(1 - \frac{g}{n}\right)^{p.d} \tag{2}$$

These p.d location claim passes through (p.d.m) intermediate nodes. If we assume all the intermediate nodes selects different path and nodes to route, although there may be some overlap, but we are neglecting that. Then probability that any intermediate node will not hear these location claims p_{none1}

$$p_{none1} = \left(1 - \frac{p.d.m}{n}\right)^{p.d} \tag{3}$$

By combining equation (2) and (3) if we calculate total number of nodes that will receive location claim as L (Receive)

$$L(Receive) = n.\left[\left\{1 - \left(1 - \frac{g}{n}\right)^{p.d}\right\} + \left\{1 - \left(1 - \frac{p.d.m}{n}\right)^{p.d}\right\}\right] \tag{4}$$

So if we approximate it through binomial approximation

$$\text{L(Receive)} \approx p.d.g + p.d.m \tag{5}$$

So L (Receive), number of nodes will receive each location claim. If any adversary inserts L replicas of a node, so we would like to calculate the probability that two location claims will collide at any of the L (Receive) witness nodes. Following the birthday paradox [10], if for approximation we assume g $\approx m$ then L

(Receive) $\approx 2.p.d.g$, so the probability that 2 replicas claim will not have any collision is given by P_{nocol}

$$P_{nocol} = \left(1 - \frac{2.p.d.g}{n}\right)^{2.p.d.g} \quad (6)$$

Probability for all L replicas claim will not concede

$$P_{Lnocol} = \prod_{l=1}^{L-1} \left(1 - \frac{l.2.p.d.g}{n}\right)^{2.p.d.g} = e^{-2.p^2.d^2.g^2.L(L-1)} \quad (7)$$

Since the probability of collision $P_{col} = (1-P_{Lnocol})$ so

$$P_{co} = 1 - e^{-2.p^2.d^2.g^2.L(L-1)} \quad (8)$$

If we calculate P_{col} for n=10,000 ,g=100,d=20 and p=0.05 we will detect the collision probability approx. 98% even for a single replication, for more than one replication it will be approx. 99% or reaches toward 100%. Since we have taken the approximation that $g \approx m$ but practically m<g, so in practical result there may be some fluctuation. There is an energy constraint as well, so we will consider it in our implementation and result section that how much difference is there in energy consumption with respect to the other protocols.

