HITOC

(Handy tool for Identification and Tracking On Operational Canvas)

By

Umair Ali

Zain Javed

Muhammad Awais

Submitted to the Faculty of Computer Software Engineering Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment for the requirements of a

B.E Degree in Computer Software Engineering

JUNE 2012

ABSTRACT

Identification & tracking of objects, goods and people within any open or closed environment is a very important issue which has a number of applications such as access management, tracking of goods & people, toll collection & in disaster management. The same is equally important in the defense sector situations such as secure & rescue operations where identification & tracking of soldiers & equipment is imperative.

Radio- frequency identification (RFID) is a technology that uses radio waves to transfer data from an electronic tag/RFID tag attached to an object, through a reader for the purpose of identifying & tracking of the object. Now a days, RFID tags are available that can read from several meters away & beyond the line of sight of the reader. But an RFID tag & reader directly communicate with each other and one tag's data cannot be relayed by the other tag to the reader. This is a very uncial drawback of RFID technology that makes it infeasible for tracking of individuals in secure & rescue operations or tracking of troop in a combat field. Moreover, RFID tags are generally available in world –readable formats, which pose a risk to both personal location privacy and corporate/military security. Some crypto graphic solutions which attempt to achieve privacy against unauthorized reader are largely in research stage.

Another technology that is rapidly attracting both academia & industry for the purpose of identification and tracking is the Zigbee. It is a specification for a suite of high level communication protocols using small, low power, cheap digital radios based on an IEEE 802 standard for personal area networks. Zigbee is a cheap technology intended for applications which require low data rate, long battery life and secure networking.

CERTIFICATE OF CORRECTNESS AND APPROVAL

Certified that work contained in this thesis “HITOC” carried out by Muhammad Awais, Umair Ali and Zain Javed under the supervision of Asst. Prof. Dr. Awais Majeed for partial fulfillment of Degree of Bachelor of Software Engineering is correct and approved.

Approved by

____

(Dr Awais Majeed)

_____ Department

MCS

Dated: ________________

DEDICATION

In the name of Allah, the Most Merciful, The Most Beneficent.

To our teachers, without whose unflinching support and unstinting cooperation, a work of this magnitude would not have been possible

ACKNOWLEDGEMENT

We are eternally grateful to Almighty Allah for bestowing us with the strength and resolve to undertake and complete the project.

We gratefully recognize the continuous supervision and motivation provided to us by our supervisors, Assistant Professor Dr Awais Majeed and Dr Faisal Basheer for their continuous and valuable suggestions, guidance, and commitment towards provision for the undue support throughout our thesis work. We are also grateful to the other professors and instructors of the CS Dept for their guidance and support throughout the project. It is because of their help and guidance that we were able to complete the project and thesis work in time.

We would like to offer our admiration to all out class mates and seniors who have been supporting, helping and encouraging us throughout our project.

Last but not the least we are deeply obliged to our families for their never ending patience and support for our mental peace and to our parents for the strength through their prayers.

1 Chapter

Introduction to HITOC

1.1 Introduction

HITOC stands for Handy tool for Identification and Tracking on Operational Canvas. It aims at to provide a portable, light weight and handy devices by which various individuals in military and disaster relief related operations can be identified and tracked. Modern defense organizations in the world use handy devices which enable their leaders to be updated about their troop's status on ground. Moreover, such devices are commonly used by different countries during disaster relief operations. HITOC is such a system which will also be used for the same purpose for military operations but also will be useful in civil disaster relief operations. Many solutions just rely on the tracing by mobiles but it has inherent disadvantages which include cost, network availability and provision of a mobile network infrastructure.

HITOC will be used as an effective measure to support operational grip over operational activities. It will make use of ZIGBEE devices which will be worn by all the peers or the participants of the operations. Entire peer mapping and their locations will be visible at the base station. A ZIGBEE USB sink device will be connected with the laptop and in this way that can receive the data of all the peers.

Similarly various team heads locations including their peers will also be visible to the Base station. Base station will be on PC or laptop that can be connected with smart phone devices i.e. Android based mobiles on which entire zonal operational canvas will be visible. This connection can be made through GPRS or Edge based internet connections.

1.2 Background

Tracking in operational areas are done to optimize the performance of operations in an organized manner. Updated location of every individual in the area is necessary to do so. As the need of identification and tracking of the objects, goods or persons in open or closed environment is increasing therefore a lot of work for this purpose is being done to fulfill the requirements of this domain. Some examples of systems that is already exist and doing work .

1.3 Problem Addressed

The basic problem addressed in this project is to provide a cost effective solution by developing such a system that can identify & track personals in secure & rescue operations where there is no other communication is possible (i.e. GSM or WIFI). Identification means the particulars of an individual like name and rank, while tracking means the position of the individual on ground.

1.4 Goals and Objectives

This project intends to provide cost effective, less power consumption, accurate and updated positioning, real time tracking and secure and reliable communication. This system is well suited for military usage in order to track the personals in an operational area and disaster rescue missions in an effected zone.

HITOC has two main components. The first will enable wireless communication in a multi hop fashion to allow the successful sensing and network creation of ZIgbee devices. Major concern in this regard is that the network devices (Zigbee devices) are resource constrained i.e. battery powered, low computational capability and few kilobytes of memory.

The second will get the locations from GPS integrated with Zigbee devices and map them on computer screen of Base Station. In this component a user friendly GUI is desirable where user can easily see the location as well as other information of the personals present in operational area.

1.5 Deliverables

The project deliverable is an application for the identification and tracking of personals. In its entirety it should be a self configuring multi hop wireless sensor network for sensing and transmitting information detected by the GPS to a common sink. This data will serve as input for the functioning of the above mentioned application.

1.6 Summary

This chapter starts with a brief introduction and background to the HITOC project. Initial sections are followed by an explanation of the problems that the project addresses and what the HITOC project aims to achieve. It then touches upon the final product the project will deliver. In the last section document organization is elaborated.

In a nutshell the HITOC project aims at the development of an automated system for the identification and tracking of personals (In the operational area).

CHAPTER 2

2 Chapter

Literature Review & Related Work

2.1 Introduction

In this chapter some examples of systems that is already exist and doing work in the field are described. These examples include location aware mobile system, sahana disaster management system and global positioning system. After that part the literature review of zigbee technology is given, including the protocols being used in it and types of zigbee devices.

