Detection of Sybil Attack in WSN using State Information and Enhanced Techniques.

A DISSERTATION 2

Submitted By

Shiva Chandel (11006588)

to

Department of Electronics and Communication

In partial fulfillment of the requirement for the

Award of the degree of

Master of Technology in Electronics and Communication

Under the Guidance of

Asst. Prof. Nilufar Yasmin

April 2015

CERTIFICATE

This is to certify that Dissertation titled "**Detection of Sybil Attack in WSN using State Information and enhanced techniques**" that is being submitted by **SHIVA CHANDEL** is in partial fulfillment of the requirements for the award of MASTER OF TECHNOLOGY DEGREE, is a record of bonafide work done under my guidance. The contents of this Dissertation, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

Date: Signature of the Advisor

Asst. Prof. Nilufar Yasmin

ACKNOWLEDGEMENT

I take this opportunity to express a deep sense of gratitude to **Ms. Nilufar Yasmin** for providing excellent guidance, inspiration and encouragement to go ahead throughout this Dissertation. It is because of her constant and general interest and assistance that supports me in the compilation of this Dissertation.

I would like to declare that this dissertation report is my own by made by following the guidelines of LPU. This is entirely the piece of work done on my own.

In the last, I would also like to thank my family and friends who have been a source of encouragement and inspiration throughout the duration of this dissertation.

Shiva Chandel

11006588

DECLARATION

I hereby declare that the dissertation entitled "**Detection of Sybil Attack in WSN using State Information and enhanced techniques**" submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: **Shiva Chandel.**

Regn. No. 11006588

ABSTRACT

Security of Wireless Sensor Networks is one of the major issue because of the prevalence of WSN in the military and civil domains. There are certain constraints in Wireless sensor networks such as limited power, limited storage, latency, low bandwidth and small physical size. These constraints are the obstacles to sensor security which allows different types of attacks that can take place during communication among the nodes. Among different attacks, Sybil attack is one of the harmful threat against the sensor network as this attack can make the network easily vulnerable to other attacks. In Sybil attack, Sybil node has multiple fake identities which disrupt the network's protocols. As Sybil attacker communicate with legitimate nodes by using fake identities and get access to the sensitive information which affect the normal working of the network. There in attempting to protect WSNs against Sybil attack, this dissertation analyzes and discusses different prevention methods. State Information scheme comes out to be a promising scheme to detect Sybil Attack with good accuracy rate hence it has been implemented on software MATLAB. Simulation results shows the detection rate of Sybil Attack in WSN.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURES

LIST OF ABBREVIATIONS

WSN	Wireless Sensor Network
BS	Base Station
UWSNs	Underwater Wireless Sensor Networks
VBF	Vector Based Forwarding
HHVBF	Hop by Hop Vector Based Forwarding
FBR	Focused Beam Routing
DFBR	Directional Flooding Based Routing
RTS	Request to Send
CTS	Clear to Send
DBR	Depth Based Routing
H2-DAB	Hop by Hop Dynamic Addressing Based
DOS	Denial of Service
CA	Certificate Authority
PKC	Public Key Cryptography
KPD	Key Pre-distribution
CIA	Central Identification Authority
TIA	Trust Identification Authority
TBS	Trusted Base Station
RSSI	Received Signal Strength Indicator
AOA	Angle of Arrival
TDOA	Time Difference of Arrival

LOS	Line of Sight
RANSAC	Random Sample Consensus
PES	Presence Evidence System
VANETs	Vehicular Ad-hoc Networks
CAM	Compare and Match
PVM	Position Verification Method
RSDs	Regional Statistics Detection Scheme
MANETs	Mobile Ad-hoc Network
SDTM	Sybil Attack Detection Using Traffic Monitoring
LSDF	Lightweight Sybil Attack Detection Framework

Chapter 1
INTRODUCTION

Wireless sensor networks are composed of many small devices called nodes which are the most basic building blocks for the network. Thus nodes are used to sense physical parameters such as temperature, sound, pressure, motion or vibration etc from the environment.

A sensor node consist of a processing unit, limited computational power and limited memory like a general computer have. These nodes suffer from the limitation of energy because the power source of a node is a battery having a limited lifespan.

These nodes communicate with each other via a wireless medium and forward the sensed data to the Base Station. Base station provides the path to connect with the other world apart from the network itself.

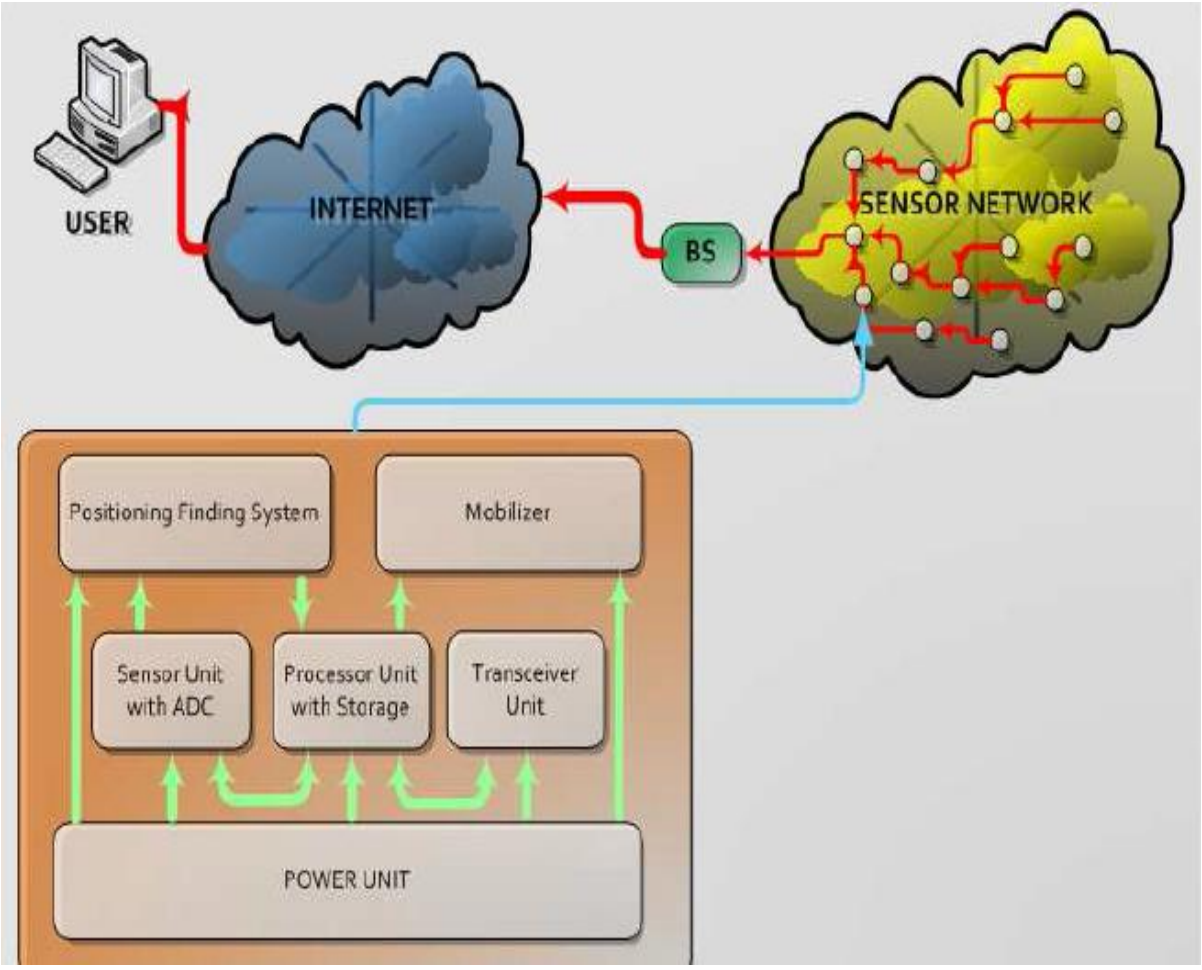

Figure 1.1: Architecture of Wireless Sensor Network.

1.1 WSN Topologies

Wireless Sensor networks can be arranged in either homogeneous or heterogeneous topologies. According to homogeneous arrangement, all sensor nodes send their data to the base station directly and in this topology base station is only the leader (head) of the system. This type of system having both advantages and disadvantages but on the size of the network, this topology is suited to smaller networks.

According to the heterogeneous arrangement, which is also called cluster-based arrangement, here the entire network is subdivided into clusters (small networks). In each cluster there is a cluster-head who is responsible for allocating channel to all its member nodes, collecting sensed data, forward this data to the BS and also manages the received data by the Base Station. Here base station is able to talk with the every cluster head in its network.

In both of the above mentioned topologies, there are three types of communication methods used, named Unicast, Multicast and Broadcast.

Unicast- If a sensor node wants to transmit a message to just one other node.

Multicast- If a sensor node wants to transmit a message to the selected few nodes (group of nodes).

Broadcast- If a sensor node wants to transmit a message to every sensor node present in the network.

1.2 Applications of WSN

Here is the list of some prominent areas of WSN applications:

a. Military Applications:

A figure of WSN applications have been found in military, for example: biological and chemical attack detection, battle damage assessment, battlefield surveillance.

b. Health Care Applications:

WSNs has a collection of health care applications that includes diagnostics, drug administration in hospitals and tracking and monitoring doctors and patients inside hospital.

c. Home Applications :

As we mentioned the technology is civilizing swiftly and many smart sensor nodes and actuators can be found in home appliances, that includes vaccum cleaners, micro-wave ovens, and refrigerators. These

sensor nodes are appeared inside home devices that can act together with each other and with external network that permits end user to administer home devices locally and remotely.

d. Environmental Applications:

WSN are used in numerous applications for examine the environment. For example, there are various applications for monitoring the movements of animals, flood detection, forest fire discovery and inspection of the environmental factors that affects livestock and agricultural crops.

e. Other Commercial Applications:

Commercial applications of WSN include constructing smart office spaces; robot control; guidance in automatic manufacturing environments; inspecting and administering car thefts and vehicle tracking.

1.3 Underwater Wireless Sensor Networks

As wireless Network Sensors become smaller in size (dimensions) and cheaper, so that researchers are deploying them in the environment which is unconventional for electromagnetic waves to travel.

It has given the birth to the new and developing application of WSN that is Underwater Sensor Network. An underwater sensor network is made up of many autonomous and sensor nodes which performs data collection, storage operation and forwarding operation. The communication done by the nodes in underwater is through the acoustic channel. The propagation speed of acoustic signals in underwater is typically 1500m/s.

We use acoustic signals in underwater network because radio waves do not propagate in a well manner in underwater because of high energy absorption of water. Also the power consumption in underwater communication is much higher than the terrestrial radio communication. Due to absorption, the acoustic band for underwater is limited, most of the acoustic system operate below 30 kHz.

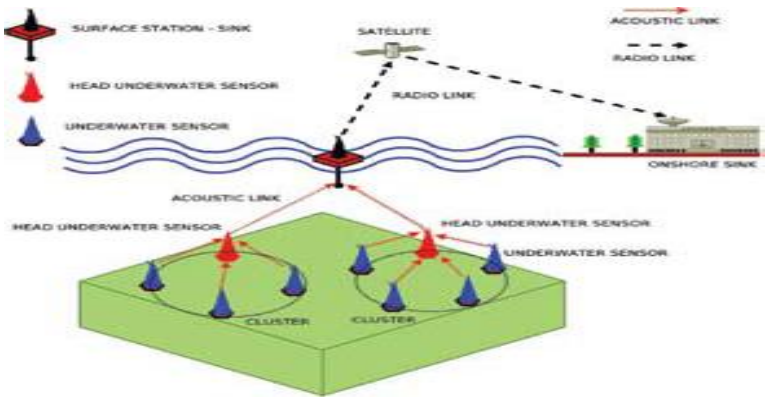

Figure 1.2: Architecture of Underwater Sensor Network.

1.3.1 Application of UWSNs

Inspite of all these problems, underwater sensor network have many potential applications such as:

- Seismic Monitoring.
- Swarm under water robots.
- Fish or micro-organism tracking.
- Equipment monitoring and leak detection.
- Undersea earthquake study.

1.3.2 Routing Protocols for UWSNs

Due to the challenges such as propagation delay, high bit error rate and limited bandwidth, the communication routing proposed for terrestrial network cannot be applied to UWSNs.

UWSNS routing protocol can be classified into:

a. Localization based and

b. Localization free routing protocol.

Generally, Localization protocol is not preferred because of the harsh environment underwater and mobility of nodes. Therefore localization free routing protocol is preferred and demanded by researchers.

a. Localization based routing protocol

These protocols depend on the localization of nodes in UWSNs.

1. In Vector Based Forwarding (VBF) protocol, a source node calculates a vector from itself towards the sink and nodes forward the data packets. But VBF has limitations, of hard assumption of sensor localization and sensor node unavailability in the routing pipe.

2. Hop-by-Hop Based Forwarding (HHVBF) is the successor of VBF, it computes the routing vector at each hop starting from each sender towards sink.

3. Focused Beam Routing (FBR) uses the different power levels of transmission during the next relay node selection, by broadcasting the packet RTS (request to send) and the receiver reply with CTS (clear to send) packet. The drawback of FBR is time delay during transmission of RTS and CTS packets and high energy consumption.

4. Directional Flooding Based Routing (DFBR) use the concept of scoped flooding where only limited number of nodes can participate in forwarding the data. The scoped flooding zone can be decided on the angle among the source, current forwarder and the sink node.

b. Localization free routing protocols

The routing protocols which do not assume any kind of localization are known as localization free routing protocol.

1. Depth Based Routing (DBR) protocol uses the depth of the node as a routing metric and assumes that each sensor node has a depth sensor. This protocol suffers from the transmission of redundant packets and extra energy consumption because of long propagation delay in underwater network.
2. In Hop by Hop Dynamic Addressing Based (H2-DAB), the routing can be done using Hop ID (address assign to each node), based on the hop count from the Sink node. The Hello packet is broadcasted by the sink node and receiving nodes are assigned a Hop ID. These receiving nodes then rebroadcasted the Hello packet after an increment in the Hop ID. The drawback is also delay and excessive energy consumption.

1.4 Security in WSN

Wireless Sensor Networks has laid down on the foundation of combination of sensor nodes and sink nodes. There are the constraints in sensor node such as low power, limited storage, low latency, low bandwidth, small physical size. These constraints are the obstacles to sensors security.