4.8 Project Snapshots

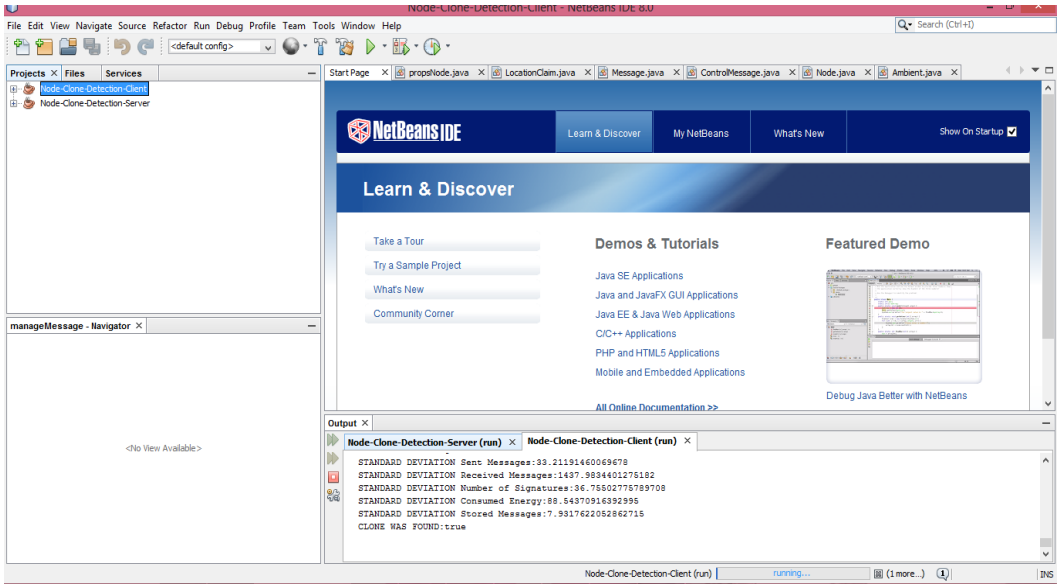

Fig-4.3 Demo of Java node clone detection simulator

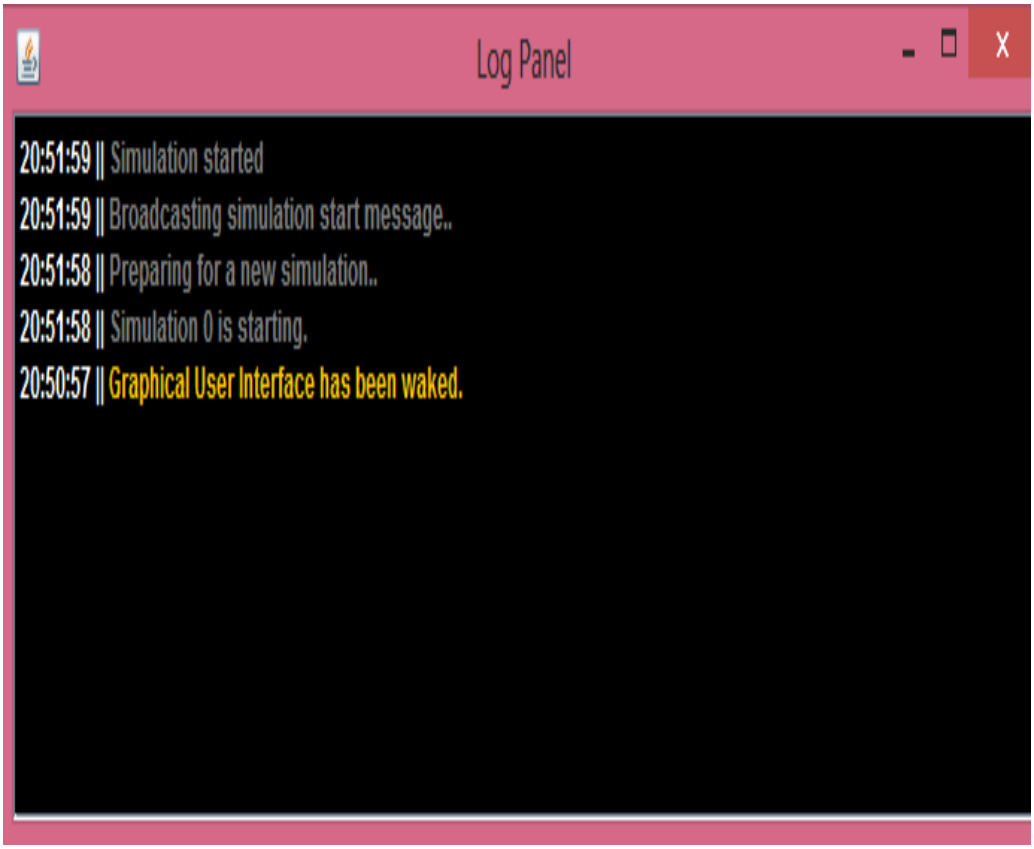

Fig-4.4 Demo of Log panel

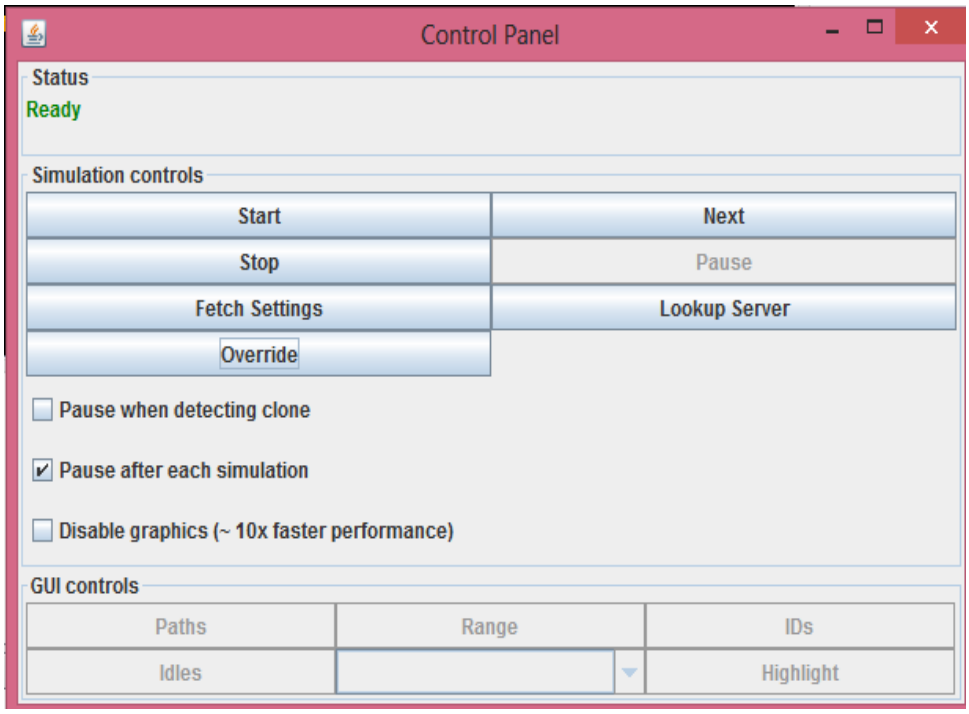

Fig-4.5 Demo of Control Pane

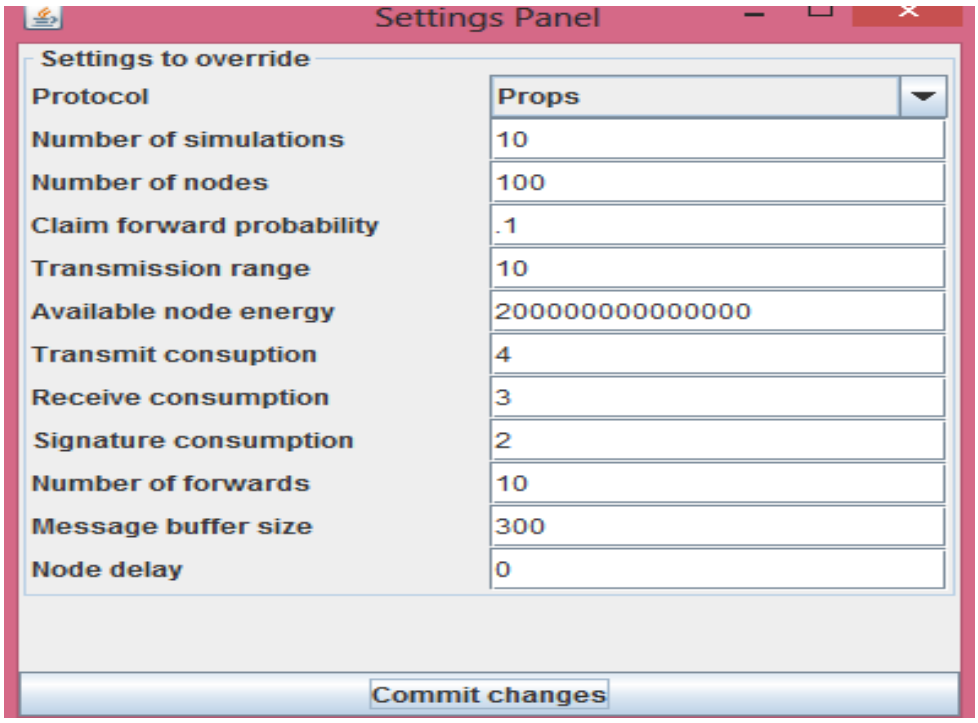

Fig-4.6 Parameter values of proposed protocols at setting panel

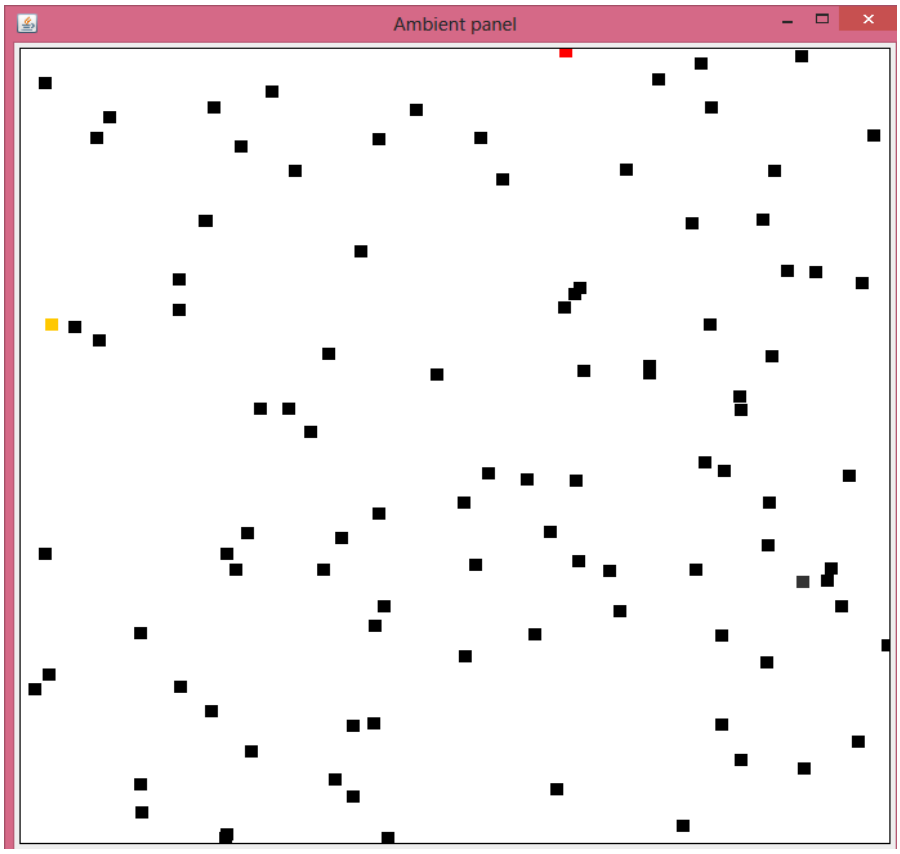