2.2 Related Work

The details of related works are given below

2.2.1 Location aware Mobile System

Use smart phone applications to track the peers location. In this system mobiles use the GPS service provided online by connecting through the internet like GPRS/Edge. These are being used to track the participants of the civil disaster management institutes.

2.2.2 SAHANA Disaster management tracking system

SAHANA is a web based portal system which aims to track missing persons and internally displaced persons after a disaster. Different organizations coordinate to help the affected people. Different type of mobile and network technologies have been used to establish the system

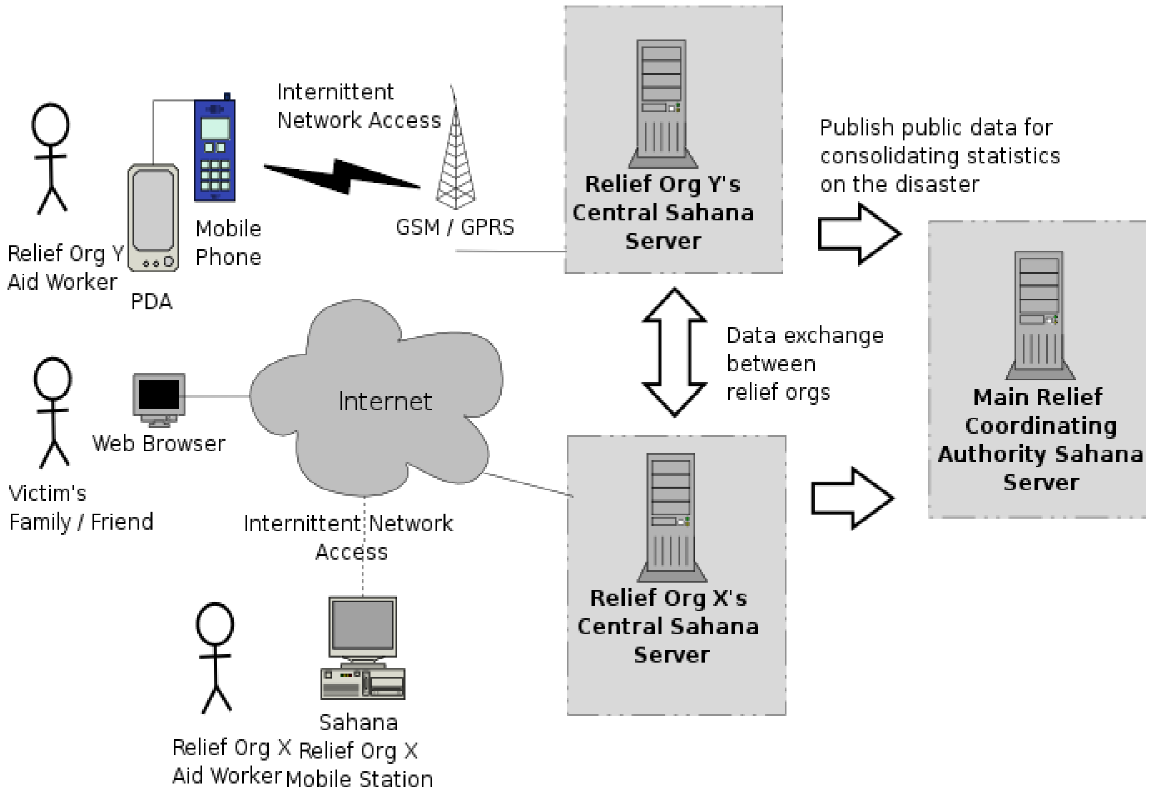

Figure 2-1 Sahana disaster management system

2.2.3 Global Positioning System

GPS service is very suitable for tracking and finding the location of objects. A GPS tracking unit is a device that uses the Global Positioning System to determine the precise location of a vehicle, person, or other asset to which it is attached and to record the position of the asset at regular intervals. The recorded location data can be stored within the tracking unit, or it may be transmitted to a central location data base, or internet-connected computer, using a cellular (GPRS or SMS), radio, or satellite modem embedded in the unit. This allows the asset's location to be displayed on a map.

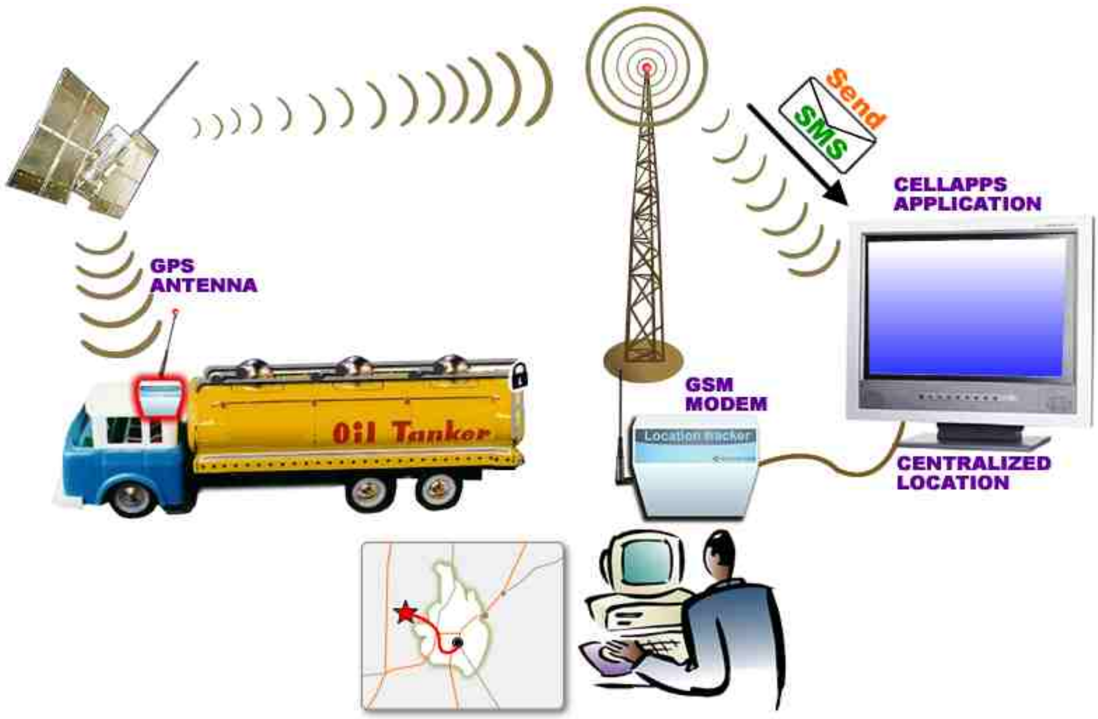

Figure 2-2 Global positioning system

2.3 Overview of Zigee technology and device

This section includes zigbee technology and hardware components description used in HITOC.