There are different types of attacks that can be took place during the communication among the nodes. So security is an important concern of WSN. In this section we discuss the different types of attacks in WSN.

a. Active attacks

These types of attacks are responsible for destruction in the network. The physical damage in network like alteration of data, destruction of resources, changing traffic direction are done by these attacks which can be easily identifiable and therefore we can stop the attackers.

b. Passive attacks

In this attack, the attacker observes the different activities in the network, check confidential information but do not bring any physical damage to the network. However the passive attackers can launch active attacks and become a cause of big damage because the passive attacker can find the weak points and clues in the network during observations of different activities and whenever he got the chance to attack, he will attack. Passive attacks are more dangerous as compare to active attacks because in this attack you are unable to identify your attacker.

c. Flood attack

Karlof in 2003 introduced a attack named flood attack in WSNs. In this attack Hello packets are used to down the network. The attacker floods Hello messages in the network that are dispersed in the whole network. In this attack, the attacker pretends that sender of packet is in their , and then when any sender node tries to transmit any sensed data to the sink node then they forward it towards the malicious (attacker) node, because they thinks that the attacker node is in their and therefore information forwarded towards BS can be easily access by the attacker.

d. Black hole attack

In this attack, the attacker node act like a black hole, where the attacker node listen to the route request packets from his neighbors and respond them back using wrong (fake) information about

shortest path towards sink node. So any node who wants to send the data to the BS will forward it to attacker.

e. DOS (Denial of Service) attack

The main aim of this attack is to waste the available resources of the network by sending the extra packets in the network without any need and keep the route and Base Station busy so that authorized users are unable to send data and access the resources.

f. Information Alteration

It is the responsibility of a sensor node to sense the data from its physical world and transfer that data towards Base Station. But in the middle of propagation of data there is chance of spoofing data by an attacker, so that he alters the message to misguide the BS. Here the attacker can observe all the traffic inside the network therefore if the attacker did any alteration then we can identify it and detect the attack but if he observing all the activities and ask someone else to attack then it can be very difficult to prevent such attack.

g. Wormhole attack

This attack happen when a sender (transmitting node) transmits a message to the receiver (receiving node) and then the receiving nodes attempts to transmit the message to its neighbors. The neighbor thinks that the message was transmitted by the sender (transmitting node), so they tries to send the message to the originating node but because it is too far away from them so this message never arrives.

h. Looping

In this attack some of the nodes in the network cause the circulation of data packets in a specific ratio. This attack stops the data packet to reach to the destination node and make it revolve in the same region which increases the traffic in the network.

i. Sybil Attack

Wireless Sensor Networks are more vulnerable to Sybil Attack and this attack is very harmful to the sensor network as this attack can make the network easily vulnerable to other attacks. Because this research concentrates on Sybil Attack, therefore now we will elaborate this attack briefly.

1.5 Sybil Attack

Douceur has first identified the Sybil Attack. In this attack, the attacker pretends to be at different places at the same time. The Sybil node has multiple fake identities. This Sybil node transmits the false information to another node in the network. This false information can be anything such as position of node, making up node that do not exit, signal strength.

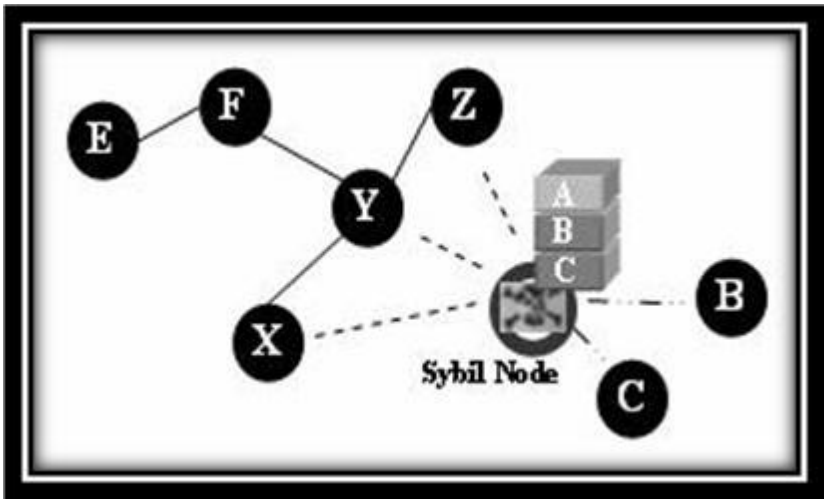

Figure 1.3: Sybil Attack.

Therefore an attacker using Sybil identities will communicate with legitimate node (authorized nodes) and get the access to the sensitive information and affect the normal working of the network. To illustrate the Sybil attack deeply, take an example.
Let us suppose a network with legitimate nodes A, B, C and D.

Note that the adversary can replicate the nodes by using the stolen information and these fake nodes can easily placed at several locations and communicate with nodes, so that the replicated nodes able to participate in the network.

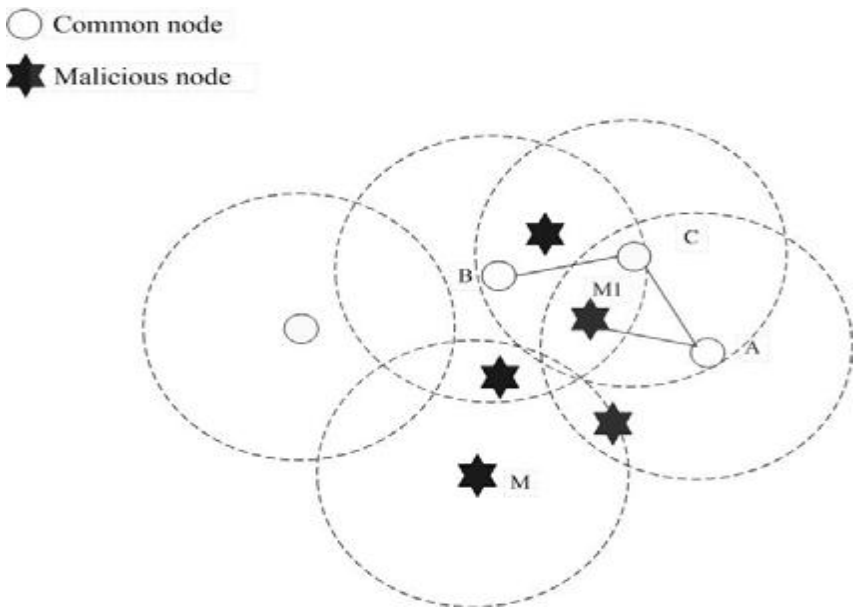

Figure 1.4: An example of Sybil Attack.

Under normal conditions, the common node A is not in the range of communication range of node B. therefore they are unable to communicate with each other directly but can share information via node C. When attack happens, malicious node M clones come into play. When node A broadcasts to establish a route to node B, M1 will immediately respond to A, claiming itself as a destination node. This will lead the node A to take node M1 for node B. So that attacker can access the sensitive information.

1.5.1 Types of Sybil Attack

It is important to understand the different forms in which the network is attacked to prevent the Sybil Attack.

a. Direct and Indirect communication

The legitimate (authorized) nodes communicates directly with Sybil nodes in direct communication while in indirect communication, the legitimate nodes communicate with Sybil node through malicious node.

b. Fabricated and Stolen identities

In fabrication, the Sybil node fabricate (create) a new identity for itself according to the identities of the legitimate nodes. Suppose if an authorized node have an identity with 32-bit length integer then Sybil node create ID of 32-bit integer randomly. While in stolen identity method, an attacker

identifies the legitimate node identities and then use it. The attacker cannot be identified if the node whose identity stolen is destroyed.

c. Simultaneous and non-simultaneous attack

In simultaneous attack, at the same time, all the Sybil nodes participate in the network and only one identity appears at a time. While in non-simultaneous attack, the attacker uses the number of identities is equal to the number of physical devices where each device presents different identities at different times.

1.5.2 Existing Detection Methods of Sybil Attack

a. Radio Resource Testing

In radio resource testing, here is an assumption that every device in the network has only one radio which is capable of simultaneously transmitting and receiving on one channel. Suppose that a node wants to verify that none of it is a Sybil node, so this node will assign each of its neighbor a different channel to send a message on and request that all send a message at same time. After that node will randomly choose a channel to listen on and if node received nothing that will conclude that channel to the node is a Sybil node.

Drawback of this method is when there are enough channel available to assign each a different channel and in this prevention method, the node can only test some set of its s at one time, so if there 'n' channels, then the node can test 'n' neighbors at once.

a. Trusted certification

John R Douceur presented the trusted certification method in which each node in the network have some certificate (some unique information that cannot be forged) issued by CA (certificate authority). This is the duty of CA to make sure that each certificate is unique and each node has only one certificate.

John R Douceur also proves that without the presence of CA, it cannot be possible to prevent Sybil Attack completely but he was unsuccessful to provide formal method to establish this uniqueness because this method can only be employed by human or manual intervention. Symmetric and Asymmetric Encryption are the example of this technique.

In symmetric encryption same key enables encryption and decryption of a message and in asymmetric encryption which is also known as public key cryptography (PKC), the public key is

used for encryption and the private key is used for decryption. In this approach, one can broadcast the public key, but only the corresponding private key can decrypt the encrypted message.

b. Random Key Pre-Distribution

Key pre distribution (KPD) is a challenge for key management schemes in which key are stored in each node before the deployment of nodes by CIA (central identification authority)/ TIA (trust identification authority)/ TBS (trusted base station).

In random key pre-distribution scheme, before the nodes deployment each node is loaded with a random set of 'N' keys from a pool of available keys. After the process of deployment of nodes, each node exchanges it stored keys with the nodes and establishes a secured link if they find a matching pair. However, if two nodes unable to find a matching pair then they can still communicate with each other if they manage to find another third node which shares a key with both of them.

In this method, here is also validation of key where validation ensures that network is able validate the key that a node might have. So, the Sybil node cannot pass the key validation test because the keys associated with the random identity will not heaven intersection with the compromised key set.

c. Localization techniques

Localization is the process of calculating the node position with the help of reference nodes. In the wireless sensor networks, these reference nodes are also known as Anchors because their position is known to the network. And these nodes can be either Base Station or cluster head. The nodes whose location has to be find called unknown nodes**.**

Generally, there are two methods of localization algorithms:

- Three point localization method and
- Angle localization method.

In the algorithms, the data assumes is the distances or angles, are available. In the first algorithm the requirement is the distance between the unknown nodes and at minimum 3 anchor nodes which are not in one line and in one place. The second algorithm requires the angle between the unknown node and two anchor nodes, distance of two anchor nodes.

These algorithms uses this information and then uses Euclidian geometry, triangulation or max. likelihood estimation methods to localize the position of unknown nodes. It can be noted

that minimum only two anchor nodes require for localization but for simplification of the above methods uses 3 anchor nodes.

- RSSI (received signal strength indicator).
- AOA (angle of arrival).
- TDOA (time difference of arrival).

These are the examples of localization techniques. Sybil node can be detected because one of two reasons:

1. If the identity presented by the unknown node that is known by the system but location is different to what has already been mapped, this will give indication to the system that a malicious node is stealing an existing identity. Note that here WSN is static in nature mean to say nodes are not moving.
2. If the identity presented by the unknown node that correlates to a position that is known to be mapped to another node, then this unknown node is a Sybil node.

Localization can be done in one of two ways:

1. Centralized Localization: All information is gathered to a central node which is more powerful node as Base Station or a cluster head, where algorithm of localization is executed. The advantage of centralized localization is it requires more memory and computational power to execute the algorithm which will provide more accurate localization result.
2. Distributed Localization: it is a localization method in which the information is interchanged between different nodes.

d. RSSI (received signal strength indicator)

RSSI is a technique which uses the signal strength to find the physical location of a node to detect Sybil attack. RRSI value can be found by the form

$$R_i = \frac{Po\ K}{d^{\alpha}}$$

where,

Ri= RSSI.

P0=Transmitting power.

K=Constant.

D= Distance between node i and node 0.

Alpha= distance-power gradient (i.e. path loss parameter).

RSSI method calculates the received power of incoming signal and relates this information with unique location and subsequently a unique ID. Generally there are several nodes uses to measure this value in order to triangulate this position. In a system if a node receives another message having the same physical location but claims to have a different identity then the system will conclude that this node is a Sybil node.Generally 3 nodes are required to locate a node but in the case of RSSI method, 4 nodes are required to complete the task accurately and effectively. Example will demonstrate RSSI in mathematical terms. Now, assume that S1 and S2 are the same node but have two different identities. D1, D2, D3, D4 are the four Detection nodes. When Sybil node attack happens i.e. S1 and S2 broadcast messages, then the 4 Detection nodes comes into play.

$$\frac{RSSI(S1,D1)}{RSSI(S1,D2)} = \frac{RSSI(S2,D1)}{RSSI(S2,D2)}$$

$$\frac{RSSI(S1,D1)}{RSSI(S1,D3)} = \frac{RSSI(S2,D1)}{RSSI(S2,D3)}$$

$$\frac{RSSI(S1,D1)}{RSSI(S1,D4)} = \frac{RSSI(S2,D1)}{RSSI(S2,D4)}$$

If all of the above equations become correct then it is proved that S1 and S2 must be at same position and is a sybil node has two identities.

e. Time of Arrival (TOA)

TOA can be defined as the measured time at which the incoming message first arrives at the receiving node. The assumption in this method is that time delay $T_{i,j}$ between the transmitting node I and receiving node j is the distance between them divided by propagation velocity $v_{p.}$ Free space wave propagation models are used for this technique where $v_{p=}3*10^8$ m/s.

f. Time Difference of Arrival (TDOA)

TDAO method is an extended version of TOA method. In the TOA method, there are the requirements such as to know the actual timestamps when messages are transmitted and when they reached at the anchor node. Therefore there is the need of proper time synchronization for the whole network. Hence this technique TDOA uses the time difference of signal propagation between the unknown nodes and the anchor nodes (or beacons). By doing so, it reduces the requirement of proper time synchronization for WSN. There are two methods of achieving TDAO in WSNs:

1. The measurement of time of arrival (TOA) from an unknown node to two different anchor nodes (beacons) must be known and after that time difference can be calculated.
2. The second method is the calculation of distance by forcing the unknown node to resend message and after that by using triangulation or maximum likelihood estimation (MLE), the position of the unknown node cab be found.

1.5.3 Disadvantages

Each of the prevention schemes against the Sybil Attack that we have mentioned above has different tradeoffs. Most of prevention methods are not capable of defending every type of Sybil attack. Each method has different cost and relies on different assumptions. With the help of custom radio hardware, radio resource verification defense can be breakable, trusted certification can only be employed by human or manual intervention. Similarly all the techniques have some drawbacks and still research is going in this area by many of intelligent researchers. They are proposing new techniques or developing techniques to prevent Sybil Attack.

Table1.1: Various Techniques to prevent Sybil Attack in different application domains.

S.no.	Techniques to mitigate Sybil Attack.	Disadvantages / Limitations	Application Domain
1.	Trusted Certification	Significant performance overh and expense.	General
2.	Random Key Pre-distribution	Limited to Sensor networks	Sensor networks.
3.	Location/ Verification	Limited to only Ad-hoc netwo	Wireless Ad-hoc Networks
4.	RSSI (Received Signal Strength Indicator)	Costly and limited to sensor network.	Sensor networks

Chapter 2
LITERATURE SURVEY

Bo Yu et al.,(2013) [1], Cheng-Zhong Xu et al.,(2013), and Bin Xia et al.,(2013) explained that Sybil attack is a harmful attack to ad-hoc as well as for wireless sensor networks. In the research paper, authors proposed a method to detect Sybil attack by analyzing the signal strength distribution. Authors first find the position of potential Sybil nodes then uses RANSAC (random sample consensus) algorithm to counter sybil attack and they also uses PES (Presence Evidence System), with the help of PES, authors enhance the detection accuracy using statistical analysis. First, author's proposed a co-operative method to find the position of a suspicious node but due to some reasons this method not so accurate so, authors gave two solutions against the challenge, that is, PES and the statistical detection method. Although this schemes scheme cannot guarantee 100% detection.