Fig-4.7 GUI for the deployment of sensor node in target region

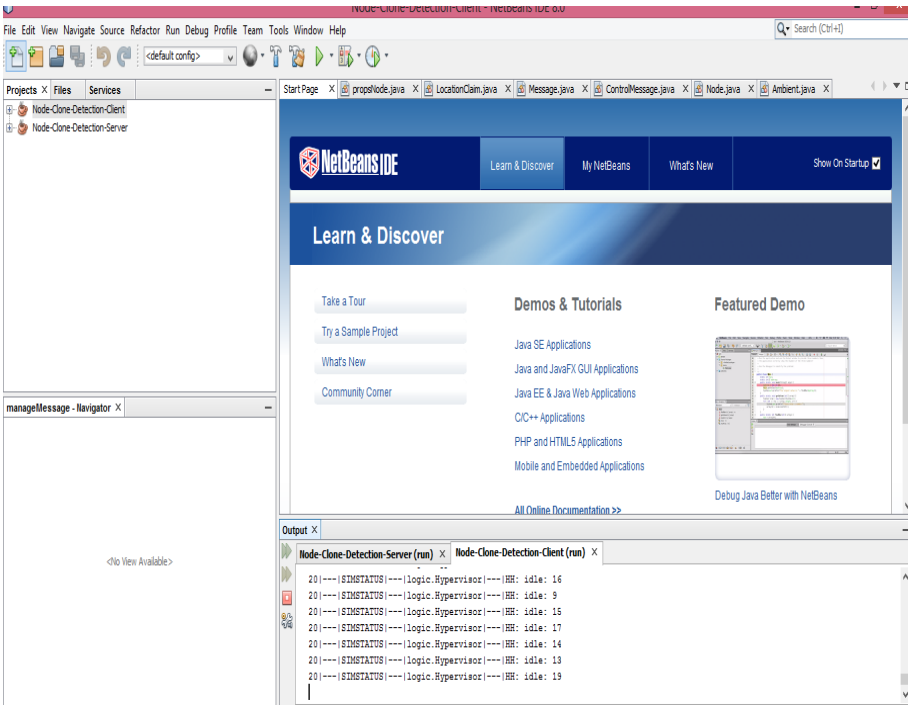

Fig-4.8 Demo of protocol executing at net beans

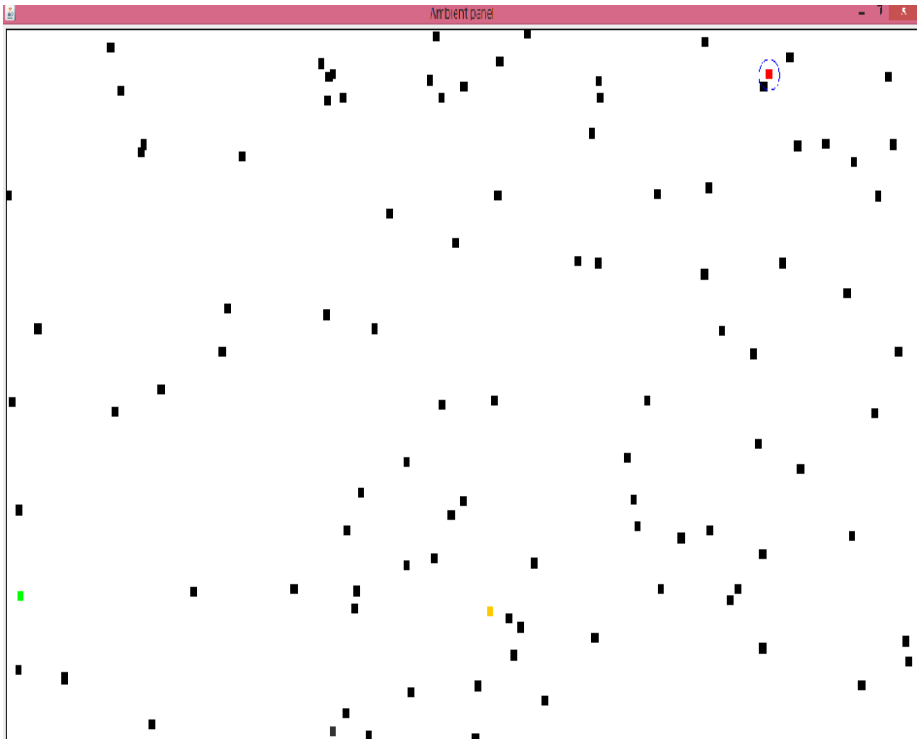

Fig-4.9 GUI of sensor node on protocol execution

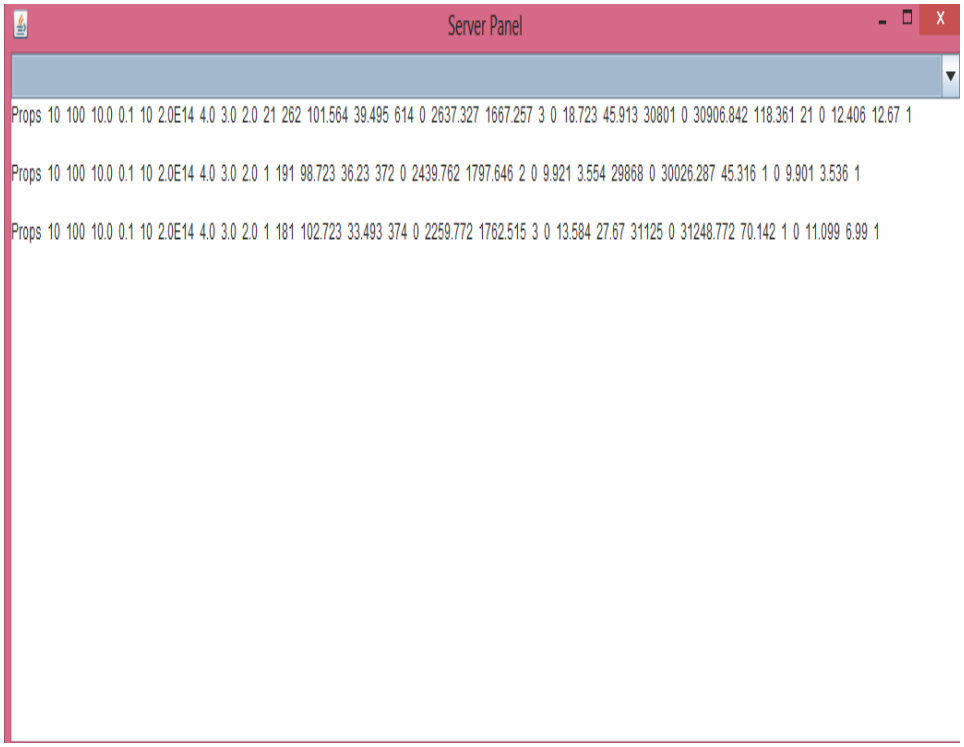

Fig-4.10 value of WSN parameters at Server Log

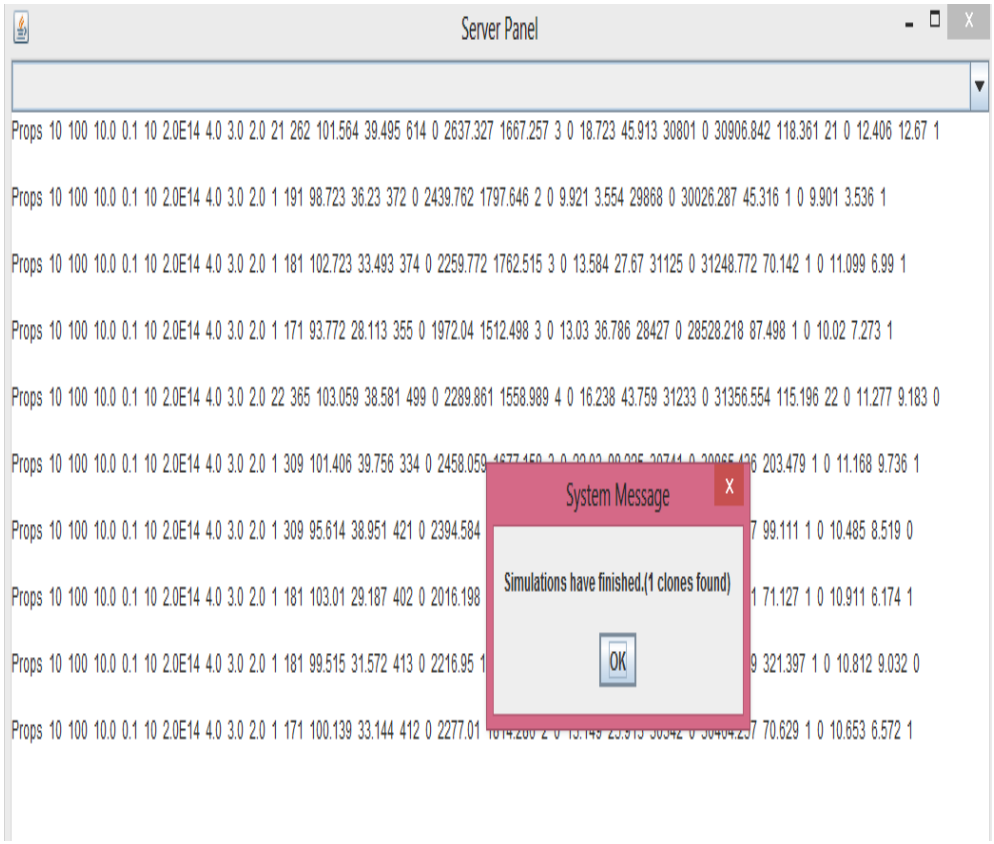