2.3.1 Introduction to ZigBee technology

ZigBee is a specification for a suite of high level communication protocols using small, low-power digital radios based on an IEEE 802.15.4 standard for personal area networks.

ZigBee is a low-cost, low-power, wireless mesh network standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications. Low power-usage allows longer life with smaller batteries. Mesh networking provides high reliability and more extensive range. ZigBee chip vendors typically sell integrated radios and microcontrollers with between 60 KB and 256 KB flash memory.

ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz in most jurisdictions worldwide. Data transmission rates vary from 20 to 900 kilobits/second.

The ZigBee network layer natively supports both star and tree typical networks, and generic mesh networks. Every network must have one coordinator device, tasked with its creation, the control of its parameters and basic maintenance. Within star networks, the coordinator must be the central node. Both trees and meshes allows the use of ZigBee routers to extend communication at the network level.

ZigBee builds upon the physical layer and medium access control defined in IEEE standard 802.15.4 (2003 version) for low-rate WPANs. The specification goes on to complete the standard by adding four main components: network layer, application layer, ZigBee device objects (ZDOs) and manufacturer-defined application objects which allow for customization and favor total integration.

Besides adding two high-level network layers to the underlying structure, the most significant improvement is the introduction of ZDOs. These are responsible for a number of tasks, which include keeping of device roles, management of requests to join a network, device discovery and security.

2.3.2 Overview Of ZigBee Devices

There are three kind of ZigBee devices used in our network which are Cluster Heads (Coordinators), End Devices and Sink.

a) Cluster Head

These are the devices which will be connected to a GPS to get current location; these devices will carry out the routing in the network. These devices will have an external antenna attached to enhance transmission range. These devices will be installed on some cars or other facility where sufficient battery arrangements are provided.

b) End Device

These devices will be given to personals, the location of these devices will be calculated by calculating the signal strength drop from the cluster head, as we have got the exact location of cluster head through its GPS, we can thus calculate end devices location by considering its signal strength drop from its respective cluster head. End devices consume low battery because they are in SLEEP mode till they get external stimulus.

c) Sink Device

This device will be attached to the PC/Laptop at the base station, all the signals of the network are directed towards the sink and they terminate here. Sink node will collect all the data and pass it to our application through a serial port.

2.4 Limitations

Existing systems for identification and tracking have some shortcomings which are follows

1. No cheap solution exist
2. Heavy and big systems difficult to carry with
3. At present our operational leaders face great difficulty in having updated operational tracking facility.
4. In disaster management lot of work has to be done in order to manage the operation. This redundancy can be reduced if we introduce some handy tracking device where operational leaders can take decisions on updated operational canvas.

2.5 Summary

As we see that already existing system in the domain of tracking and identification have different type of drawbacks so our project aims to resolve those problems.

1. Provide cheap solution as compared with existing systems to our national departments for tracking operational canvas. It is cheap solution in the sense that it will only consume the battery required to operate the devices. And it is using the GPS transceiver for getting its location. It will use personal network established by Zigbee devices for relaying the location of different objects to the base station.
2. It will provide the map on which the location of the objects will be shown. So one can easily see the complete picture of the operational situation and can take decision accordingly.
3. Allow higher level officers in military operations to take decisions on the updated situation of their soldiers.
4. Assist all disaster management team to effectively manage and control their workers
5. Simple, handy and cost effective tool. And one can easily move by carrying it.

CHAPTER 3

3 Chapter

Requirement Specification

3.1 Introduction

Identification & tracking of objects, goods and people within any open or closed environment is a very important issue which has a number of applications such as access management, tracking of goods & people, toll collection & in disaster management. The same is equally important in the defense sector situations such as secure & rescue operations where identification & tracking of soldiers & equipment is imperative.

Radio- frequency identification (RFID) is a technology that uses radio waves to transfer data from an electronic tag/RFID tag attached to an object, through a reader for the purpose of identifying & tracking of the object. Now a days, RFID tags are available that can read from several meters away & beyond the line of sight of the reader. But an RFID tag & reader directly communicate with each other and one tag's data cannot be relayed by the other tag to the reader. This is a very uncial drawback of RFID technology that makes it infeasible for tracking of individuals in secure & rescue operations or tracking of troop in a combat field. Moreover, RFID tags are generally available in world –readable formats, which pose a risk to both personal location privacy and corporate/military security. Some crypto graphic solutions which attempt to achieve privacy against unauthorized reader are largely in research stage.

Another technology that is rapidly attracting both academia & industry for the purpose of identification and tracking is the Zigbee. It is a specification for a suite of high level communication protocols using small, low power, cheap digital radios based on an IEEE 802 standard for personal area networks. Zigbee is a cheap technology intended for applications which require low data rate, long battery life and secure networking.

3.2 Project Scope

The HITOC is a self configuring multi hop wireless sensor network that will use GPS to get the locations. There will only be a single sink i.e. the final destination no matter what route is followed will be the sink node. It is aimed for such open operational areas where there is no other way to track the personals. The software application will allow the monitoring and setting application parameters.

3.3 Overall Description

The overall descriptions of the system including the product features, perspective and network perspective are elaborated in this section.

3.3.1 Product Features

The final product is intended to have a number of features. These features are provided using different modules in a way to achieve the overall functionality. The basic product features are elaborated in the remaining of this section.

3.3.1.1 Multi Hop Routing Protocol

The HITOC must allow all active devices (end nodes) to communicate with each other in a multi hop fashion i.e. each node should forward data packets to the next node and this process should continue until the packet reaches the sink node. This is a major requirement of the system as the current routing protocol implemented one the sensor motes does not support multi hop routing.

This requires the selection and implementation of a multi hop routing protocol that can be implemented on the resource constrained ETRX3 zigbee devices. Multi hop routing will enable these devices to establish a mesh topology and will increase the range of observed phenomena.