John R. Douceur et al.,**(**2002**)** [2] explained that peer to peer systems facing the problem of security threats from faulty remote computing elements. If a single faulty entity have multiple identities, and if it is controlling a substantial fraction of the system, then this node is called as Sybil node and attack is called as Sybil attack. To prevent this attack, there should be proper trusted agency certify identities. The research paper proposed that without a logically centralized authority, Sybil attack cannot be prevented completely in the network.

Kuo-Feng Ssu et al.,(2009) [3], Wei-Tong Wang et al.,(2009), and Wen Chun Chang et al.,(2009) explained that need of a network security has become a critical concern because of the use of WSN grows rapidly in the military and civil domains. In the Sybil attack, a malicious node forges number of identities of legitimate node to disrupt the network protocol. Author's proposed a method to detect Sybil attack. In the proposed scheme, the node identities can be verified by analyzing the neighboring node information of each node. All Sybil nodes have a same set of neighbors because all the identities presented by the Sybil node are associated to same physical node. But this condition cannot be satisfied with the normal node because each normal node has a unique identity and has a specific location at a time.

Navneet et al.,(2013) [4] and Rakesh Gill et al.,(2013) present the detection of Sybil attack using AODV in VANET. Sybil attack is a major threat in VANETs (Vehicular Ad-hoc Networks). It is the attack where a malicious node has the ability to presents different identities. There are several techniques developed to prevent this attack in VANETs. In this Sybil attack is detected using SCID (secondary ID). Here the packet format of AODV consist sequence number as well as secondary identity (SCID). The Sybil node creates the copy of the nodes, so it can have the same SCID. So that attack can be detected and then AODV select alternate path to transfer the information.

Md. Ahasan Habib et al.,(2012) [5], Jia Uddin et al.,(2012) and Md. Monirul Islam et al.,(2012) presents that in underwater network, the communication can be done by acoustic signal and acoustic communication network are very prone to malicious attack such as wormhole attack, sybil attack etc due to high transmission power, high bit error rates and low bandwidth of acoustic channels. In order to achieve the optimal performance of the network there is the need of the efficient and reliable security mechanism.

In underwater networks, the Sybil attack is major threat in which an attacker node with multiple identities can pretend to be at different places at once in the communication path. Proper authentication and position configuration are the techniques which can be use to prevent Sybil Attack.

Nitish Balachandran et al.,(2012) [6] and Sugata Sanyal et al.,(2012) presents that a malicious node which claims to have multiple identities in the network is a Sybil node. Sybil node disrupts the proper functioning of the network. Such attacks may become the cause of major damage because on a large scale are difficult to detect. The author's research discusses the different schemes to prevent Sybil Attack, like trusted Certification with the help of CA (certifying authority), Location verification, RSSI- based schemes, Random Key Pre-distribution method. Research work discusses all the techniques with their application domain and disadvantages/limitations too.

Manju V C et al.,(2014) [7] presents that Sybil Attack is one of the harmful attack in sensor network in which forged identities are used by Sybil node to get an illegitimate entry into the

WSN. Due to Sybil attack, security is affected and information can be lost. To prevent this attack author proposed a combined CAM- Compare and Match approach and PVM- Position Verification Method scheme. If one approach fails to detect the attack another one can catch like try-catch method.

In CAM, each node gets its key value from Base Station dynamically so when any node wants to communicate with another node then it should provide their key which is given by BS. If the key is not matched with the key given by Base Station then it is a Sybil node. In PVM, the prevention from this attack can be done by verifying the position of nodes. Here the Sybil node goes with the multiple identities but cannot have same position a legitimate node do, so Sybil node can be detected by PVM method.

Mignxi Li at al.,(2013) [8], Yan Xiong et al.,(2013), Xuangou Wu et al.,(2013), Xianchun Zhou et al.,(2013), Yuhui Sun et al.,(2013), Shenpei Chen et al.,(2013) and Xiaoya Zhu et al.,(2013) presents that in WSN, the detection of replication attack has been a long standing problem. Sybil attack is one of replication attack in WSNs. In their research they proposed a Regional Statistics Detection scheme (RSDs) to prevent Sybil attack. RSD is an effective solution to 3 key issues: first, detection of Sybil attack by RSSI-based detection mechanism. Second, this protocol can prevent the network from a large number of nodes failure caused Sybil attack. Third, with the help of RSD, it is easy to achieve high detection rate with low system overhead. Authors run their protocol in a physical environment with 32 nodes and at the end of experiments result confirmed its high efficiency.

Atichart Tangpong et al.,(2009) [9], George Kesidis et al.,(2009), Hung-Yuan Hou et al.,(2009) and Ali Hurso et al.,(2009) propose Sybil Attack Detection mechanism for MANETs (Mobile Ad-hoc Networks) based on cooperative monitoring of network activities. In this scheme, no node is able to replicate its generated traffic. Asymmetric keys are used for hop by hop authentication that means the signature of a packet is the proof its observation and only the owner of private key can generate this signature and hence a sybil attacker will not be able to confuse the detection algorithm by fabricating false traffic observations.

Shahrzad Golestani Najafabadi et al.,(2012) [10], Hamid Reja Naji et al.,(2012) andAli Mahoni et al.,(2012) presents that for large sensor network applications, security is an important

issue especially when a sensor network monitors critical infrastructures such as electric power infrastructure. Sybil attack is one of the most disrupting attack for WSNs, in which a Sybil node forges multiple identities and therefore this node access the confidential information. A noble approach is used to prevent approach is used to prevent this attack which called SDTM (Sybil Attack Detection Using Traffic Monitoring). This scheme is based on the Traffic density around nodes and uses statistical method to detect Sybil node.

P. Raghu Vamsi et al.,(2014) [11] and Krishna Kant et al.,(2014) presents that in the field of WSN, the problem of Sybil Attack is widely considered by researchers. Among all the existing techniques/ solution to this attack, LSDF (Light Weight Sybil Attack Detection Framework) is presented which consist of two components, Evidence Collection and Evidence Validation. By observing the activities of neighboring nodes, every node in the network collects the evidences. To decide whether the neighbor node is a benign (legitimate) node or Sybil node, these evidences are validated by Running Sequential Hypothesis test. With the help of LSDF, a node approaches to a decision on deciding a Sybil attack with the related to location, RSS (Receiver Signal Strength) values, distance measurement.

Shanshan Chen et. al.,(2010) [12], Geng Yang et al.,(2010), Shengshou Chen et al.,(2010) proposed a security technique to mitigate the Sybil attack in the network which is basically based on the Leach routing protocol and RSSI technique. In this detection technique RSSI increase or improves the security of leach protocol. Each time when Sybil attacker changes its id, it will broadcast it to his neighbor nodes and claims that it is a cluster head. The number of cluster head is continuously collected I leach protocol. According to their mitigation technique technique, detection will started up until the number of cluster heads exceeds the value of N_{thread}.

Murat Demirbas et al.,(2006) [13], Youngwhan Song et al.,(2006) present that a node which broadcast the multiple node identities is a Sybil node. Their proposed solution for mitigation of Sybil attack is based on RSSI values of information messages. They shows that RSSI (Receiver signal strength indicator) is time varying and unreliable in general and transmission is nonisotropic so to overcome these problems they uses multiple radio receivers.

Bin TIAN et al.,(2013) [14], Yizhan YAO et al.,(2013), Shuai SHAO ety al.,(2013), Zhaohui LIU et al.,(2013), Changxing XUet. Al.,(2013) present that with advances in the wireless communication technology and microelectronics technology to encourage the rapid development of low price, low power, multifunction sensor and wireless sensor networks have been extensively used in general. Due to the restrictions of node resources and scenarios, security becomes a major issue which is like an obstacle to the wireless sensor network. Among different attacks, sybil attack is a major attack. Researchers proposed sybil attack detection scheme which is based on the location of the anchor nodes. In this technique, very simple localization method is used which do not require any additional special equipmentlike GPS.

Shaohe Lv et al.,(2008) [15], Xiaodong Wang et al.,(2008), Xin Zhao ety al., (2008), and Xingming Zhou et al.,(2008) presents that Sybil node is a malicious node which declare numerous illegal identities which confuses or even fall down the network. To prevent this attack researchers proposed a detection scheme named CRSD which can work in only static wireless sensor network. It uses the received signal strength to calculate the distance between two identities and then determines the positions of the identities by using the RSS information from multiple neighbor nodes so when two or more different identities have the same position that depicts the Sybil node and this node further will be detected.

Xun Li et al.,(2013) [16], Guangjie Han et al.,(2013), Aihua Qian, Lei Shu et al.,(2013) and Joel Rodrigues et al.,(2013) presents that Sybil Attack is one of the most common and harmful attack in the Underwater Sensor Networks. Author's proposed their scheme to detect the Sybil attack, the scheme is based on state information of nodes.

UWSNs consist of large number of sensor nodes, which are deployed in the water environment to gather data. These nodes suffer from limited memory capacity and computational ability. Because of these resource constraints, UWSNs faces variety of assaults. In the research, the deployment of nodes is normal distribution, the environment consist of 100 normal nodes, 200 beacons and 20 Sybil nodes. All nodes have the same transmission range of 10 m. The beacons periodically broadcast a query in its communication range, some nodes receive the packets, these nodes update and maintain the information list and then reply to the beacon. It uses radio energy model.

$$E(K,R) = E_{elec}\, K + E_{amp}\, Kd^2$$

where, K: bits.

E_{elec}: Energy needed for transceiver circuitry.

E_{amp}: Energy needed to process one bit of data for transmitter amplifier.

d: communication radius of node.

In the Basic scheme of the research, author's provided method to detect Sybil node.

a. Node A broadcast a query packet in his communication range.

b. If a node which is not in list of A, do not respond him, then it is a Sybil node.

c. If node A get the response from a node whose identity has never appeared in A's neighbors list, then it is a Sybil node.

d. Because of the change in the network topology, some nodes exhausted in energy and become dead nodes, so they cannot communicate and therefore they are also considered as Sybil node and remove from the network.

e. If the two results of residual energy received at the beacon are in contradiction then the nodes will regarded as Sybil node.

In order to fully detect Sybil Attack in the network, author's uses the state information of every suspicious node.

Chapter 3
PRESENT WORK

Wireless Sensor Networks are composed of many small devices called nodes which are the most basic building blocks for the network. Wireless Sensor Networks has laid down on the foundation of combination of sensor nodes and sink nodes. There are the constraints in sensor node such as low power, limited storage, low latency, low bandwidth, small physical size. These constraints are the obstacles to sensor security. Wireless Sensor Networks are more vulnerable to Sybil Attack and this attack is very harmful to sensor network. Douceur has first identified the sybil attack. In this attack, the attacker pretends to be different places at the same time. The Sybil node has multiple fake identities. This Sybil node transmits the false information to another node in the network. This false information can be anything such as position of node, making up node that do not exist, signal strength.

In recent years, WSN is widely used in the fields of military, Environmental monitoring, medical area and forest monitoring etc. Because nodes have limited power , limited storage and limited computational resources therefore it can easily be attacked. Sybil attack is one of the most of the harmful attack this attack can make the sensor network easily vulnerable to the other attack. Sybil node is a node which claims multiple identities. Now a days sybil attacker threaten the WSN in voting system, routing, Fair resource allocation. Hence many detection methods are being proposed to prevent Sybil Attack in Wireless Sensor Network.

3.1 Problem Formulation

Wireless Sensor Networks has laid down on the foundation of combination of sensor nodes and sink nodes. There are the constraints in WSNs such as limited power, limited storage, latency, low bandwidth, small physical size and these constraints are the obstacles to WSN security. Among different types of security attack, WSN is more vulnerable to Sybil Attack as this attack can make network easily vulnerable to other attacks. A Sybil node has multiple fake identities which communicate with the legitimate nodes and get access to the sensitive information and affect the normal working of the network.

There are many existing detection methods of Sybil attack such as:

-Radio resource Testing.

-Trusted Certification.

-Random Key Pre-Distribution.

-Localization Techniques.

-RSSI (Received Signal Strength Indicator).

-TOA (Time of Arrival).

-TDOA (Time Difference of Arrival).

These all prevention techniques we have already discussed in the Chapter 1. Each of the above mention prevention schemes has different trade off and are not capable of defending every type of Sybil Attack.

Xun Li et al.,(2013) [16] presents that Sybil Attack is one of the most common and harmful attack in the Underwater Sensor Networks. Author's proposed their scheme to detect the Sybil attack, the scheme is based on state information of nodes.

UWSNs consist of large number of sensor nodes, which are deployed in the water environment to gather data. These nodes suffer from limited memory capacity and computational ability. Because of these resource constraints, UWSNs faces variety of assaults. In the research, the deployment of nodes is normal distribution, the environment consist of 100 normal nodes, 200 beacons and 20 Sybil nodes. All nodes have the same transmission range of 10 m. The beacons periodically broadcast a query in its communication range, some nodes receive the packets, these nodes update and maintain the information list and then reply to the beacon. It uses radio energy model.

Therefore because of high accuracy of detection scheme named "Detection of Sybil Attack based on State Information of nodes". The simulation results demonstrate that the detecting accuracy can be upto 94 precent. Therefore because of better accuracy in the detection rate given by State Information technique I have decided to improves the detection rate by improving some parameters of State Information technique. First we implemented existing technique i.e. State Information on MATLAB according to the following steps:

-First we deploy normal nodes with the communication range of 10m. The number of nodes are user defined.

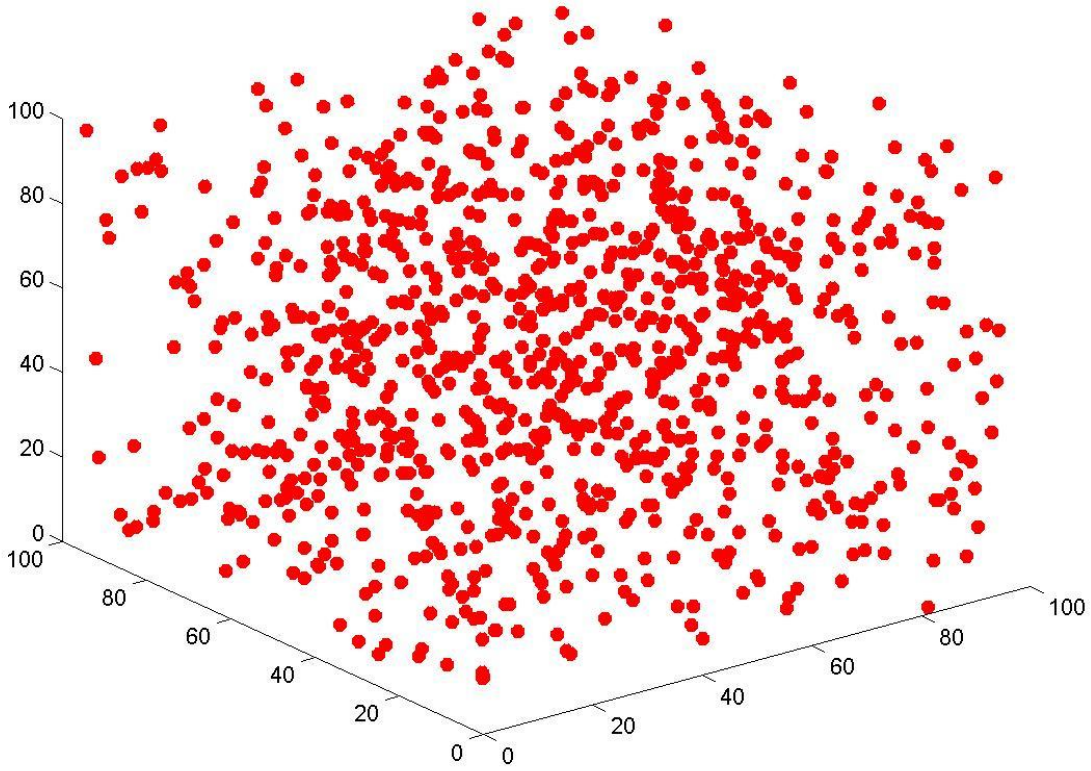

Figure 3.1: A WSN with 1000 sensor nodes deployed randomly in 100m *100m*100m

- Then the selection of source node and destination node can be done. The node which is closer to the origin will be the source node and the node which is closer to the extreme end of the node will be taken as destination node which shows the concept of multihop communication in better way.