Fig-4.11 Final result of proposed Clone detection Algorithm

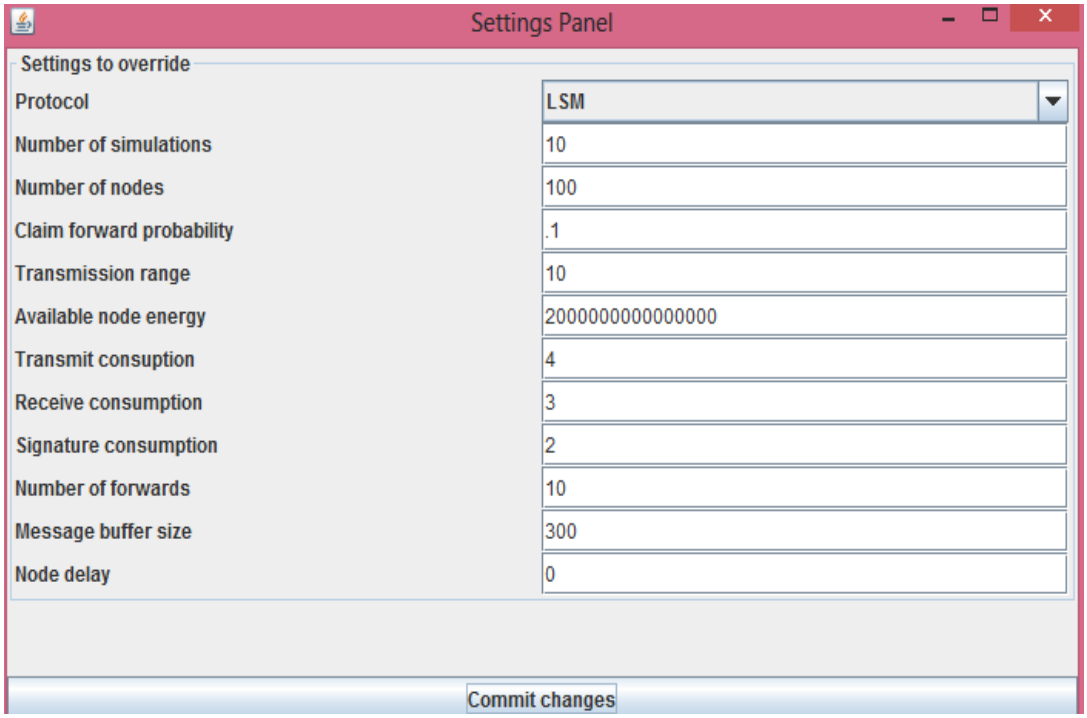

Fig-4.12 Setting panel for line selected multicast protocol execution

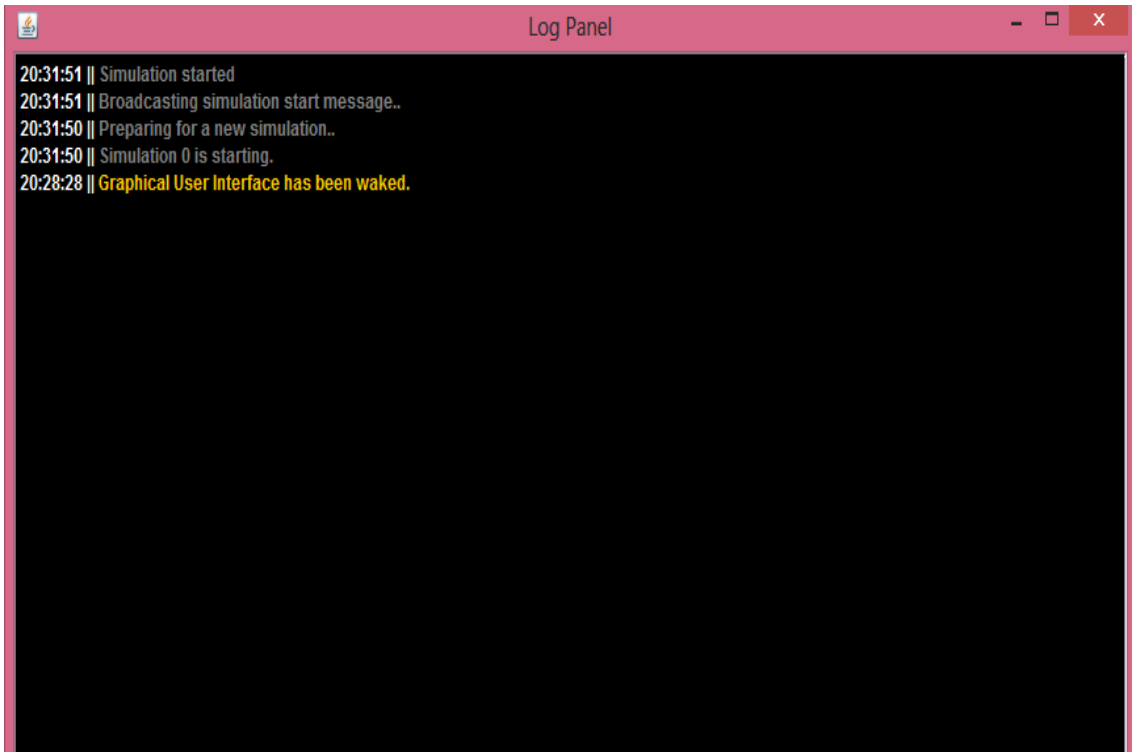

Fig-4.13 Log panel for Line selected multicast protocol execution

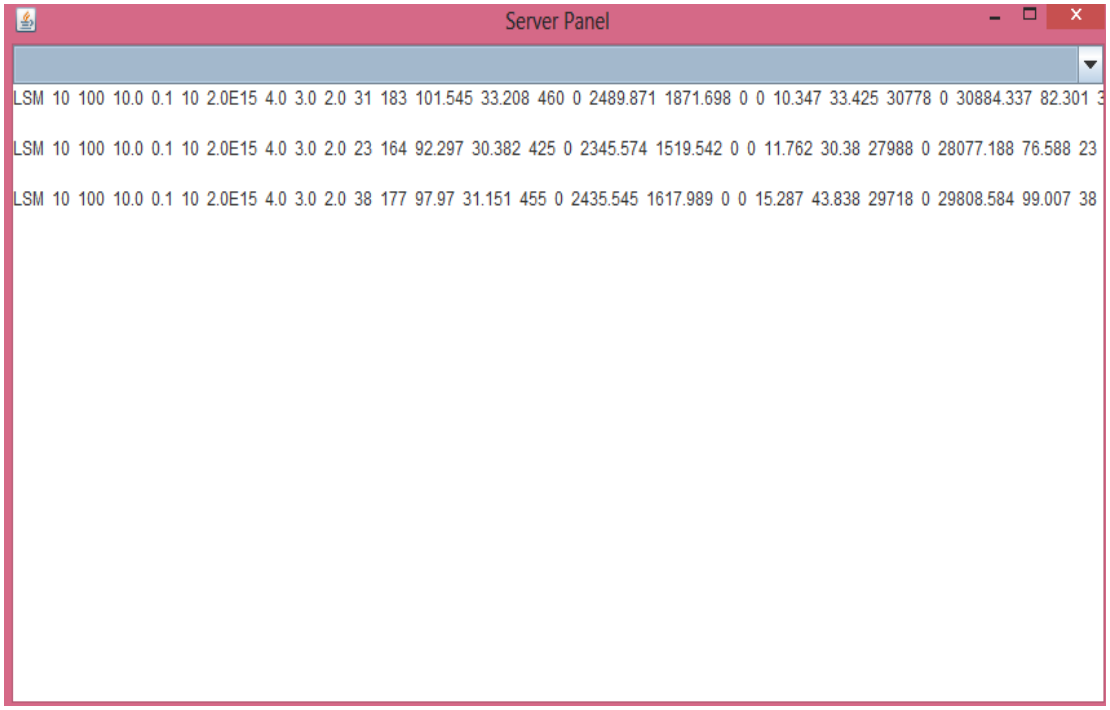

Fig-4.14 Server panel showing results of 3 times execution of line selected multicast protocol