3.3.1.2 Data Transmission

Data displayed i.e. location of the personal is fresh, HITOC get the location of device carriers after a 30 sec interval. This interval can be reduced programmatically up to 5 sec.

3.3.1.3 HITOC Application

HITOC application has the functionality of zooming in and out on operational canvas and to show every individual’s position as well as their other information.

3.3.2 HITOC Perspective

In present deteriorating law and order situation and inflicted terrorism activities has compelled Armed forces along with law and order keeping organizations like police, Rangers, Military to operate in urban areas tribal belts. Now these areas are not purely open battle fields and are cluttered with buildup areas communication infrastructure, markets and civil population .

3.3.3 Network Perspective

The HITOC uses ETRX3 Zigbee devices which form the network infrastructure. Every mote communicates its sensed data to the closest mote based on the gradient protocol using the wireless medium.

The farthest node sends the data to the closest node in the network and the transfer of the data continues until the data is reached to the sink node. Figure 3.1 shows how nodes communicate with each other in the network.

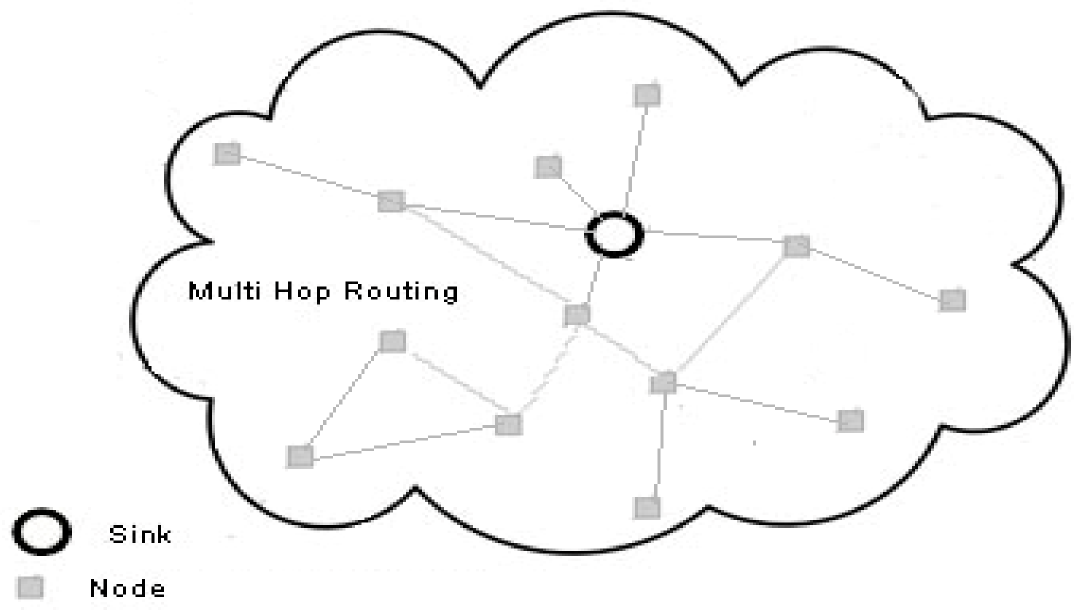

Figure 3-1 Multihop Routing

3.3.4 System Features and Functional Requirements

3.3.5 System Feature 1: Peer Client

3.3.5.1 Description:

Peer client is the end user wearing the independent **zigbee device** while at operation. This is the peer which make a component of the cluster; leading to operational canvas. This peer device has no GUI or functionality display.

3.3.5.2 Priority:

Priority of peer zigbee device is high since it is the basic block of operational canvas.

3.3.5.3 Priority Component Rating:

Benefits:

1. Peer device allow the cluster head and zigbee device to connect with each other hop to hop.

2- This device connects to cluster head providing location of his device.

3.3.5.4 Sequence of Action:

1- Peer device will keep listening for cluster head device at specific sensor frequency.
2- On receipt of message from cluster head peer device will ascertain its own location.
3- Then peer device will return to cluster head giving his location.

3.3.5.5 Functional Requirements:

FR1- HITOC peer must receive and listen to cluster head broadcast message.

FR2- Then HITOC client has to calculate and determine its relative position from the location of cluster head.

FR3- Peer device will calculate its location in accordance with location information received from cluster heads. The more cluster heads in reach of peer, the more is the accuracy of the peers location. The distance from a cluster head is calculated by comparing the strength of signal received with the ideal signal strength. Practically if we have the distances known from three cluster heads, we can calculate the exact location of the peer.

FR4- Each peer message will report back location and ID (Personal ID).

Message Format-(ID, Location Coordinates).

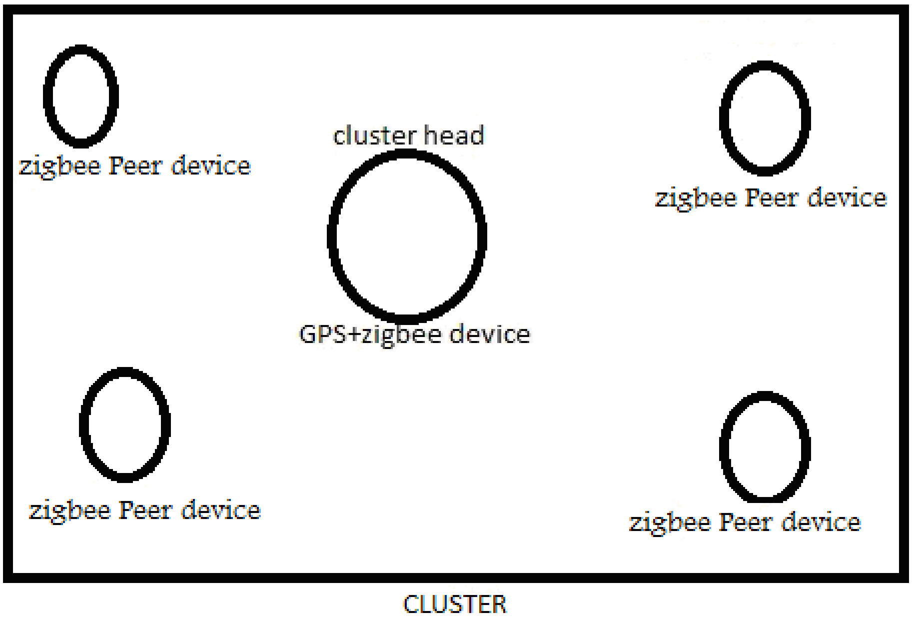

Figure 3-2 Zigbee clusterhead/peer device

3.3.6 System Feature 2: Cluster Head

3.3.7 Description:

This system feature is independent zigbee device with antenna, higher transmission range and GPS module. This device will act as cluster head. This device will be responsible to keep updated operational canvas. Then these cluster head device will map a network connecting them hop to hop searching to **base station.** Cluster head will have additional battery arrangements as well to operate high consumption GPS module.