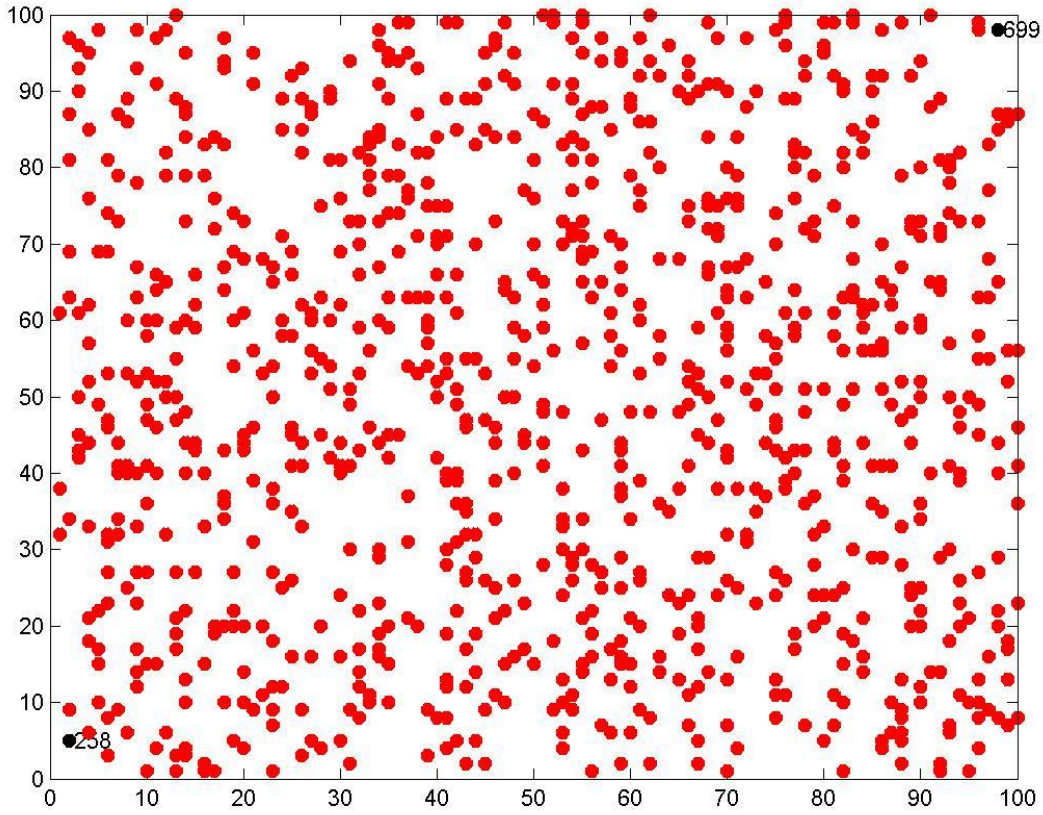

Figure 3.2: Selection of source and destination node.

- For making the route between the source node and the destination node, we will chose the relay nodes which will make the path for the source and the destination node on which information packet will be travelled and reaches its destination securely. As each node has transmission range of 10m, therefore the relay nodes will be chosen according to the concept that the node which is far away to the previous node in communication range will be regarded as relay node, and this method will go on until there is the formation of proper path from source to destination node.

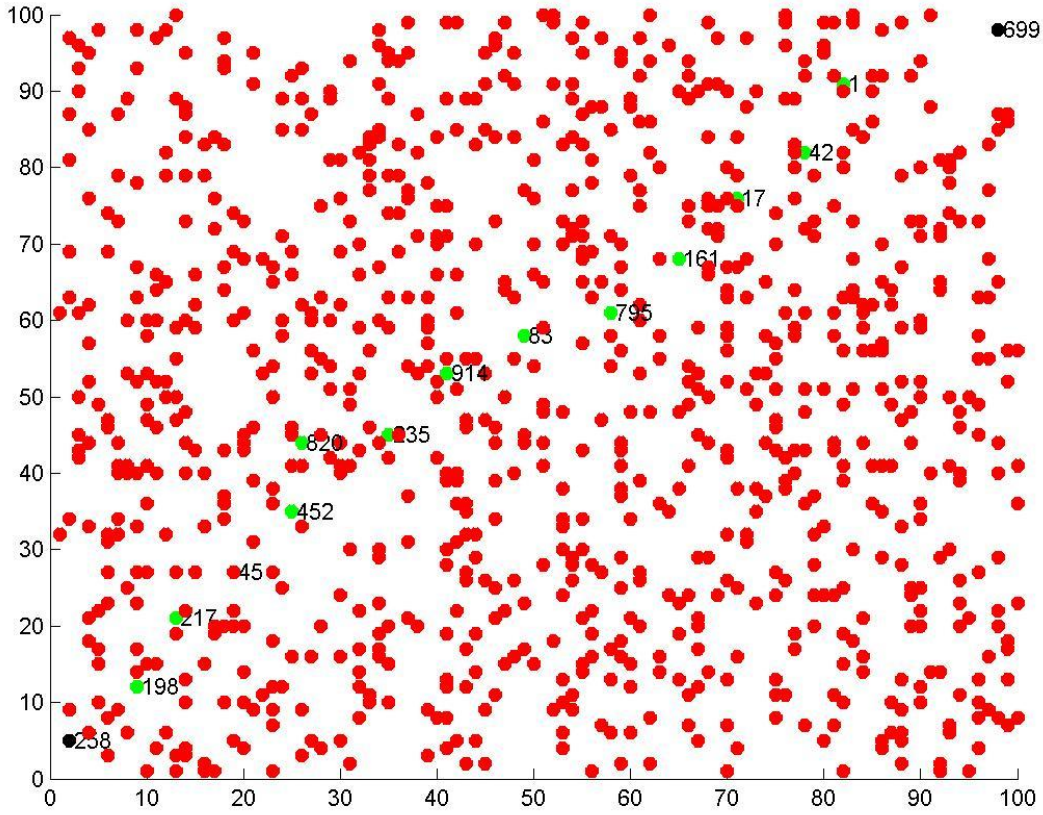

Figure 3.3: Formation of path from source to destination via relay nodes.

-Now the transportation of information packets will take place. The packets travels from source to destination via relay nodes.

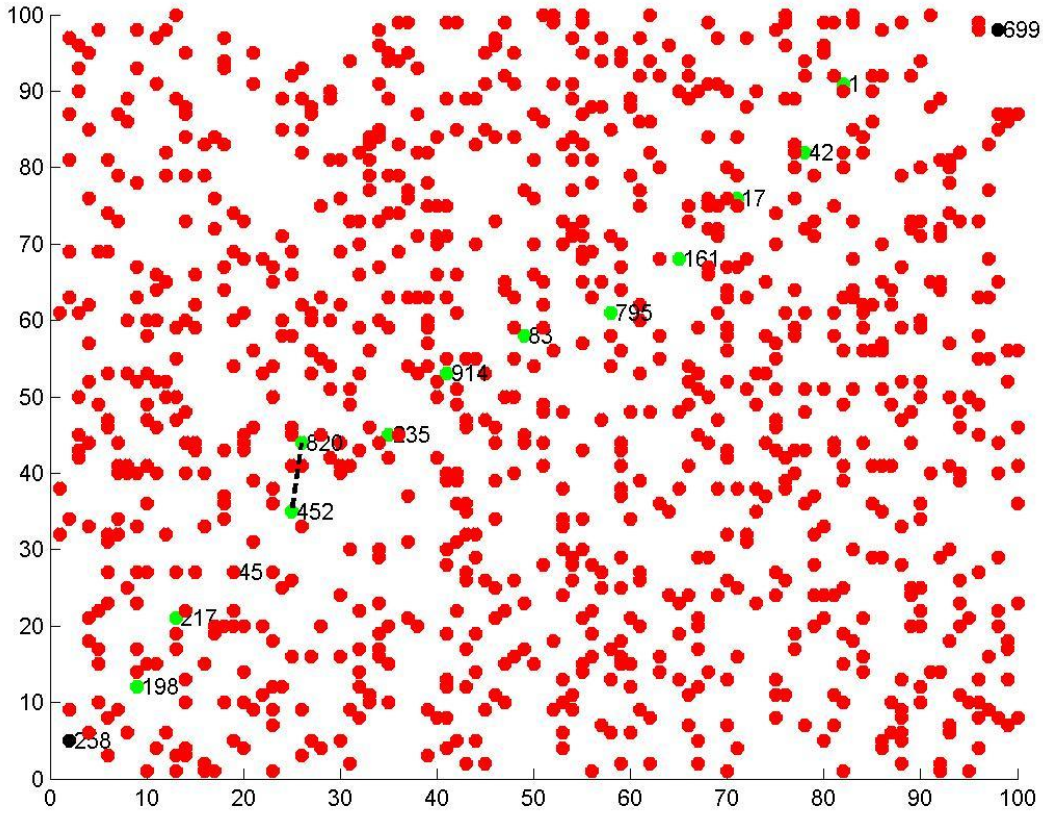

Figure 3.4: transportation of packets from source to destination via relay nodes

- Now, the Sybil node comes into play. Sybil node will forge identity of any relay node randomly. So when the information packet reaches to the relay node which is previous relay node to the relay node whose identity is forged will get confused and forward the packet to the sybil node and attack will occur.

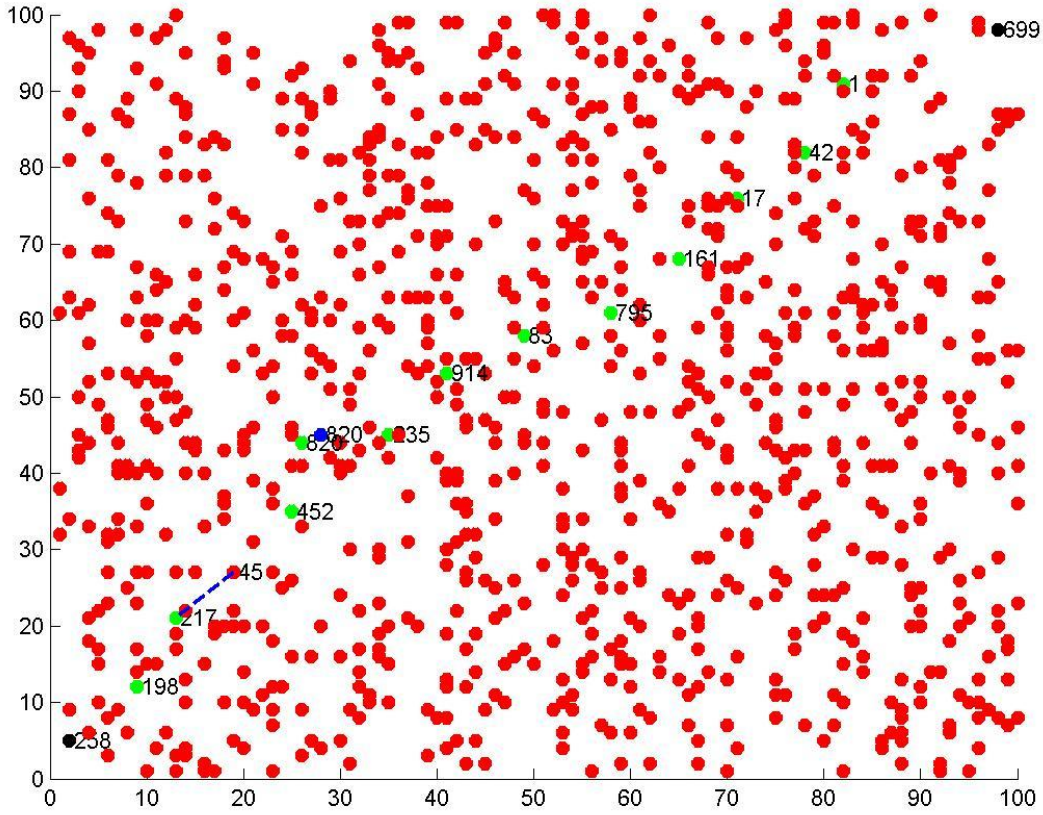

Figure 3.5: Sybil attack.

- Now, the Sybil node comes into play. Sybil node will forge identity of any relay node randomly. So when the information packet reaches to the relay node which is previous relay node to the relay node whose identity is forged will get confused and forward the packet to the sybil node and attack will occur.

-Now, we deploy the 1000 normal nodes and 200 beacon nodes with specific communication range i.e. 10m. Now we create the neighbor list of beacon nodes and further deploy the 20 Sybil nodes. After the creation of neighbor list, energy model will be used for calculating the residual energy of nodes. The energy model for sensor node is based on the first order radio model. In this model, transmitter and receiving circuitry requires power. Each node in the network has the same initial energy available. If a message of k-bit is send over the distance R then consumed energy will be:

$$E(K,R) = E_{elec}\, K + E_{amp}\, Kd^2$$

Where k is the number of bits , E_{elec} is the energy required for transceiver circuitry to deal with 1-bit of data, E_{amp} is the energy needed to process 1-bit of data for tx. Amplifier, d is the nodes communication

radius (d=R). The energy consumed when a node receives a k-bit data is $E_r=E_{elec}k$. in this energy model, the energy consumed when a node sends a packet is twice the energy consumed when a node receives a packet. , the beacon nodes in the network broadcast the query packet in its communication range (communication range is 10m). Beacon node only broadcast the query packets to the normal nodes, not to the Sybil nodes.