Fig-4.15 Server panel for 8 time execution of Line selected multicast protocol

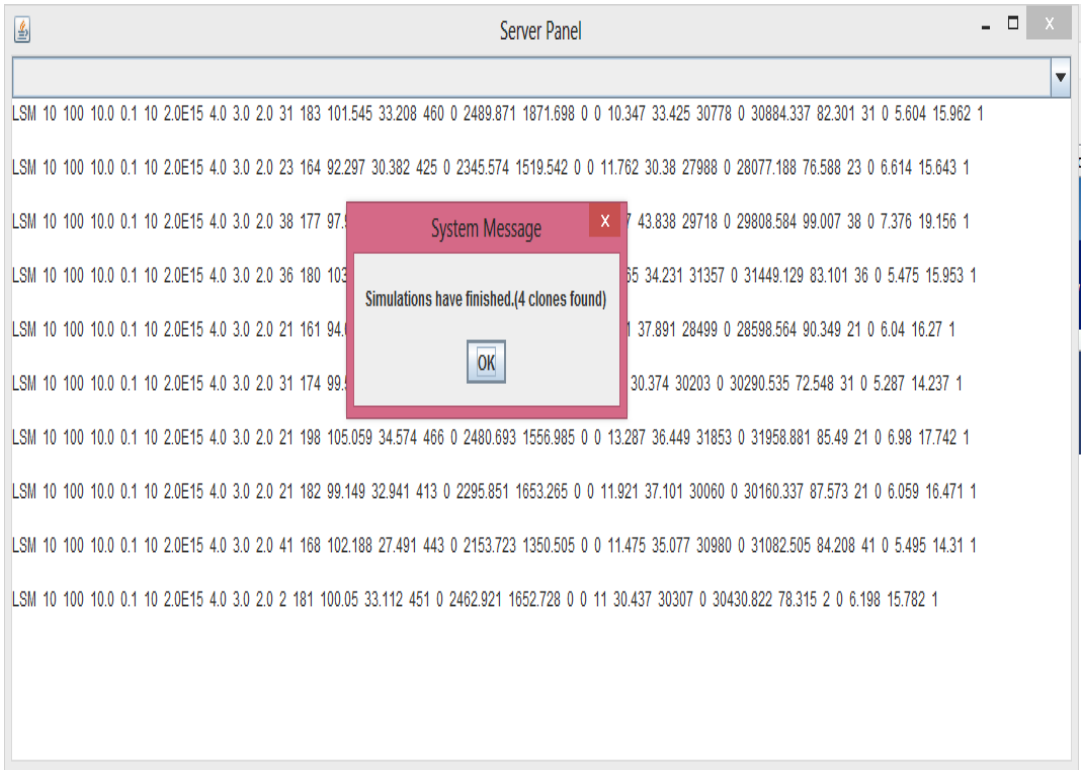

Fig-4.16 Final result of Line selected multicast protocol for clone detection in WSN

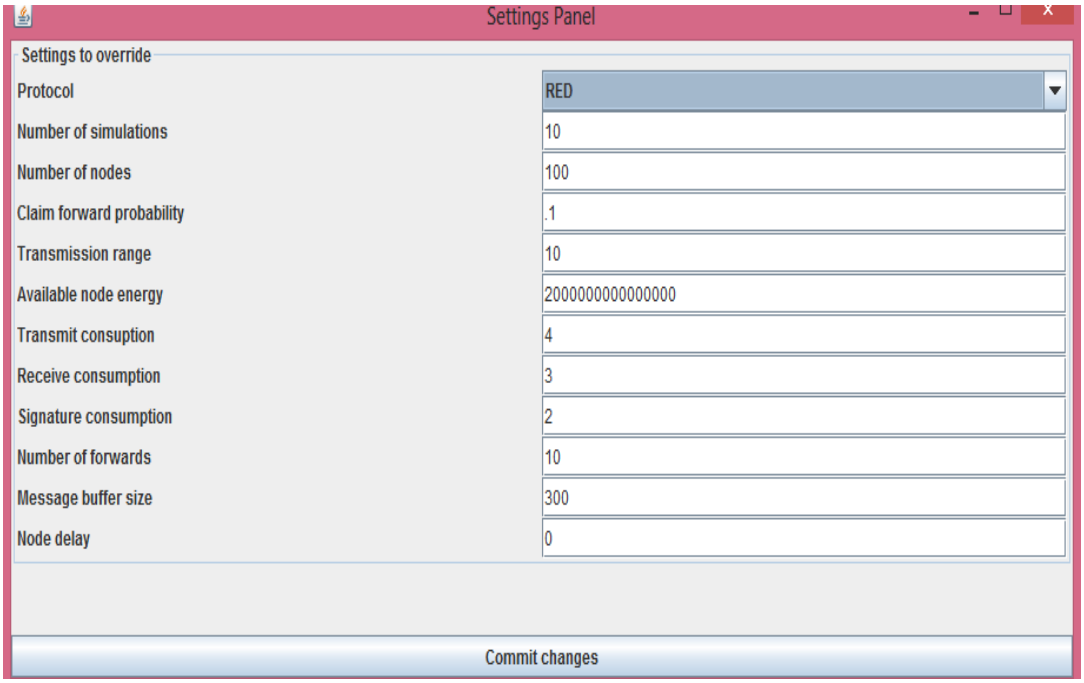

Fig-4.17 Setting panel for RED protocol of clone detection in WSN

Fig-4.18 Server Panel for the execution of RED protocol for clone detection in WSN