3.3.7.1 Priority:

Priority of cluster head zigbee device is ‘High’. Since this device has networking responsibility up to base station. Along with this cluster head is responsible for the cluster determination.

3.3.7.2 Priority Component Rating:

Benefits:

1- This will enable determination of cluster operational canvas.

2- This will enable networking up to the **base station.**

3- -This will enable enhanced range due to antenna.

4- This will enable root level GPS positioning.

3.3.7.3 Sequence of Action:

1- Cluster head will determine his own location using GPS.
2- It will then broadcast location message to all pears with his own location.
3- It will be receiving location i.e., relative locations of all peers and then route it towards the **base station.**
4- Cluster head will broadcast the following information regarding peers
   ID, Location
5- Cluster head will transmit its own location and ID as well towards **base station.**

3.3.7.4 Functional Requirements:

FR1- Cluster head will keep broadcasting its location to its peers on regular intervals.

FR2- Receive the reply messages of peers which would contain ID and Location.

FR3- Receive messages from other cluster heads for the purpose of multi hop routing.

FR4- Forwarding the messages received from peers in its clusters and other cluster heads.

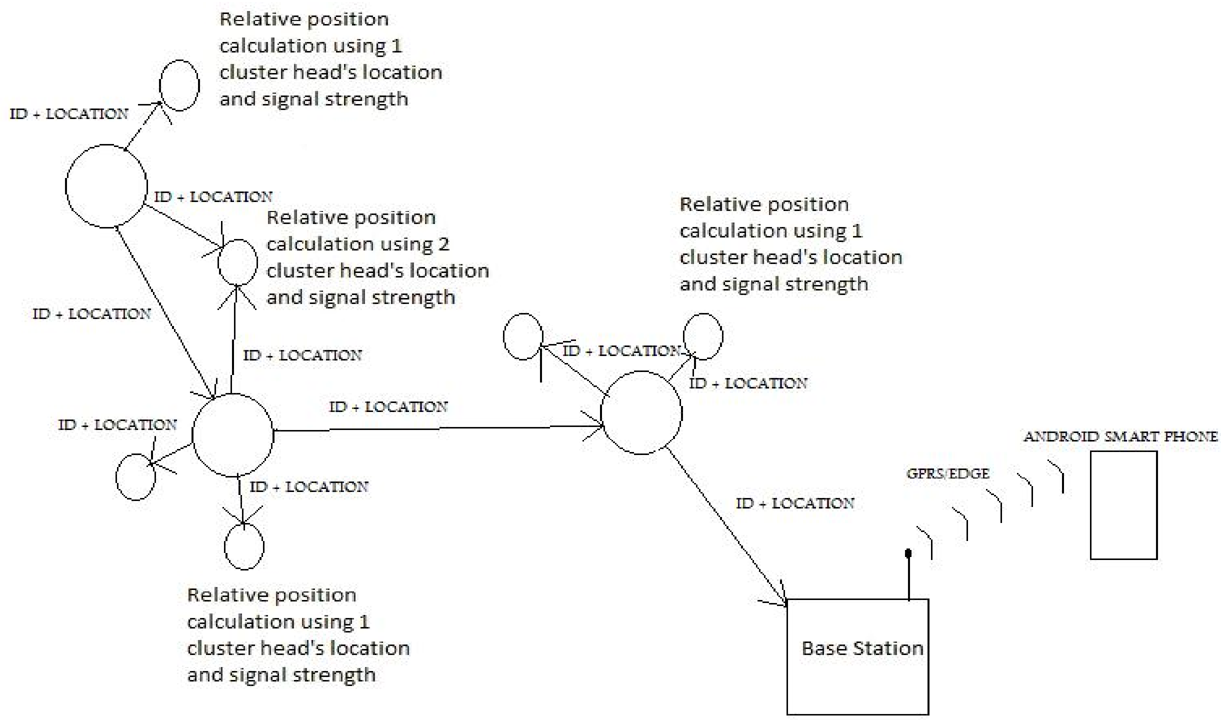

Figure 3-3 Working of HITOC

3.3.8 System Feature 3: Base Station:

3.4.3.1 Description:

This is the first locality where operational canvas can be physically seen on computer. This base station is connected to laptop with **SINK ZIGBEE DEVICE** via USB port. This connected zigbee device is accessing the locations received from cluster head peers.

3.4.3.2 Priority:

The priority of this component is ‘high’ since it holds the first GUI visibility of operational canvas.

3.4.3.4 Priority Component Rating:

Benefits:

a. This enables connectivity with cluster heads which is networked till base station via SINK ZIGBEE DEVICE.

b. This allows mapping of operational canvas on the laptop device as well as smart phone connected via GPRS/EDGE.

c. It allows mapping of ID of zigbee device holder to the individuals data that include UNIT, DUTY and Personal ID.

d. This allows connectivity to smart phone i.e., Android via GPRS and allowing operational canvas to the mobile elements to offices etc.

3.4.3.5 Sequence of Actions:

a. Base station terminal i.e., laptop allows connectivity through USB port with SINK ZIGBEE DEVICE.

b. Through this terminal base station is connected to cluster heads network.

c. Base station will receive the message of location and will resolve their ID’s to the individual UNIT, DUTY and Personal ID.

d. Base station will then plot the location of all peers onto the map along with their ID’s and other information.

e. Base station will allow smart phone connectivity via GPRS. On getting connected will disseminate them on the operational canvas.

3.4.3.6 Functional Requirement:

FR1- Base station will connect to cluster head peer via USB connected SINK ZIGBEE DEVICE.

FR2- base station will access Database and resolve ID's to UNIT, DUTY and Personal ID.

FR3- The map will display the locations on the operational canvas.