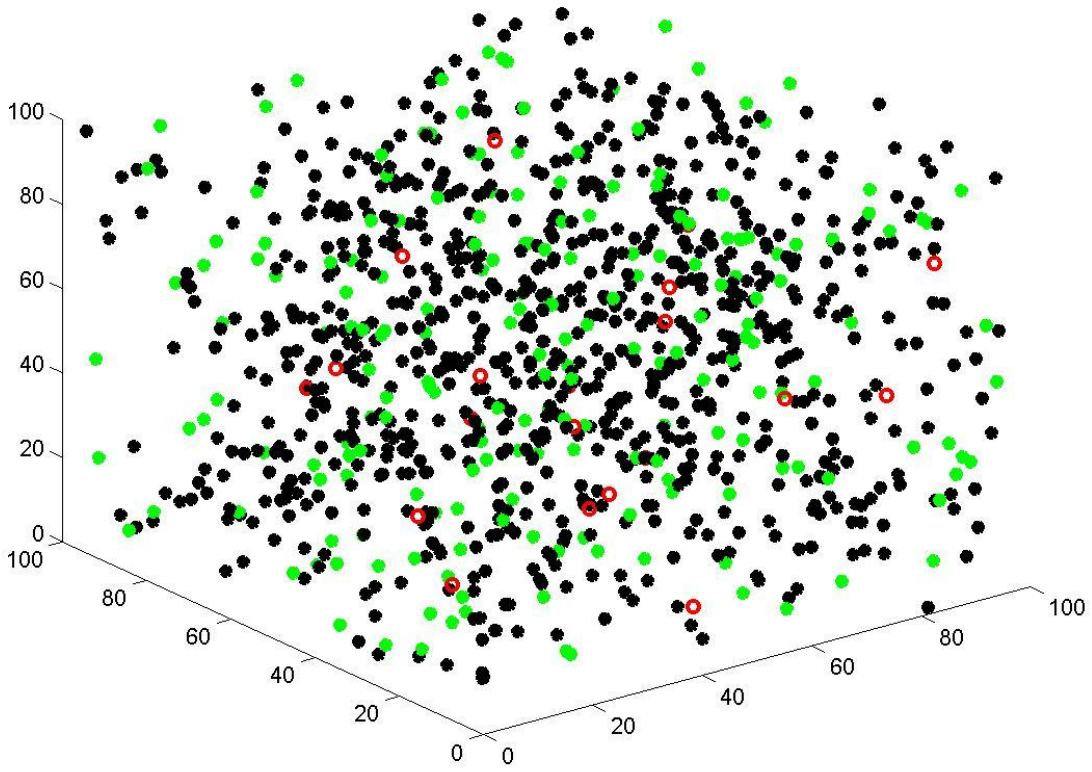

Figure 3.6: Deployment of beacons and sybil nodes in the network.

If any Sybil node has beacon node in its neighbor list, then Sybil node will reply to the beacon node. Beacon node check its neighbor list and detect the nodes whose identification is not appeared in neighbor list, therefore Sybil nodes will be detected. After that, beacon nodes check the residual energies of the normal nodes using radio energy model, if two result of the residual energies of the normal nodes are in contradiction, then the nodes will be treated as the Sybil nodes.

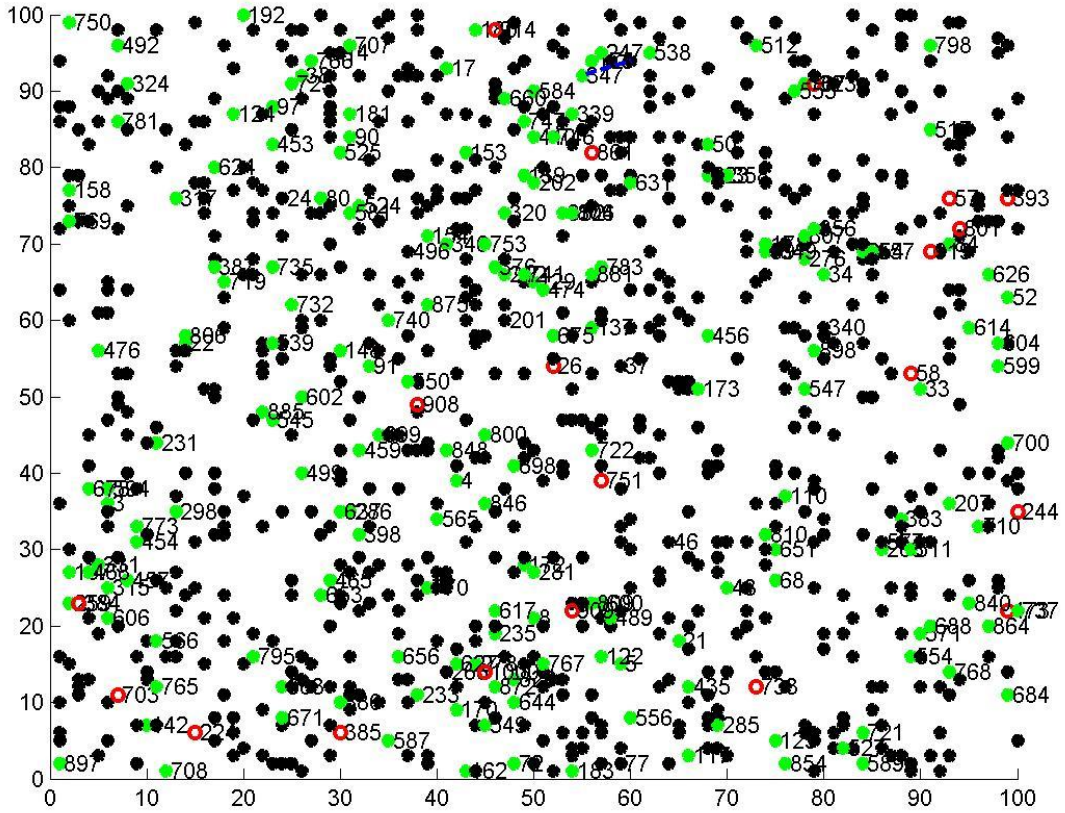

Figure 3.7: Detection of Sybil nodes by using beacons neighbor list.

Further for better accuracy in detection rate this technique uses different packet rates to detect Sybil nodes accurately. Beacon node starts timer (at specific Time period T) and then sends Ms packets to destination node. Destination node may receives Mr packets actually. Sender records the end of timer Tr and number of response packets Mr after receiving response (ACK) packets, then destination node deals with the Md packets at the same time. Now we calculate the different ratios i.e. Receive packets rate Rr, disposed packet rate Rd, Identification packets rate, Received time rate.

Formulas of different rates are as follows:

1. Rr = Mr / Md.
2. Rd = Md / Mr.
3. Ri = Mi / Ms.
4. Rt = Tr / T.

Now according to the above four different ratios beacon node calculates the evaluation of each node.

$E_i = \alpha N_d + \beta N_s$, $\alpha+\beta=1$…. Equation(1)

$N_d = \lambda R_r + \mu R_d$, $\lambda+\mu=1$…. Equation(2)

$N_s = \psi R_r + \varphi R_t$, $\psi+\varphi=1$….. Equation(3)

The evaluation of source node Ns and destination node Nd is done. The higher the evaluation then there will be safer the node. The node which has the lowest evaluation, beacon node chose that node as a suspected node. Then the query message is send by the beacon node to the suspected node.

Then the suspected node send its neighbor list to the beacon node which will calculates the suspected node's coordinates by using the distance between three neighbor nodes and the suspected node. Finally, compares the co-ordinates with the recorded co-ordinates to ensure that the suspected node is Sybil node. And then beacon node broadcasts Sybil node in UWSNs and remove it from the netwok.

As this technique using the beacon nodes for broadcasting the query messages to detect Sybil attack but drawback of this technique is that the all the Sybil nodes are not coming in the communication range of beacon nodes therefore all the Sybil nodes cannot be detected by State information scheme. Therefore in proposed scheme we overcome from this drawback and as a conclusion, detection rate improved. The proposed scheme is elaborated in next chapter. So in this semester in my problem, I am going to implement the Sybil attack model on MATLAB and also implement the detection of Sybil Attack based on State Information and enhanced techniques.

3.2 Objectives of Problem

- The main objective of the work is to improve the security level of Wireless Sensor Network with improved throughput.
- Designing a Sybil Attack model on MATLAB.
- Implementation of Sybil node detection scheme based on State Information of nodes and proposed enhanced scheme.

3.3 Methodology

Our focus will be on increasing the Sybil attack detection rate in underwater Sensor network using State information and enhance technique

I am going to do implementation in 2 phases:

1st Phase: Sybil Attack model

In Sybil attack model, we assume that Sybil node has the ability to duplicate the identity of normal nodes in the network. The Sybil node can replicate the normal node identity in the network. The sybil node can forged the identity of normal node by using the stolen information. The sybil node can be placed at different locations of network and then communicate with the neighbor nodes and then misguide the neighbors and affect the proper working of the network. We design the sybil attack model according to the following steps:

1. In the first step, we deploy 1000 normal nodes randomly in the network area of 100m*100m*100m.
2. All the normal nodes get their neighbor list.
3. Now, selection of source node and destination node will take place. The node which is closer to the origin will be the source node and the node which is closer to the extreme end of the node will be taken as destination node which shows the concept of multihop communication in better way.
4. For making the route between the source node and the destination node, we will chose the relay nodes which will make the path for the source and the destination node on which information packet will be travelled and reaches its destination securely. As each node has transmission range of 10m, therefore the relay nodes will be chosen according to the concept that the node which is

far away to the previous node in communication range ill be regarded as relay node, and this method will go on until there is the formation of proper path from source to destination node.

5. Now, the normal communication will take place.
6. Now, the Sybil node comes into play. Sybil node will forge identity of any relay node randomly. So when the information packet reaches to the relay node which is previous relay node to the relay node whose identity is forged will get confused and forward the packet to the sybil node and attack will occur.

2nd Phase: Detection of Sybil Attack using proposed scheme.

The proposed algorithm is the combination of state information of nodes and arrangement of nodes in Grids. In this enhanced technique, concept of grid is used which provided the better detection rate as compared to state information detection technique because of better accessibility and connectivity in the network. The proposed algorithm is describe below in steps:

1. First we deploy the 1000 normal nodes in the network area of 100m*100m*100m.
2. Here the concept of grid comes into play. All 3 axis i.e. x, y and z has the length of 100m. So, we form the grids by expanding the length parameter of x, y and z axis and I each grid, places the beacon node which improves the connectivity in the network and beacon nodes almost covers every part of the network. The total area of the network is 100m*100m*100m and size of each grid is 20m*20m*20m, hence the number of grids is 125. Because there are total 200beacon nodes, therefore out of 200 beacons, 125 beacon nodes are deployed in 125 grids and rest 75 beacons will be deployed randomly. First, we chose the beacon nodes from the grid size of 0-100*20*20 and after that variation will be along y-axis i.e. we chose the beacon nodes from the grid size 0-100*0-100*20. This process goes on until beacon nodes from 3-D network will be selected completely.
3. After the deployment of beacon nodes, deployment of 20 sybil nodes will take place in the network.
4. Now, the beacon nodes create its neighbor list.
5. After the creation of neighbor list, energy model will be used for calculating the residual energy of nodes. The energy model for sensor node is based on the first order radio model. In this model, transmitter and receiving circuitry requires power. Each node in the network has the same initial energy available. If a message of k-bit is send over the distance R then consumed energy will be:

$$E(K,R) = E_{elec}\, K + E_{amp}\, Kd^2$$

Where k is the number of bits , E_{elec} is the energy required for transceiver circuitry to deal with 1-bit of data, E_{amp} is the energy needed to process 1-bit of data for tx. Amplifier, d is the nodes communication radius (d=R). The energy consumed when a node receives a k-bit data is $E_r=E_{elec}k$. in this energy model, the energy consumed when a node sends a packet is twice the energy consumed when a node receives a packet.

6. Now, the beacon nodes in the network broadcast the query packet in its communication range (communication range is 10m). Beacon node only broadcast the query packets to the normal nodes, not to the Sybil nodes.
7. If any sybil node has beacon node in its neighbor list, then Sybil node will reply to the beacon node.
8. Beacon node check its neighbor list and detect the nodes whose identification is not appeared in neighbor list, therefore sybil nodes will be detected.
9. After that, beacon nodes check the residual energies of the normal nodes using radio energy model, if two result of the residual energies of the normal nodes are in contradiction, then the nodes will be treated as the Sybil nodes.

Summary of the proposed scheme:

1. Deployment of normal nodes in 100m * 100m * 100m area.
2. Choosing 200 beacon node from the Grids. Expand along X, Y and Z axis until beacon nodes from 3-d network are selected.
3. Deployment of 20 Sybil nodes and getting coordinates of sybil nodes.
4. Getting the neighbors of beacon nodes.
5. Calculating the Energy of each node using radio energy model:
   $$E(K,R) = E_{elec}*k+ E_{amp}*k*d^2$$
   where E_{elec} is the transceiver energy and E_{amp} transmitter amplifier energy and d is the communication radius of nodes.
6. Broadcasting of query packets by beacons in communication range.
7. Reply by the neighbors of beacon nodes.
8. Getting neighbors of Sybil nodes.
9. If any Sybil node has beacon node in its neighbor list, then Sybil node will reply to the beacon node.
10. Beacon node check its neighbor list and detect the Sybil node whose identification is not in neighbor list.
11. Checking the Residual Energies of normal nodes using energy model. If two results of the residual energies of normal nodes are in contradiction, then the nodes will be treated as the Sybil nodes.

Detailed proposed Algorithm:

x_cod = set of x coordinates of nodes.
y_cod = set of y coordinates of nodes.
z_cod = set of z coordinates of nodes.

Algo 1: choosing beacon nodes uniformly

```
for i=1:N                N:set of sensor nodes.
a=rand( )
      if a lies in 10*10*10 area
          beacon=a;
      end
end
```

Expand along X Y and Z axis until beacon nodes from 3-d network is selected.
If no. of nodes < 200
Choose remaining nodes randomly
end

Algo 2: Detection of Sybil nodes

N_b= set of neighbor nodes of beacon nodes.
B= set of beacon nodes.

```
for i=1:B
  each node in B – broadcast( );
  end
end
broadcast( )
node broadcast Query packets to all nodes in neighbor set.
for j=1: N_b
   for i=1:B
     each node replies to Beacon
     end
end
```

N_s = nodes that broadcast query messages.

N_l = nodes that recieve query messages.