4.9 Comparative Analysis

RED and LSM protocols perform better when p.d.g = $\sqrt{n}$. To compare our protocol with the best case performance of LSM and RED, we have used the entire variable used in the past for all the three protocol simulation. We have deployed n number of nodes randomly in the M × M area, each node having transmission range of r, then d can be calculated by.

$$d = \pi r^2 \times \frac{n}{M\ X\ M} \quad \ldots\ldots\ldots\ldots\ldots (9)$$

We have started simulating the protocols from 10 to 10, 00 number of nodes on a 500 × 500 playground having forward probability p =.1. We have calculated d by equation (9), and according to this we are providing parameter values to the algorithm. We found following results in terms of detection level and energy consumption. Every value used in fig-2, fig-3 and fig-3 is the mean of value obtained after 100 simulations at each parameter value.

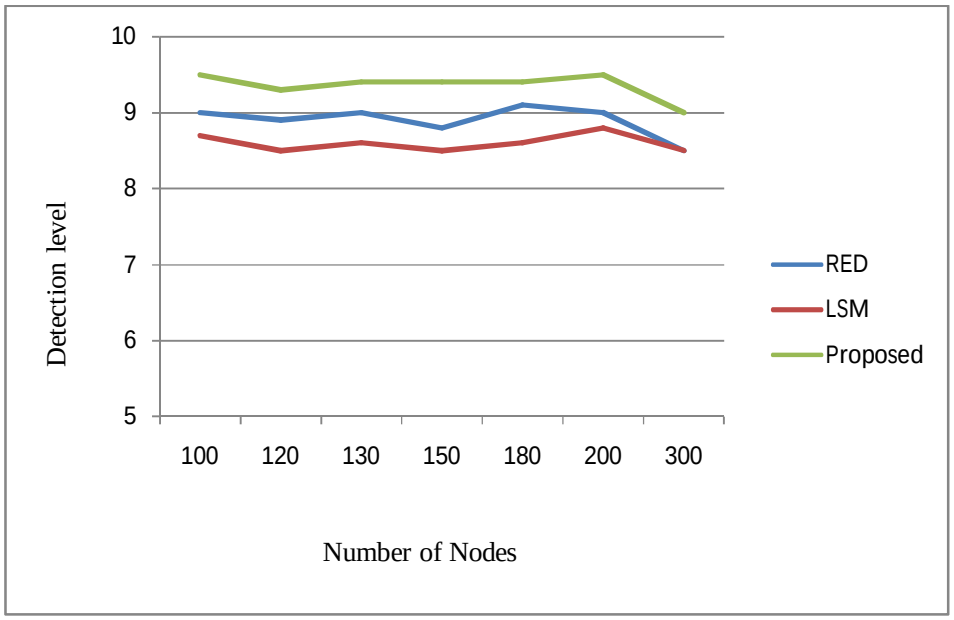

Fig-4.19 Comparison of detection level of LSM, RED, Proposed

As in Fig-6.1 proposed protocol for WSN node clone detection has higher detection level as compared to the RED and LSM. We have simulated all the three protocols. Detection level of proposed protocol is almost greater than 90% for all the parameter value. When we are increasing the number of nodes in the area then probability of

detection will come down but still it will be greater than 90%. We have taken two approximations in our mathematical proof so we are getting small difference proved and actually implemented values.

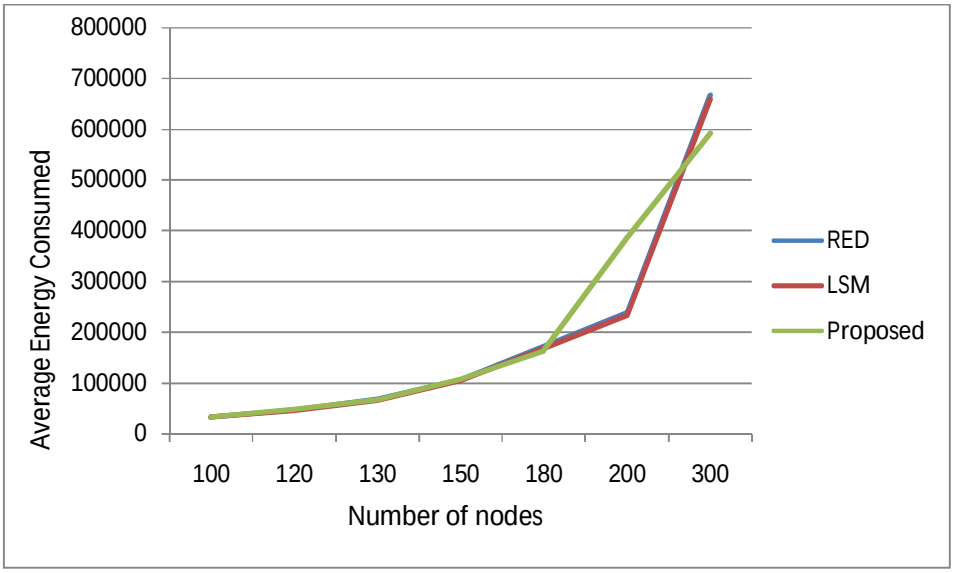

Fig-4.20 Average Energy Consumed by sensor nodes in LSM, RED Proposed

Networks performance can be measured by its throughput, latency, and other factors of the networks. But WSN is a special kind of networks with limited resources, so we have to utilize our networks resource efficiently. Our proposed protocol is for detecting clones in the networks, so we have to measure the accuracy of our protocol, which can be better measured by the detection level. So we have tried to measure the performance of our proposed protocol by the detection level. Other performance factor we have used in this paper is energy consumption and memory consumed. In fig-3 we have plotted the curve of average energy consumed by sensor node with varying the number of nodes in the area. The plot we have got is comparatively same with the existing protocol as shown in Fig-6.2.In Fig-6.3 we have plotted the curve between the numbers of message stored at every node in WSN, while increasing the number of nodes in the area. Here we got little bit of memory overhead. In last 10 to 15 years the average growth of memory size and reduction in cost is very high, so this small amount of memory overhead we can neglect in present scenario. So when we compare overall protocol with the existing it is giving better result with existing.