FR5- Base station will transfer operational canvas to smart phone only after getting authenticated.

3.4.3.7 Tools:

We will be using GOOGLE MAPS API to plot the operational canvas, location of zigbee devices will be shown as 'DOT' on the map.

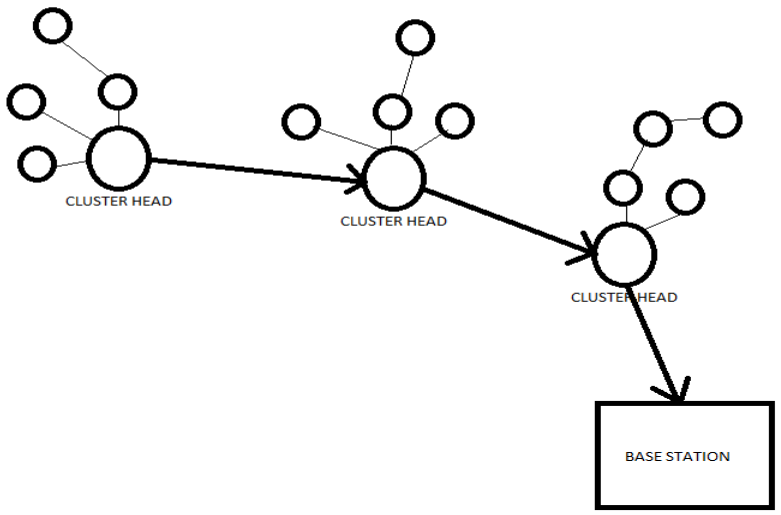

Fig3-4 Multihop Routing towards Base Station

3.4 Assumption and Dependencies

In the process of development of HITOC few assumptions have been made. In this section these assumptions have been explained.

3.4.1 Basic Assumptions

This project has following assumptions and dependencies.

a. Zigbee devices which are being used to establish network will be in the specific range from each other. End nodes should not be more than “100 meters” apart from the cluster head device and similarly one cluster head should not be away more than “500 meters” from other cluster head device. If a device is outside the range of the network it would not be the part of the system.

b. As cluster head devices will be configured with “external antennas” to enhance their network range and “GPS receivers” to get their locations, so they need more battery consumption. So it has been assumed that they will have sufficient battery power to fulfill their need.

c. We have only ONE GPS receiver, so this causes error in location calculation of end devices because to calculate exact location we need at least THREE GPS receivers.

3.4.2 Operating Conditions

HITOC is designed for outdoor usage. So it is assumed that there is no walls or other such hurdles between the personals which can reduce the signal strength of ZIGBEE devices.

3.5 Nonfunctional Requirements:

3.5.1 Availability

The *HITOC* will be optimized to give it’s maximum functionality however in case of hardware failure the failed device will simply be skipped out of the hop and other devices which were routing through it will have to find another routing path in their range. If there is no other routing device then that portion of network will be cut off from the network hence there will be no data of them on server until unless it becomes the part of network again.

The end devices are small etrx3 zigbee chips that which use an onboard power source. The availability of their function totally depends upon how long they have been given power.

To maximize the battery timing, non routing zigbee devices will go in a less power consumption mode (deep sleep) where they will be requiring only 1 µA current.

To show the position of troops on an android device which is far away from the operational area (OA), base station transmits the location points by means of internet. Hence this operational factor depends upon the connectivity with internet.

3.5.2 Performance

As this project is to be deployed in the real life so it will have the high processing of data. The mapping of GPS co-ordinates on Google maps will be done by using effective coding style to minimize the errors.

3.5.3 Environmental

The system should be able to do it’s task in low temperature as well as high temperature areas (-25’ C to 85’C). It should have tolerance to resist the probable damage caused by high moisture/vapor density areas also it should be able to resist the shock pressure caused in OA.

3.5.4 Extensibility

The system can be extended to perform other duties like sending the pulse rate or body temperature of the personals in OA to the base center. Furthermore it can also perform the duty of sending beep messages to personals in OA from base center.

3.5.5 Security

User authentication will be done by using login system. Only administrator can have full privileges on the system, he can add or remove the authentic personal's login from main databases.

Each and every zigbee device will be associated to a personal in the operational area. Name/id of personals will be written against the issued device ID.

Real time data showing on android device on the internet will also be done after user confirmation i.e. login and password.

3.5.6 Scalability

The nature of the system is such that it can be scaled to large no of clients or objects wearing Zigbee devices.

3.5.7 Other Requirements

The HITOC is developed with available devices. Also the cost of modification required within devices (like PIR sensor) should be low. It should be well documented, understandable, fault free at the time of delivery. It must allow the interfacing of additional sensors if required in the future.

3.6 Summary

In this chapter the requirements of the HITOC project are described. These requirements include the application, functional and non functional requirements and also the important features of the system. These requirements will serve as a basis for checking back if we have completed all that was decided at the start and also for testing purposes.

4 Chapter

Software Design

4.1 Introduction

The design and architecture of the system which is to be developed is very important because whole system qualities are based upon the design. The good Software design includes all requirements given by the user or client and managed considering all non functional requirements. Hence it is very important to have a good design for the development of the system. The design and architecture specification of the HITOC are explained in this chapter.

4.2 System Architecture

The architecture of the HITOC is given in this section along with description of hardware components procured.

4.2.1 Overview Of ZigBee Devices

There are three kind of ZigBee devices used in our network which are Cluster Heads (Coordinators), End Devices and Sink.

d) Cluster Head

These are the devices which will be connected to a GPS to get current location; these devices will carry out the routing in the network. These devices will have an external antenna attached to enhance transmission range. These devices will be installed on some cars or other facility where sufficient battery arrangements are provided.

e) End Device

These devices will be given to personals, the location of these devices will be calculated by calculating the signal strength drop from the cluster head, as we have got the exact location of cluster head through its GPS, we can thus calculate end devices location by considering its signal strength drop from its respective cluster head. End devices consume low battery because they are in SLEEP mode till they get external stimulus.

f) Sink Device

This device will be attached to the PC/Laptop at the base station, all the signals of the network are directed towards the sink and they terminate here. Sink node will collect all the data and pass it to our application through a serial port.