R_q = nodes that responded to query messages.

for i= R_q

for j=1: N_r

if N_l ~= R_q

add node in suspected list

end

end

end

E= energy of all nodes

for i=1:N

if E_i ~= E_i+1

add node in suspected list

end

end

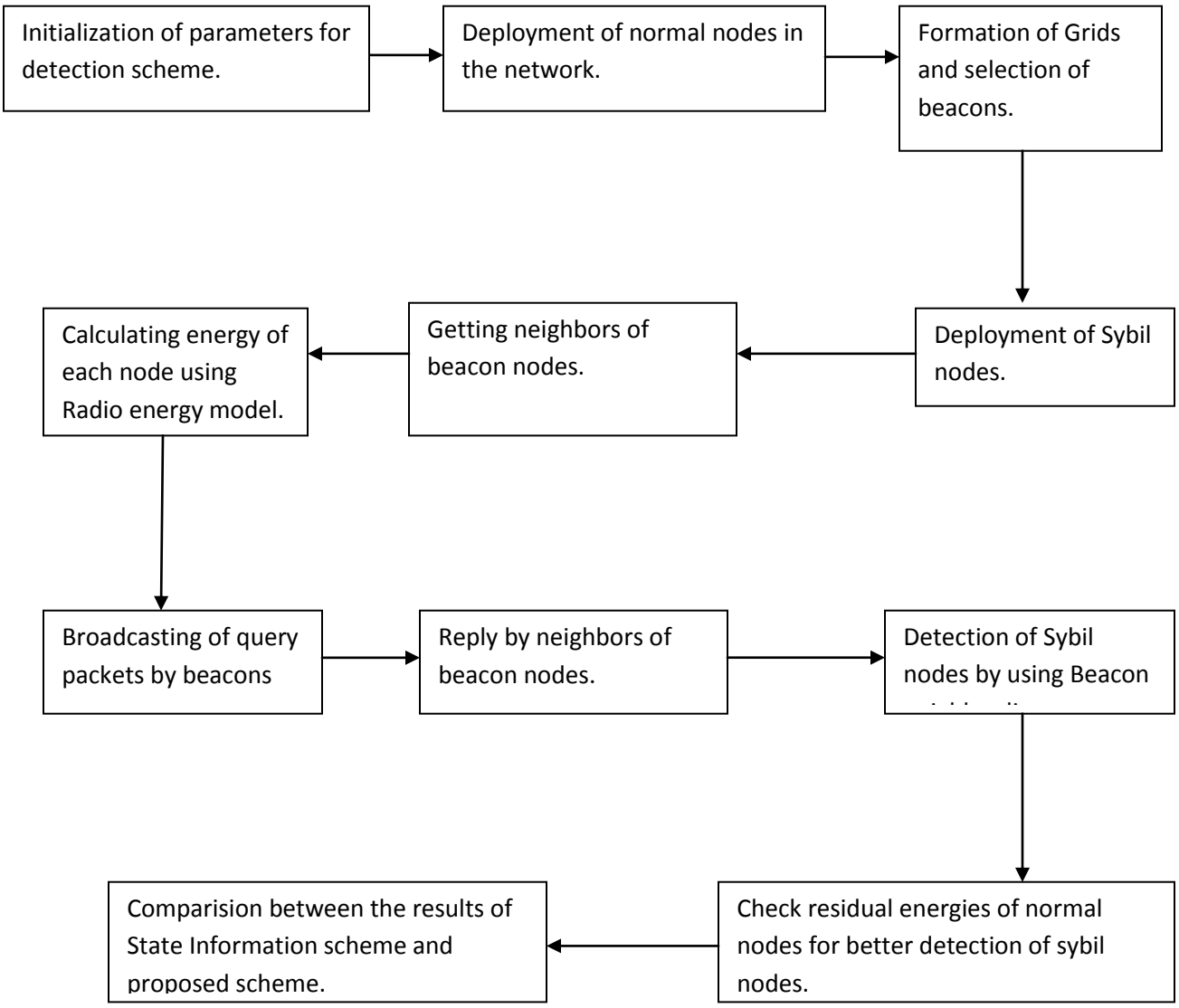

Figure 3.8: Block Diagram of Methodology.

Chapter 4

RESULTS AND DISCUSSIONS

4.1 Deployment of Sensor Nodes

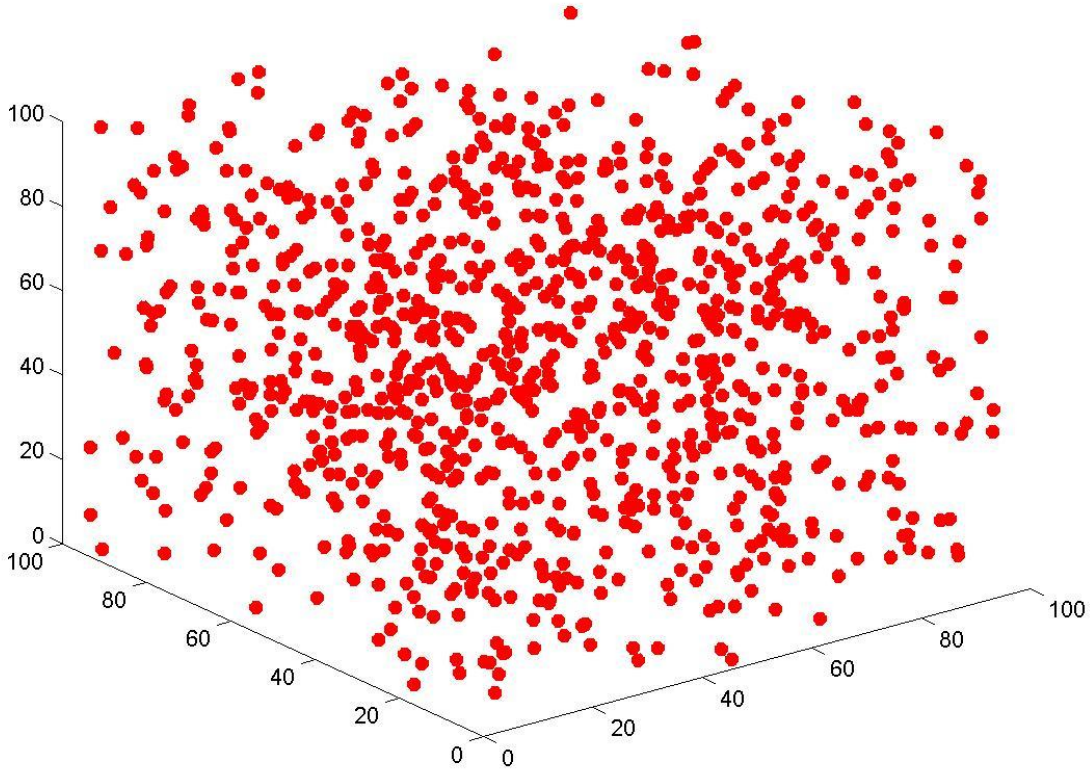

Figure 4.1: A WSN with 1000 sensor nodes deployed randomly in 100m *100m*100m

Figure 4.1 illustrates the random distribution of nodes in the network of 100m*100m*100m area.

4.2 Communication in Sensor Network

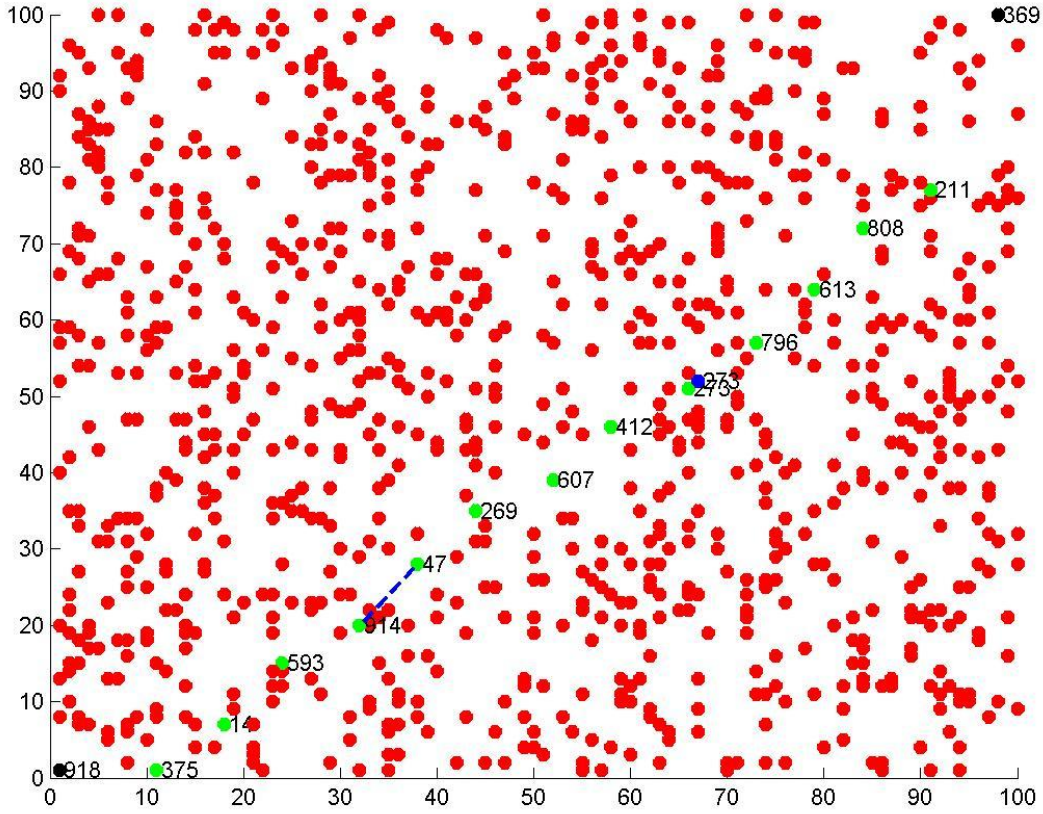

Figure 4.2: Communication between source node and destination node via relay nodes.

Figure 4.2 illustrates the communication between source node (id 918) and destination node (id 369) in the network of 1000 normal nodes. Figure also depicting the presence of 13 relay nodes and 1 Sybil node (stolen id 273) in the network which is having replicate identity of relay node (id 273). The message is passing through relay nodes from Source node to Destination node.

4.3 Sybil Attack Model

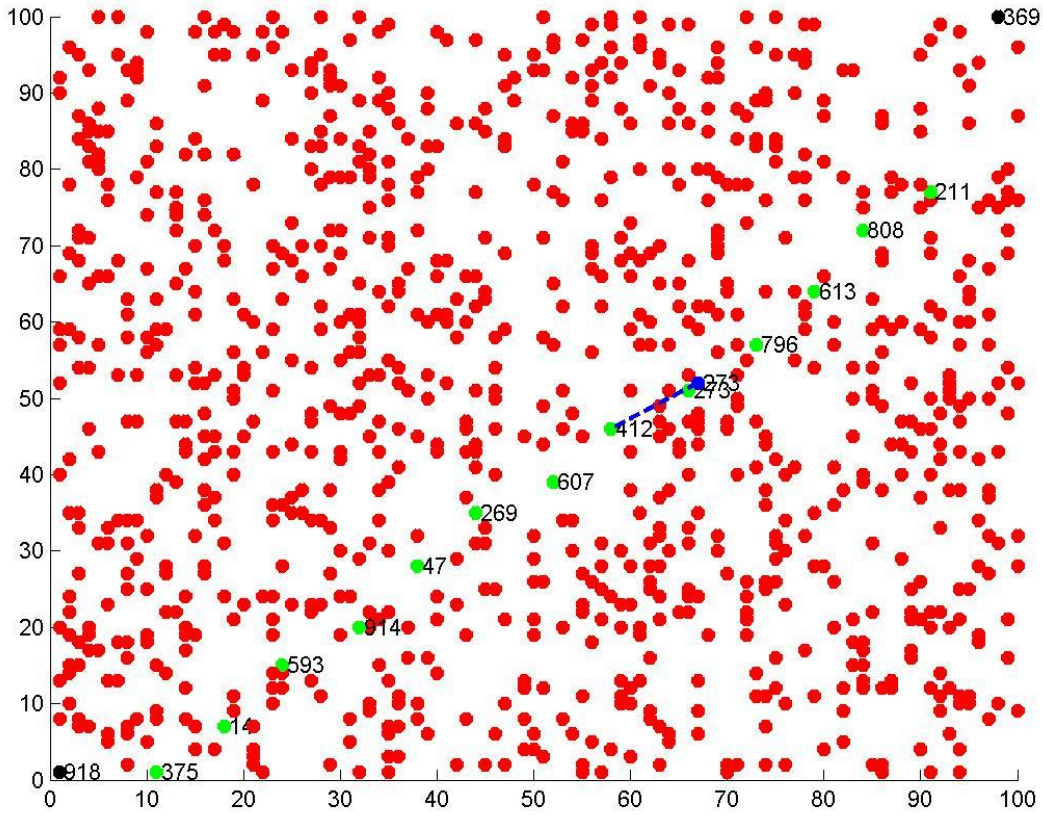

Figure 4.3: Sybil Attack occurs in WSN

Figure 4.3 illustrates the play of Sybil node. It is depicting that Sybil node has the replicate identity of relay node (id 273). When Source node forward the information packet through relay nodes and when this message reaches relay node (id 412) then this relay node will be misguided by Sybil node and this relay node forward the data to sybil node as shown in figure. This is a Sybil Attack model in WSN.

4.4 Direct Communication in Sensor Network

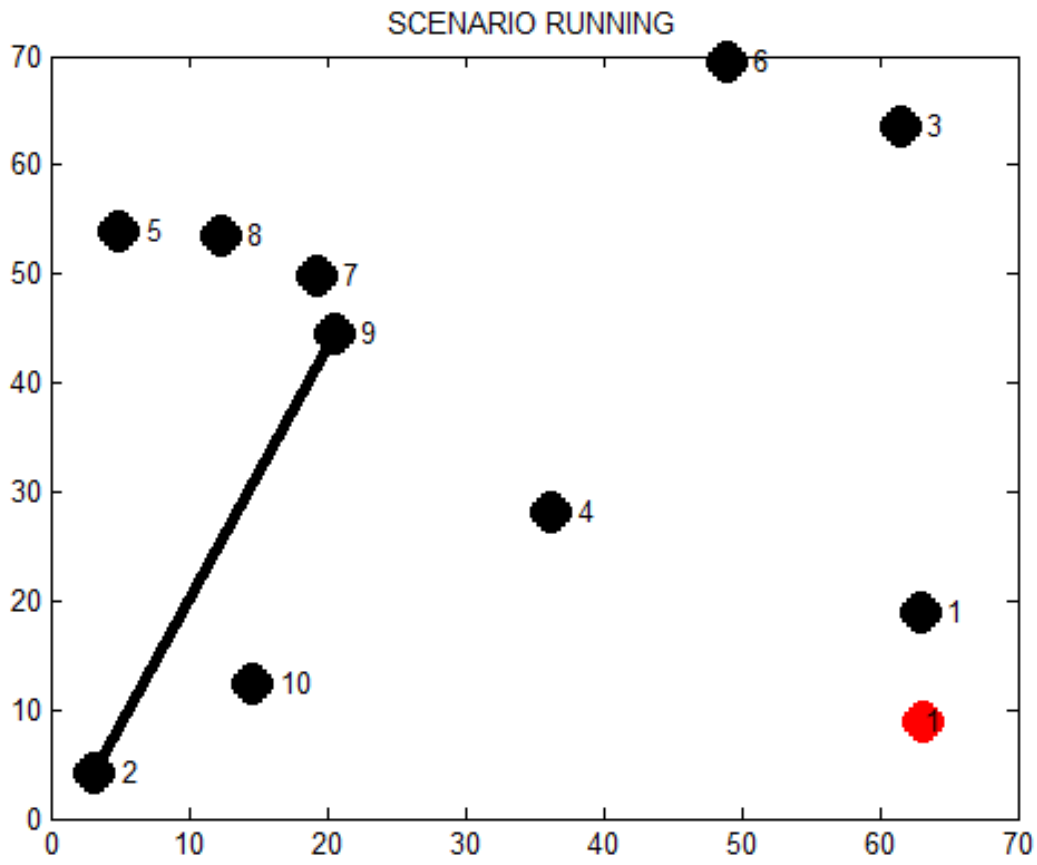

Figure 4.4: Communication between source node 2 and destination node 9

Figure 4.4 illustrates the direct communication between source node and destination node in the network of 10 normal nodes. Figure also depicting the presence of Sybil node in the network which is having replicate identity of node 1.With respect to the change of time, Sybil node change its identity and when it will have fake identity of destination node 9 then attack will occur.