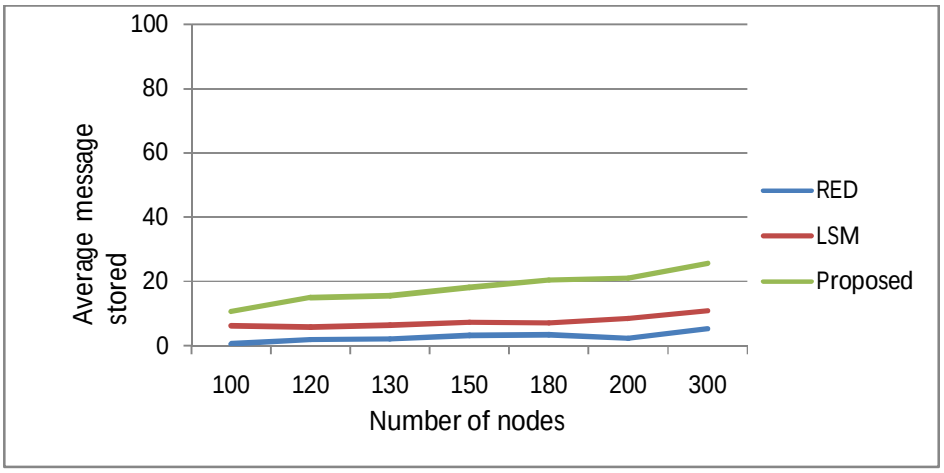

Fig-4.21 Average message stored at each sensor nodes of LSM, RED, and Proposed

4.9 Conclusion

Most of the time in WSN, we need a protocol that gives adequate result with limited resource usage. Proposed approach improved the detection level having 3 - 7% improvement in detection level with comparatively same energy consumption. We found approx. 10 message storage overhead at each node as compared to LSM and RED. Overall performance of our proposed protocol is better than LSM and RED in terms of detection level and energy.

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

The energy consumption in WSN is still an active research area and we believe that most of the energy is consumed in communication, which is controlled by the MAC protocols at data link layer. Although, many protocols have been presented in literature, the selection of an efficient MAC protocol is significant for the WSN performance. WSN uses a shared communication medium which is very unreliable and prone to attacks. Security of wireless sensor networks is another very important issue.

Most of the power in WSN is consumed by the radio unit of a sensor node, which are active for the transmission and recipient of the data packets. We have discussed all the MAC layer protocol, analysis shows that a good MAC protocol will improve the life time of Sensor networks.

In this dissertation we have taken the challenge to secure the wireless sensor network from node clone attack. We have discussed all the protocols of WSN in literature, and proposed a novel approach for clone detection. We have compared our proposed protocol with the past on the basis of parameters detection level, energy consumption and memory overhead. The detection level of our proposed protocol is 6-7 % higher than the previous protocol LSM and RED discussed in literature. However, the energy consumption of each node is same as the previous protocols. We have got approx 10 message overhead at each node for 5-7 % improvement in detection level. According to the Moore's law, a little amount of memory overhead should not be major concerned. So the overall performance of our protocol is better than the pervious.

REFERENCES

1. Ferri, Richard, Moon Kim, and Eric Yee. "Wireless sensor networks." U.S. Patent Application 10/856,684.
2. Pottie, G. J. (1998, June). Wireless sensor networks. In *Information Theory Workshop, 1998* (pp. 139-140). IEEE.
3. Stankovic, J. A. (2008). Wireless Sensor Networks. *IEEE Computer*, *41*(10), 92-95.
4. Raghavendra, C. S., Sivalingam, K. M., &Znati, T. (Eds.). (2004). *Wireless sensor networks*. Springer Science & Business Media.
5. Karl, H., &Wolisz, A. (2005). *Wireless Sensor Networks*. Springer.
6. Zia, T., &Zomaya, A. (2006, October). Security issues in wireless sensor networks. In *Systems and Networks Communications, 2006. ICSNC'06. International Conference on* (pp. 40-40). IEEE.
7. Heinzelman, W. B., Chandrakasan, A. P., &Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensornetworks. *Wireless Communications, IEEE Transactions on*, *1*(4), 660-670.
8. Karl, H., &Willig, A. (2007). *Protocols and architectures for wireless sensor networks*. John Wiley & Sons.
9. Melodia, T., Vuran, M. C., &Pompili, D. (2006). The state of the art in cross-layer design for wireless sensor networks. In *Wireless Systems and Networks Architectures in Next Generation Internet* (pp. 78-92). Springer Berlin Heidelberg.
10. Mohammadi, S., &Jadidoleslamy, H. (2011). A comparison of link layer attacks on wireless sensor networks. *arXiv preprint arXiv:1103.5589*.
11. Leon-Garcia, A., &Widjaja, I. (2003). *Communication networks*. McGraw-Hill, Inc..
12. Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. *Wireless Communications, IEEE*, *11*(1), 38-47.
13. Conti, M., Di Pietro, R., Mancini, L. V., & Mei, A. (2011). Distributed detection of clone attacks in wireless sensor networks. *Dependable and Secure Computing, IEEE Transactions on*, *8*(5), 685-698.
14. Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference* (Vol. 2, pp. 6-pp). IEEE.
15. Molla, M. M., &Ahamed, S. I. (2006). A survey of middleware for sensor networks and challenges. In *Parallel Processing Workshops, 2006. ICPP 2006 Workshops. 2006 International Conference on* (pp. 6-pp). IEEE.
16. Huang, P., Xiao, L., Soltani, S., Mutka, M. W., & Xi, N. (2013). The evolution of MAC protocols in wireless sensor networks: A survey. *Communications Surveys & Tutorials, IEEE*, *15*(1), 101-120.
17. Colvin, A. (1983). CSMA with collision avoidance. *Computer Communications*, *6*(5), 227-235.
18. García-Hernández, C. F., Ibarguengoytia-Gonzalez, P. H., García-Hernández, J., & Pérez-Díaz, J. A. (2007). Wireless sensor networks and applications: a

survey. *IJCSNS International Journal of Computer Science and Networks Security*, *7*(3), 264-273.
19. Van Dam, T., &Langendoen, K. (2003, November). An adaptive energy-efficient MAC protocol for wireless sensor networks. In *Proceedings of the 1st international conference on Embedded networksed sensor systems* (pp. 171-180). ACM.
20. Cano, C., Bellalta, B., Sfairopoulou, A., & Oliver, M. (2011). Low energy operation in WSNs: A survey of preamble sampling MAC protocols. *Computer Networks*, *55*(15), 3351-3363.
21. Arisha, Khaled, Moustafa Youssef, and Mohamed Younis. "Energy-aware TDMA-based MAC for sensor networks." System-level power optimization for wireless multimedia communication. Springer US, 2002. 21-40.
22. Li, J., &Lazarou, G. Y. (2004, April). A bit-map-assisted energy-efficient MAC scheme for wireless sensor networks. In *Proceedings of the 3rd international symposium on Information processing in sensor networks* (pp. 55-60). ACM.
23. Singh, Suresh, and Cauligi S. Raghavendra. "PAMAS—power aware multi-access protocol with signalling for ad hoc networks." ACM SIGCOMM Computer Communication Review 28.3 (1998) pg: 5-26.
24. Ye, W., Heidemann, J., &Estrin, D. (2002). An energy-efficient MAC protocol for wireless sensor networks. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE* (Vol. 3, pp. 1567-1576). IEEE.
25. Van Dam, T., &Langendoen, K. (2003, November). An adaptive energy-efficient MAC protocol for wireless sensor networks. In *Proceedings of the 1st international conference on Embedded networksed sensor systems* (pp. 171-180). ACM.
26. Rajesh Yadav, ShirshuVarma and N.Malaviya “Optimized Medium Access Control for Wireless Sensor Networks” IJCSNS International Journal of Computer Science and Networks Security, Vol. 8, No.2, pp. 334 -338 (February 2008).
27. Polastre, J., Hill, J., & Culler, D. (2004, November). Versatile low power media access for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networksed sensor systems* (pp. 95-107). ACM.
28. Buettner, M., Yee, G. V., Anderson, E., & Han, R. (2006, October). X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks. In *Proceedings of the 4th international conference on Embedded networksed sensor systems* (pp. 307-320). ACM.
29. Demirkol, I., Ersoy, C., &Alagoz, F. (2006). MAC protocols for wireless sensor networks: a survey. *Communications Magazine, IEEE*, *44*(4), 115-121.
30. C. Schurgers, V. Tsiatsis, and M. B. Srivastava. STEM: topology management for energy efficient sensor networks. In Proceedings of the IEEE Aerospace Conference, volume 3, pp. 1099–1108, Big Sky, MT, USA, 2002.
31. A. El-Hoiydi and J.-D. Decotignie. WiseMAC: an ultra low power MAC protocol for the downlink of infrastructure wireless sensor networks. In Proceedings of the International Symposium on Computers and Communications (ISCC’04), volume 1, pp. 244–251, Alexandria, Egypt, July 2004.