4.2.2 Diagrammatical Representation

The diagrammatical representation of the system is given in fig# 4-1

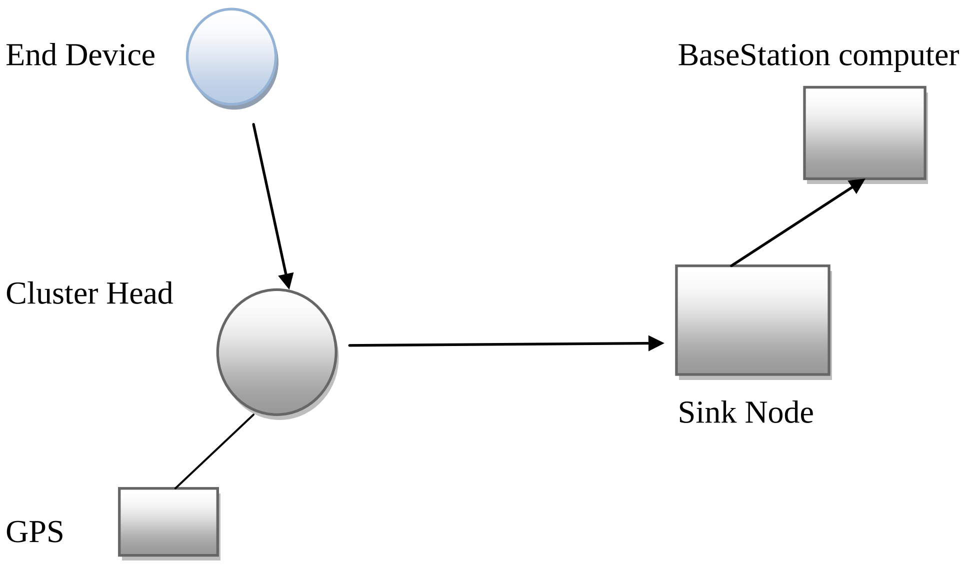

Fig # 4-1 Diagrammatic representation of HITOC hardware

4.3 Component Diagram

The Component Diagram helps to model the physical aspect of an Object-Oriented software system. It illustrates the architectures of the software components and the dependencies between them.

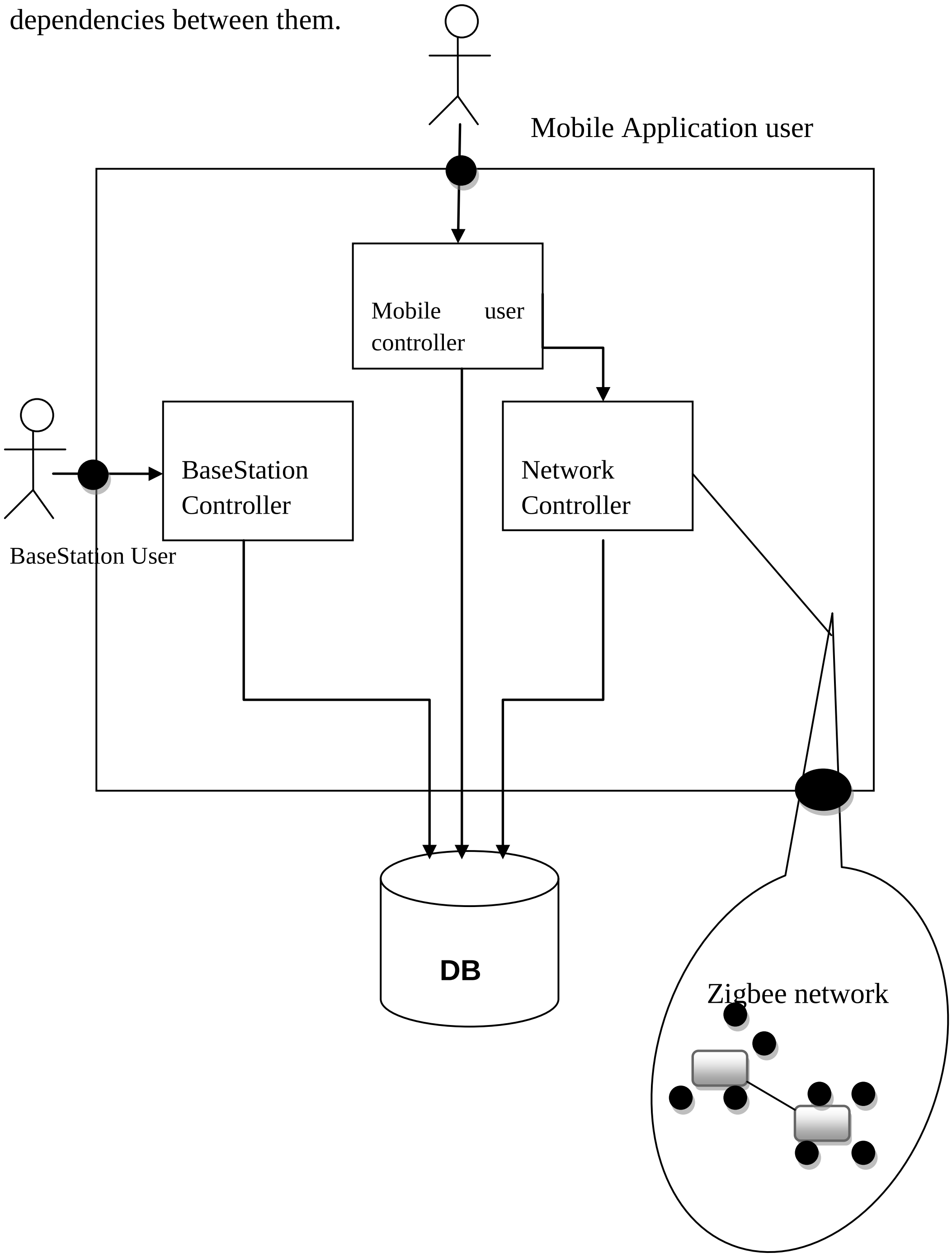

Figure 4-2 Component Diagram

4.4 HITOC Architecture Pattern

N-Layer Architectural pattern has been used to make architecture of HITOC which is shown in figure 3.

4.4.1 Why N-Layer Architecture Pattern

HITOC is a distributed system which is dealing with Base Station Operator, Remote Android Mobile application user and Zigbee Network at a same time. Due to this distributed nature of the HITOC, “N-Layer” architectural pattern has been suggested for architecture of HITOC.