4.5 Direct Sybil Attack Model

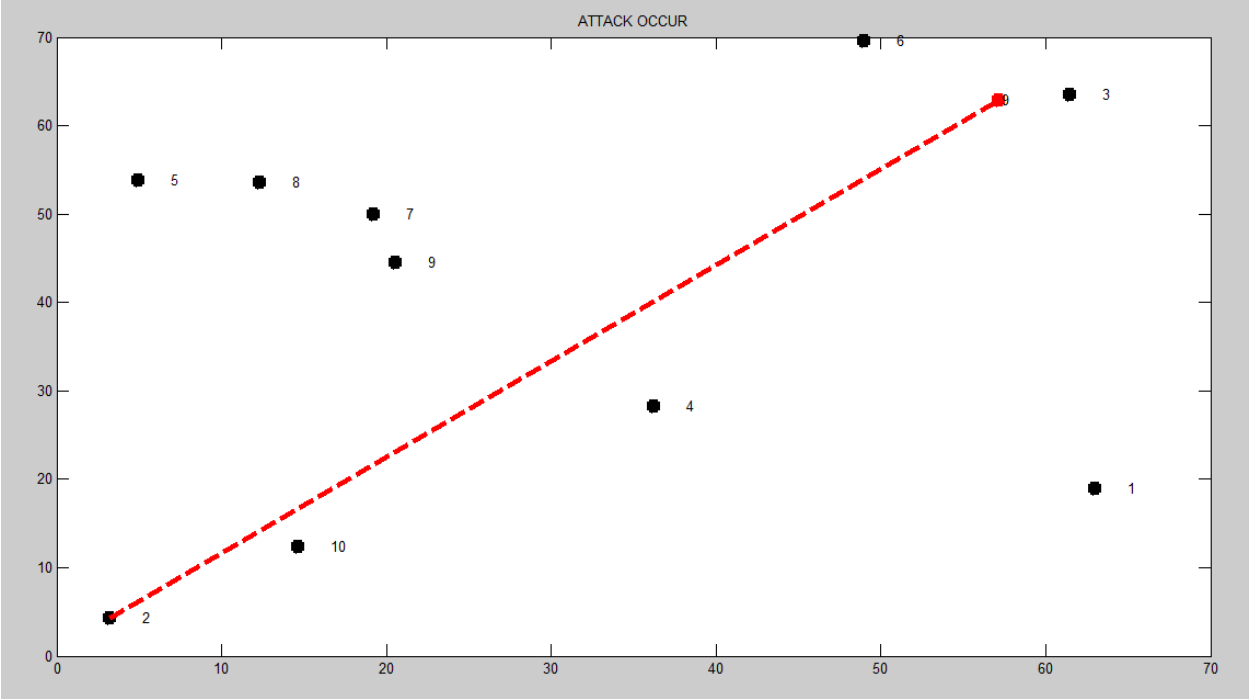

Figure 4.5: Direct Sybil Attack model.

Figure 4.5 illustrates the play of Sybil node. It is depicting that Sybil node has the replicate identity of normal node 9 which is the destination node for source node 2. Now, the node 2 will not communicate to the original node 9 but will communicate to the malicious (Sybil) node and hence the attack will take place. This is just an example to explain the Sybil Attack in the WSN.

4.6 Deployment of normal nodes, beacon nodes and Sybil nodes in the network.

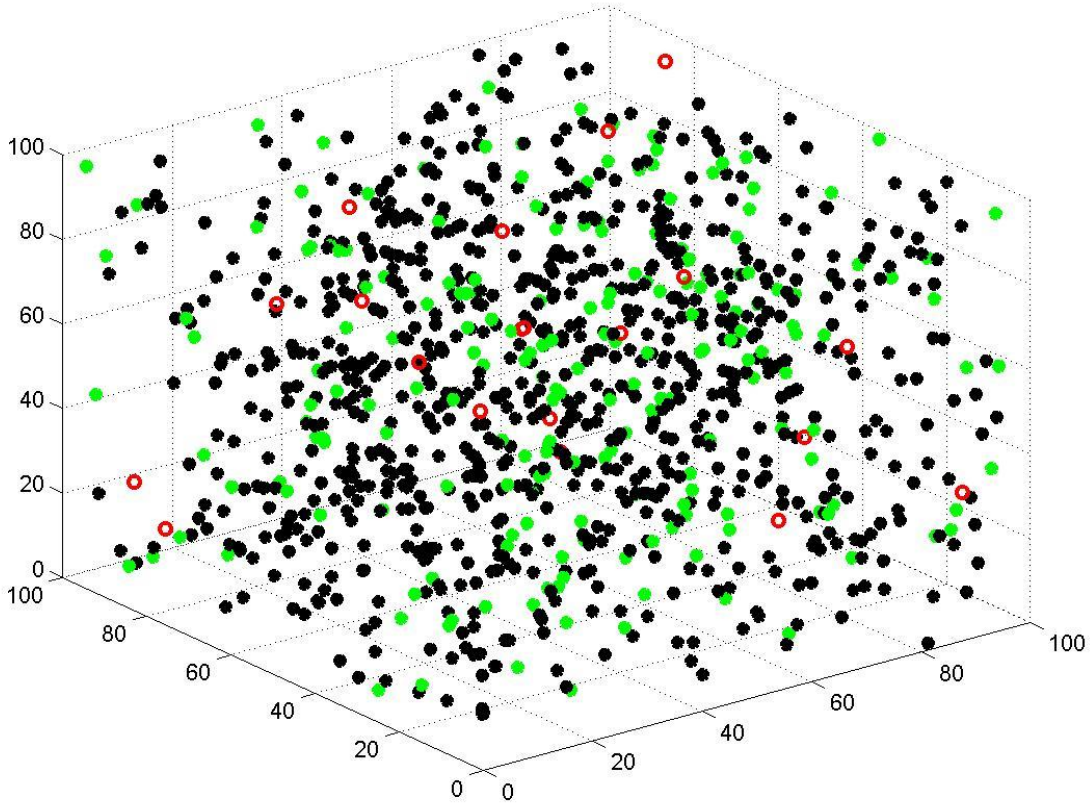

Figure 4.6: Deployment of normal, beacon and Sybil nodes in the deployment area of 100*100*100

Here the deployment of normal nodes, Beacon nodes and Sybil nodes is Normal Distribution and all nodes are deployed according to State Information method i.e in 3-D.

-Black nodes representing normal nodes.

-Green nodes representing Beacon nodes.

-Red nodes representing Sybil nodes.

4.7 Broadcasting of the Query Messages by the Beacon Nodes

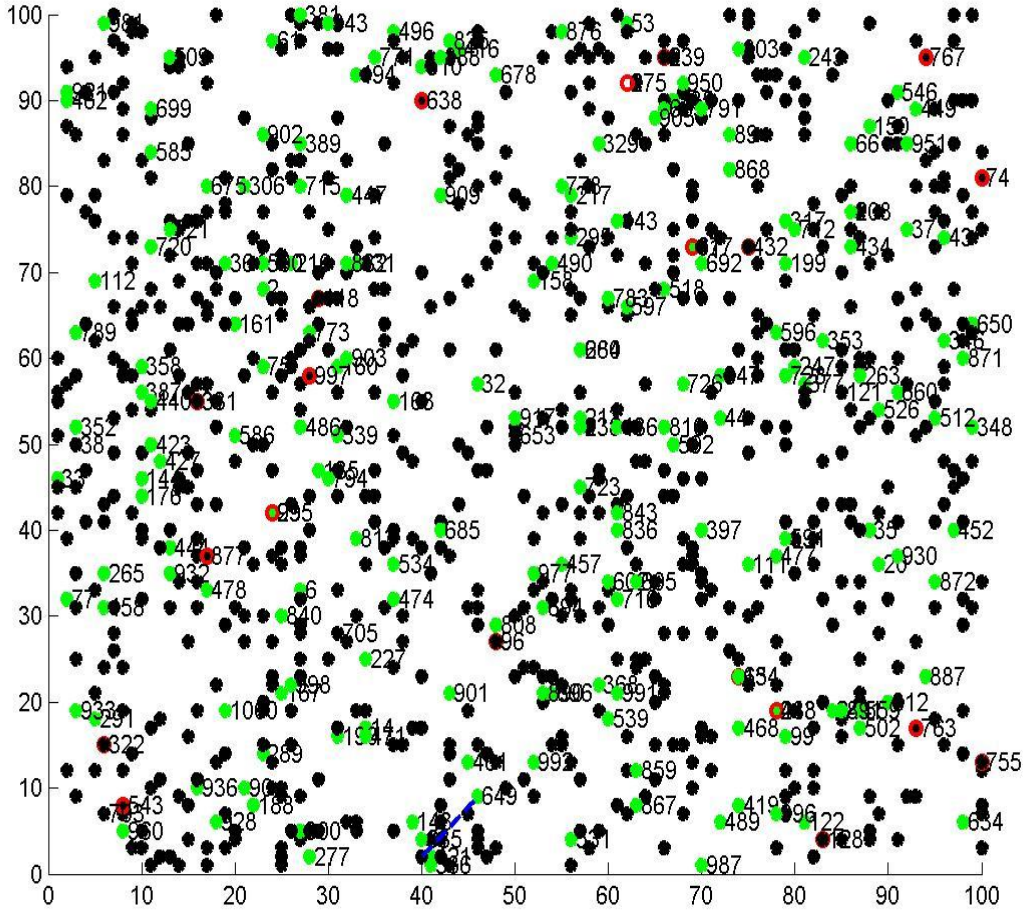

Figure 4.7: Transmission of the query packets by the beacons to their respective neighbors.

Figure 4.7 illustrates that beacon nodes (green nodes) periodically issue a query request packet. After some time, nodes receive the packet and reply to the beacon nodes. Here the range of each node for transmission of packets is 10 m.

4.8 Reply of the Query Messages by the Nodes

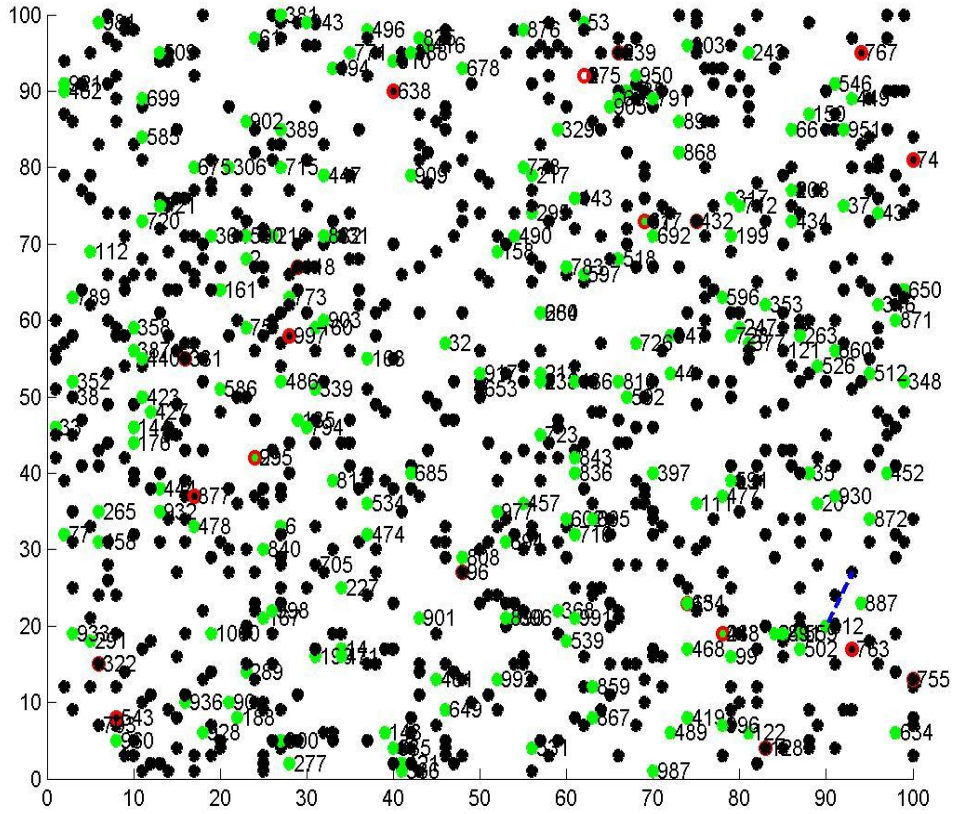

Figure 4.8: Reply of the query messages.

Figure 4.6 illustrates that normal nodes and the Sybil nodes replying to the Beacon nodes. As beacon nodes have the neighbor list of its original neighbors, so after receiving the response messages from neighbors it will detect the sybil nodes by cross checking neighbor list.

4.9 Detection of Sybil Nodes by using proposed scheme

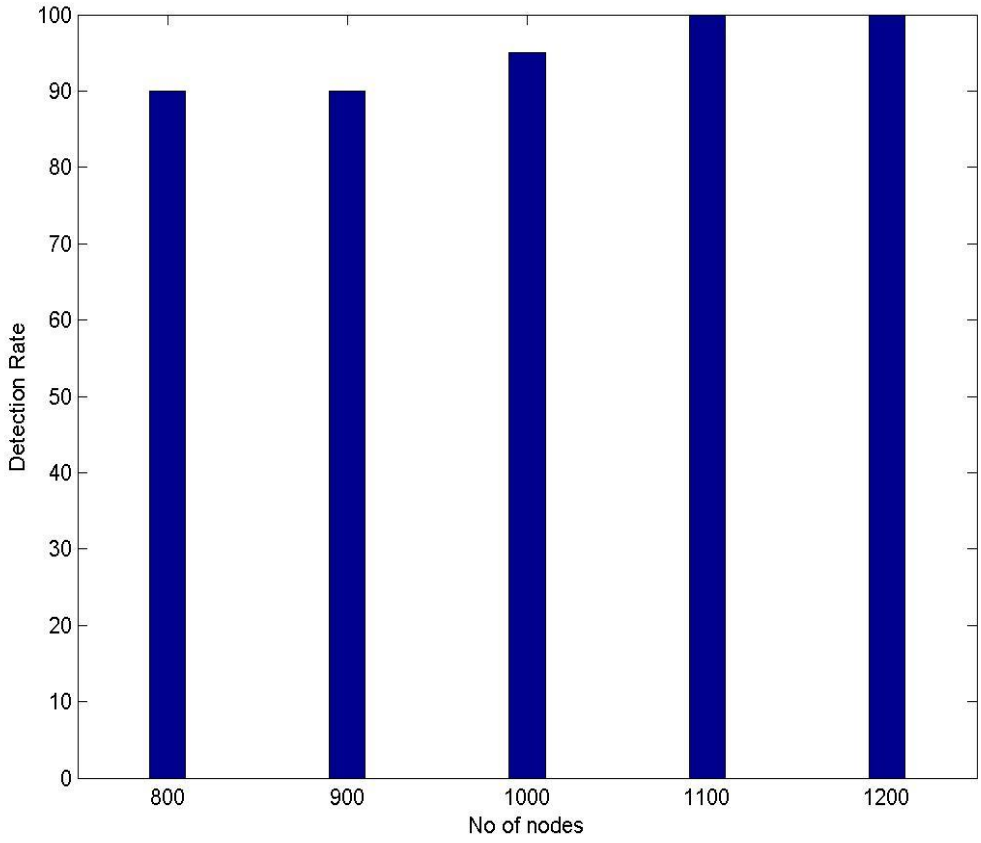

Figure 4.9: Detection rate.

Figure 4.6 illustrates the Sybil node detection rate using proposed scheme. When the number of nodes are 800 and 900, proposed scheme detecting the Sybil nodes at 90%, and as the number of nodes increases, the detection rate also increases, when number of nodes reaches upto 1000, the detection rate become 95% which is 1% more as compare to the State information detection scheme. As we increase the network density, the detection rate will be improved as shown in figure.