32. El-Hoiydi, A. (2002). Spatial TDMA and CSMA with preamble sampling for low power ad hoc wireless sensor networks. In *Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh International Symposium on* (pp. 685-692). IEEE.
33. Zhu, S., Setia, S., &Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *2*(4), 500-528.
34. Sharma, K., &Ghose, M. K. (2010). Wireless sensor networks: An overview on its security threats. *IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs*, 42-45.
35. Kahn, J. M., Katz, R. H., &Pister, K. S. (1999, August). Next century challenges: mobile networksing for "Smart Dust". In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networksing* (pp. 271-278). ACM.
36. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., &Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. *Communications Surveys & Tutorials, IEEE*, *11*(4), 42-56.
37. Becher, A., Benenson, Z., &Dornseif, M. (2006). *Tampering with motes: Real-world physical attacks on wireless sensor networks* (pp. 104-118). Springer Berlin Heidelberg.
38. Law, Y. W., Van Hoesel, L., Doumen, J., Hartel, P., &Havinga, P. (2005, November). Energy-efficient link-layer jamming attacks against wireless sensor networks MAC protocols. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks* (pp. 76-88). ACM.
39. Raymond, D. R., &Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *Pervasive Computing, IEEE*, *7*(1), 74-81.
40. Mohammadi, S., &Jadidoleslamy, H. (2011). A comparison of link layer attacks on wireless sensor networks. *arXiv preprint arXiv:1103.5589*.
41. Rajasegarar, S., Leckie, C., &Palaniswami, M. (2008). Anomaly detection in wireless sensor networks. *Wireless Communications, IEEE*, *15*(4), 34-40.
42. Sharma, K., &Ghose, M. K. (2010). Wireless sensor networks: An overview on its security threats. *IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs*, 42-45.
43. Wang, J., Zheng, Y., Leung, C., &Jia, W. (2003, October). A-DSR: A DSR-based anycast protocol for IPv6 flow in mobile ad hoc networks. In *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th* (Vol. 5, pp. 3094-3098). IEEE.
44. Perkins, C. E., &Bhagwat, P. (1994, October). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM Computer Communication Review* (Vol. 24, No. 4, pp. 234-244). ACM.
45. Wazid, M., Katal, A., Singh Sachan, R., Goudar, R. H., & Singh, D. P. (2013, April). Detection and prevention mechanism for Blackhole attack in Wireless Sensor Networks. In *Communications and Signal Processing (ICCSP), 2013 International Conference on* (pp. 576-581). IEEE.

46. Buttyán, L., &Csik, L. (2010, March). Security analysis of reliable transport layer protocols for wireless sensor networks. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on* (pp. 419-424). IEEE.

47. Mohammadi, S., &Jadidoleslamy, H. (2011). A Comparison of Transport and Application Layers Attacks on Wireless Sensor Networks. *organization*, *4*, 21.
48. Khan, W. Z., Aalsalem, M. Y., Saad, M. N. B. M., & Xiang, Y. (2013). Detection and mitigation of node replication attacks in wireless sensor networks: a survey. *International Journal of Distributed Sensor Networks*, *2013*.
49. Chan, H., Perrig, A., & Song, D. (2003, May). Random key predistribution schemes for sensor networks. In *Security and Privacy, 2003. Proceedings. 2003 Symposium on* (pp. 197-213). IEEE.
50. Choi, H., Zhu, S., & La Porta, T. F. (2007, September). SET: Detecting node clones in sensor networks. In *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on* (pp. 341-350). IEEE.
51. Parno, B., Perrig, A., &Gligor, V. (2005, May). Distributed detection of node replication attacks in sensor networks. In *Security and Privacy, 2005 IEEE Symposium on* (pp. 49-63). IEEE.
52. Flajolet, P., Gardy, D., &Thimonier, L. (1992). Birthday paradox, coupon collectors, caching algorithms and self-organizing search. *Discrete Applied Mathematics*, *39*(3), 207-229.
53. Zhu, B., Addada, V. G. K., Setia, S., Jajodia, S., & Roy, S. (2007, December). Efficient distributed detection of node replication attacks in sensor networks. In *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual* (pp. 257-267). IEEE.
54. Conti, M., Di Pietro, R., Mancini, L. V., & Mei, A. (2007, September). A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. In *Proceedings of the 8th ACM international symposium on Mobile ad hoc networksing and computing* (pp. 80-89). ACM.
55. Zhu, W. T., Zhou, J., Deng, R. H., &Bao, F. (2012). Detecting node replication attacks in wireless sensor networks: a survey. *Journal of Networks and Computer Applications*, *35*(3), 1022-1034.
56. Ho, J. W., Wright, M., & Das, S. K. (2009, April). Fast detection of replica node attacks in mobile sensor networks using sequential analysis. In *INFOCOM 2009, IEEE* (pp. 1773-1781). IEEE.
57. Yu, C. M., Lu, C. S., &Kuo, S. Y. (2008, June). Mobile sensor networks resilient against node replication attacks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON'08. 5th Annual IEEE Communications Society Conference on* (pp. 597-599). IEEE.
58. Stemm, M., & Katz, R. H. (1998). Vertical handoffs in wireless overlay networks. *Mobile Networks and applications*, *3*(4), 335-350.
59. Balmukund Mishra, VandanaMohindru, Yashwant Singh "Comparative Analysis WSN MAC protocol" JBAER October 2014 Volume 1 Number 6. Pg: 15-23 ISSN: 2350-0077.
60. Tijs van Dam, KoenLangendoen "An Adaptive Energy Efficient MAC Protocol for Wireless Networks" in Proceedings of the First ACMConference on Embedded Networksed Sensor Systems (November 2003) pg: 5-12.
61. Polastre, Joseph, Jason Hill, and David Culler. "Versatile low power media access for wireless sensor networks." Proceedings of the 2nd international conference on Embedded networksed sensor systems. ACM, 2004.