4.10 Comparison graph of detection rate with respect to number of nodes of our proposed scheme and State Information Scheme

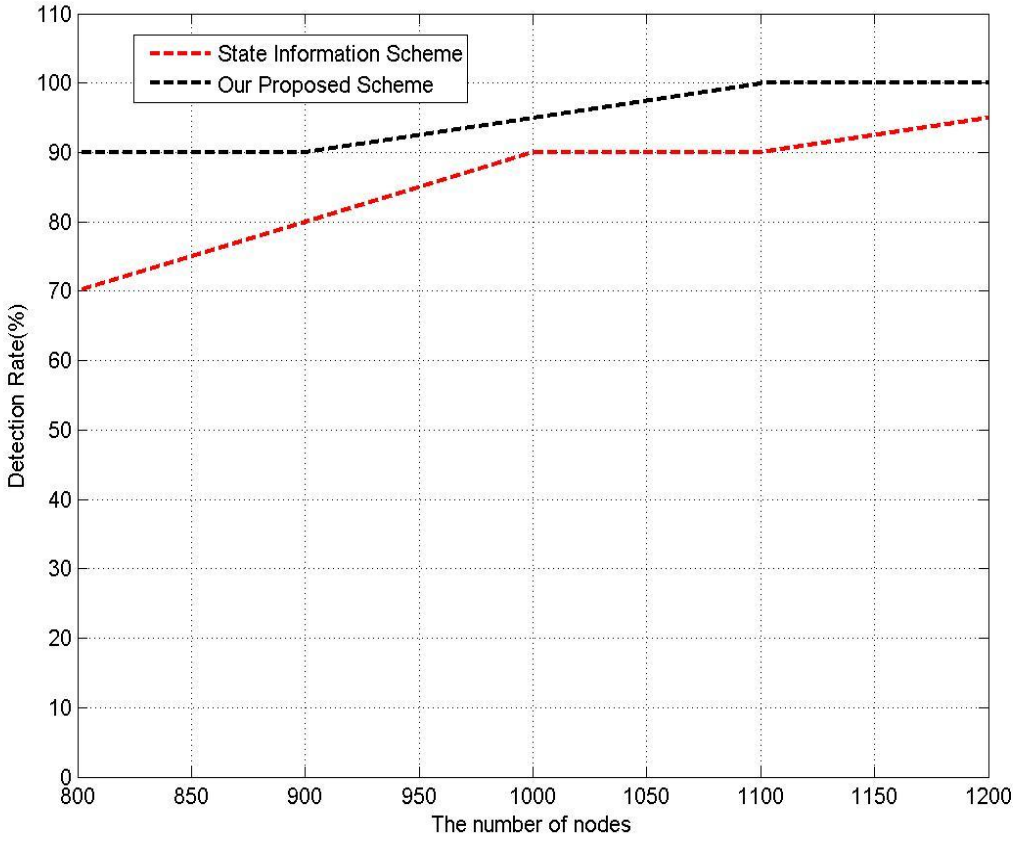

Figure 4.10: Comparison between proposed and state information scheme w.r.t. the no. of nodes.

Figure 4.10 illustrates the comparison of state information detection rate and proposed technique detection rate. At the beginning, the number of nodes is 900, and the detection rate reaches 90% while state information only reaches 80% and as the number of nodes increases, with respect to that detection rate also increase. When the network is of 1000 nodes, the detection rate of proposed scheme comes 95 % and state information detection reaches 90%.

4.11 Comparison graph of detection rate with respect to number of iterations of our proposed scheme and State Information Scheme

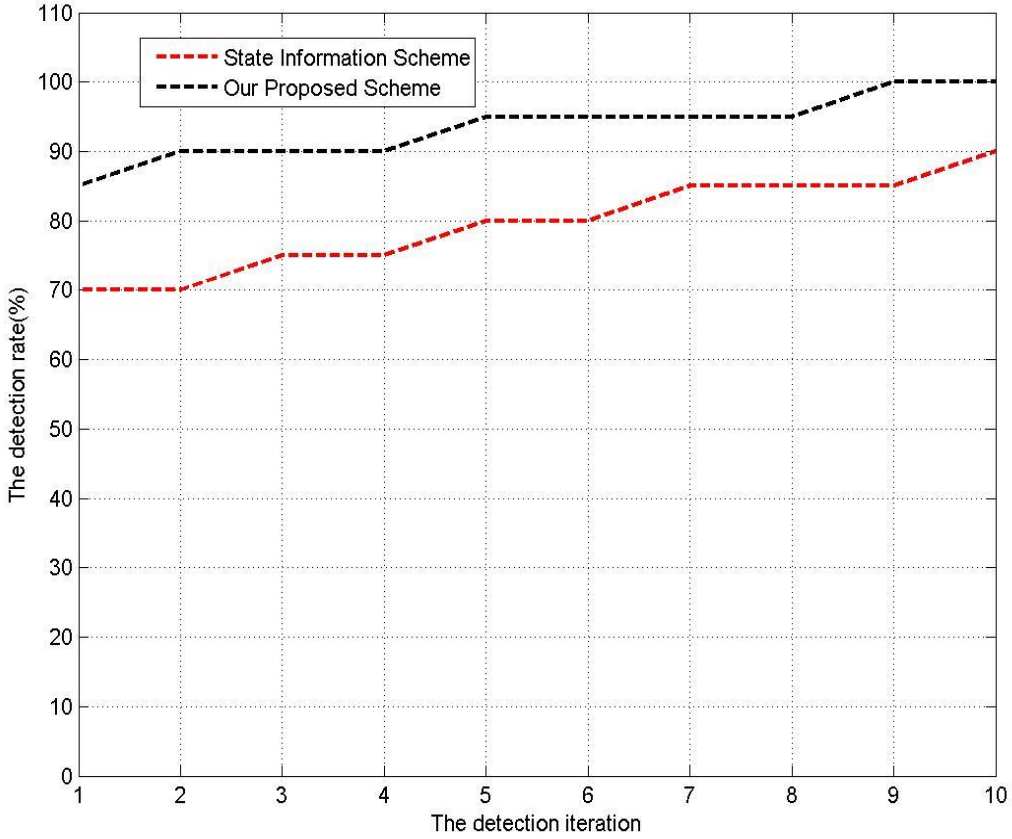

Figure 4.11: Comparison between proposed and state information scheme w.r.t. the no. of iterations.

Figure 4.11 illustrate that detection rate of both of the schemes increasing with respect to the number of detection iteration.

4.12 False Detection Rate

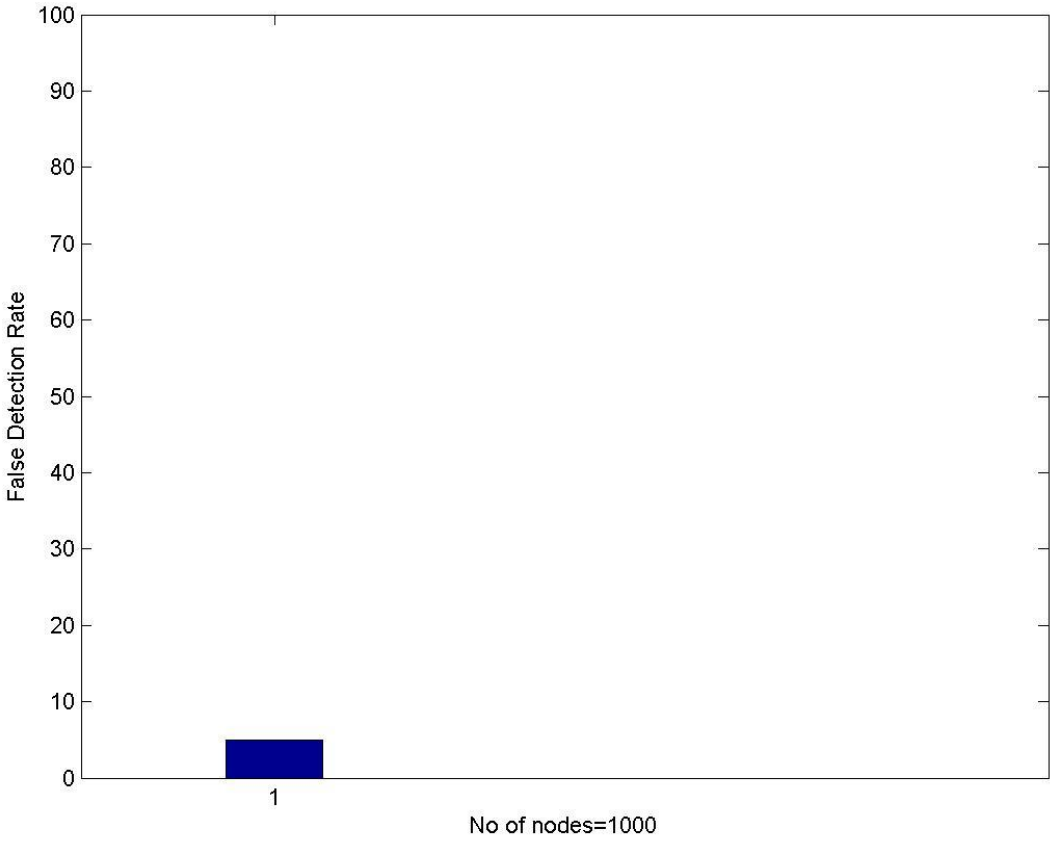

Figure 4.12: False Detection Rate with respect to 1000 nodes.

Figure 4.11 illustrate that false detection rate i.e. 5% when number of nodes is 1000. This false detection rate decreases as we increase the number of nodes mean to say with respect to increase in the density of the network this rate increases.

4.13 Comparison Table of State information and Proposed Scheme:

Table4.1: Comparison of State Information and proposed scheme.

Number of nodes	**Number of Beacons**	**Number of Sybil nodes**	**Detection Rate by State Information Scheme (%)**	**Detection rate by Proposed scheme (%)**
800	200	200	70	90
900	200	20	80	90
1000	200	20	90	95
1100	200	20	90	100
1200	200	20	95	95

Chapter 5
CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

In recent years, much more attention has been attracted in Wireless Sensor Networks recently. The problem of high security of WSNs is required to solve. It is the long standing problem to detect the replication attacks in WSNs. In report we have gone through the different schemes to detect the Sybil attack and due to high accuracy rate, State Information Detection scheme is preferred which is a superior technique as compare to other detection schemes. In our research, we divide our scheme into basic and enhancement scheme to detect Sybil attack. The simulation of Sybil Identification algorithm is done on MATLAB. The network is composed of 100 normal nodes, 20 beacon nodes, and 10 Sybil nodes. The deployment of these nodes is random in nature. Simulation results demonstrate that detection rate can be upto 95%. Based on performance result, I will continue to study about Sybil attack detection methods and will try to explore more efficient method to detect Sybil Attack.

5.2 Future Scope

In future , some extensions of our thesis proposed approach can be applied. The list contains some topics in this area:

- A similar detection scheme that can be developed and analyzed by refining some of the properties of the State Information scheme.
- Further, using the data about age of nodes play a vital role in increasing the detection rate of Sybil nodes in the network.
- By using different clustering techniques like LEACH, may be we can achieve additionally improvement in the network lifetime & energy consumption.
- In future we can chose hybrid our proposed scheme with existing detection techniques like RSSI or Random key Predistribution will improve the detection accuracy and can efficiently detect the Sybil nodes.

REFERENCES

[1]. Bo Yu, Cheng-Zhong, and Bin Xiao, "Detecting Sybil Attack in VANETs", ELSEVIER, Journal of Parallel and Distributed Computing 73((2013) 746-756.

[2]. John R. Douceur, "The Sybil Attack", Microsoft Research, 2002.

[3]. Kuo-Feng Ssu, Wei- Tong Wang , and Wen-Chung Chang, "Detecting Sybil Attacks in Wireless Sensor Networks using neighboring information", ELSEVIER, Computer Network 53(2009) 3042-3056.

[4]. Navneet and Rakesh Gill, "Sybil Attack Detection and Prevention using AODV in VANET", Internayional Journal of Computer Science & Management Studies, VOL.13, Issue 07, September 2013, ISSN: 2231-5268.

[5]. Md. Ahasan Habib, Jia Uddin, and Md. Monirul Islam, "Sybil Aspects of Enhanced Underwater Acoustic Sensor Networks", International Journal of Energy (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

[6]. Nitish Balachandran and Sugata Sanyal, " A review of techniques to mitigate Sybil Attacks", Int. J. Advanced Networking and Applications, 2012.

[7]. Manju V C, "Sybil Attack Prevention in Wireless Sensor Network", International Journal of Computer Networking, Wireless and Mobile communication (IJCNWMC) ISSN(P):2250-1562; ISSN(E):2278-9448 VOL.4, 2014.

[8]. Mingxi Li, Yan Xiong, Xuangou Wu, Xian Chun Zhou, Yuhui Sun, Shenpei Chen, and Xiaoya Zhu, "A regional Statistics Detection Scheme against Sybil Attacks in WSNs", 12th IEEE International Conference on Trust, Security and Privacy in computing and Communications, 2013.

[9]. Athichart Tangpong, George Kesidis, Hung-Yuan Hsu, and Ali Hurson, "Robust Sybil Detection for MANETs", IEEE, Proceeding of 18th International Conference on Computer Communications and Networks, 2009, ICCCN 2009.

[10]. Shahrzad Golestani Najafabadi, Hamid Reza Naji, and Al Mahoni, "Sybil attack Detection: Improving Security of WSNs for Smart Power Grid Application", 2012 Conference on Smart Electric Grids Technology (SEGT2012).

[11]. P. Raghu Vamsi and Krishna Kant, "A lightweight Sybil Attack Detection Framework for Wireless Sensor Networks", IEEE, 2014 Seventh International Conference on Contemporary Computing (IC3).

[12]. Shanshan Chen, Geng Yang, and Shengshou Chen, "A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks", IEEE International Conference on Communications and Mobile Computing, 2010.

[13]. Murat Demirbas, and Youngwhan Song, " An RSSI-based scheme for sybil attack detection in wireless sensor networks",2006.

[14]. Bin Tian, Yizhan Yao, Lei Shi, Shuai Shao, Zhaohui Liu, Changxing Xu, " A Novel Sybil Attack Detection Scheme For Wireless Sensor Network", IEEE, 2013 Proceedings of IEEE IC-BNMT2013.

[15]. Shaohe Lv, Xiaodong Wang, Xin Zhao and Xingming Zhou, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks.

[16]. Xun li, Guangjie Han, Aihua Qian, Lei Shu, and Joel Rodrigues, "Detecting Sybil Attack based on State Information in Underwater Wireless Sensor Networks", IEEE, 2013 21st International Conference on Software, Telecommunication and Computer Networks (SoftCOM).

[17]. S. Ahmed, I.U. Khan, M.b. Rasheed, M. Ilahi, R.D. Khan, S.H. Bouk, N. Javaid, "Comparative Analysis of Routing Protocols for Underwater Wireless Sensor Networks", COSMSATS Institute of IT, Islamabad, 2013.

[18]. Servapalan Govender, "A Framework for evaluating countermeasures against Sybil Attack in Wireless Sensor Network", University of Pretoria, 2010.