4.4.2 Architecture Diagram

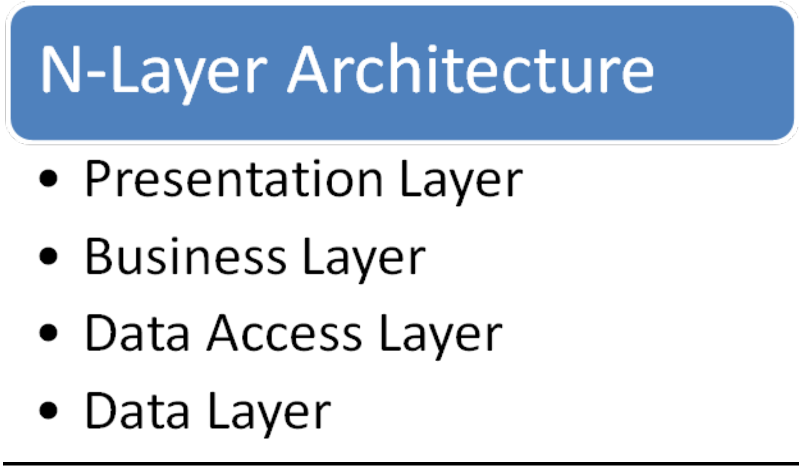

Figure 4-3 Architecture Diagram

4.4.3 Alternative Available Architecture

If we just consider that a base station is getting information of the participants of secure and rescue operation from Zigbee network and displaying them on Operational Canvas at Base Station then “Pipes and Filters” architectural pattern could be helpful to fulfill system requirements. In this way we could make different processes for

Zigbee network and Base Station, where data from Zigbee Network Process will be given to Base Station Process sequentially to parse it and display it on the Operational Canvas.

But now there is a 3rd dimension of the project which is Android Mobile application User, which can login to the system and can view the Operational Canvas. And besides this, Base Station Operator has functionality to perform on the Base Station simultaneously. Therefore "Pipes and Filters" architectural pattern is not suitable for the HITOC system due to its concurrent execution of different tasks.

4.4.4 Elaborated Architectural Diagram

This diagram shows modules of different layers of the architecture, their relationship and dependencies.

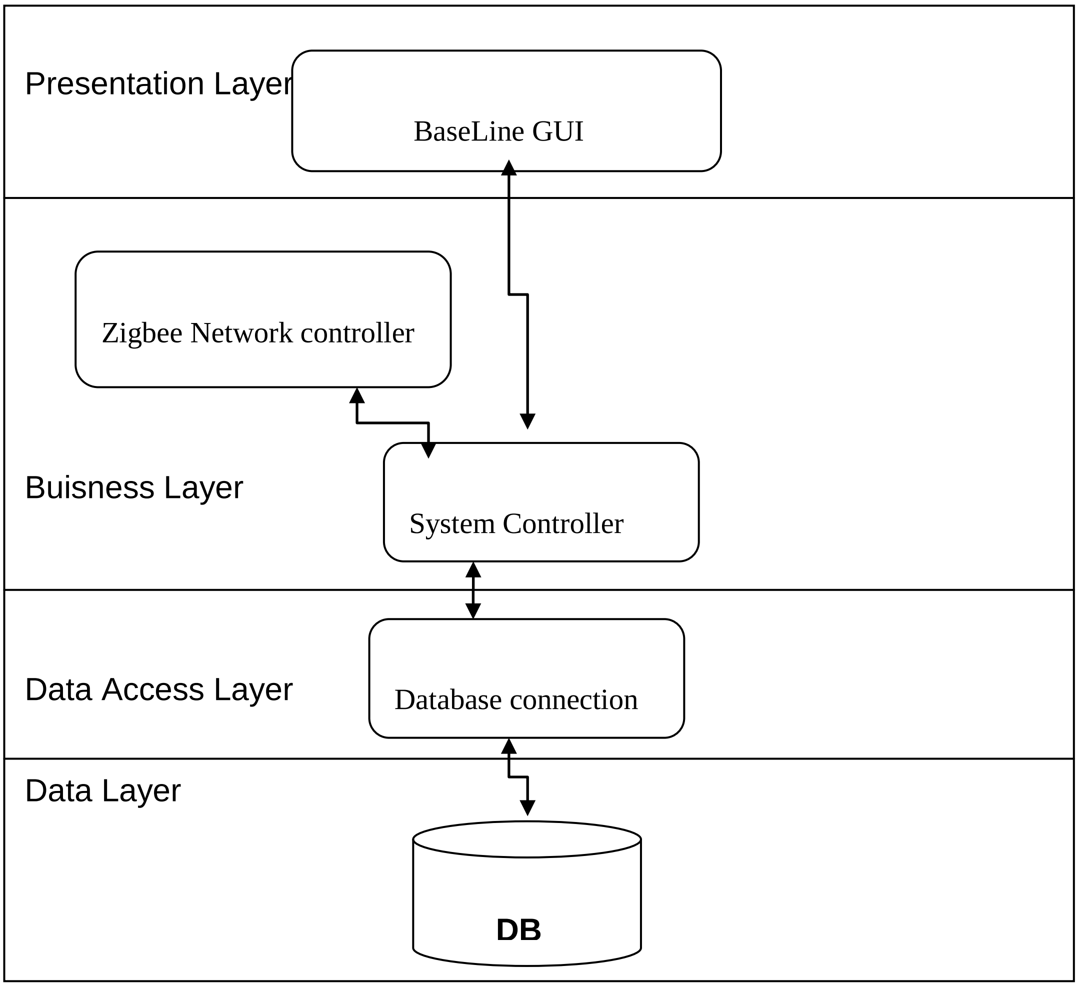

Figure 4-4 Architecture Diagram

4.4.5 Architecture Layer Description

This section includes description of different layers of architecture layers.

4.4.5.1.1 Presentation Layer

Presentation layer modules are discussed below

4.4.5.1.2 Base Station GUI

Base Station GUI provides a user interface for the base station operator to perform his tasks. Base Station GUI lies in presentation layer of architecture. Base Station GUI provides three main types of interfaces.

a) Login

Base Station GUI provides the authentication interface to the operator so that he can authenticate himself as a valid user.

b) Operational Canvas View

Base Station GUI provides the view of operational canvas.

c) Register/Delete/Edit ZigBee Devices

Base Station GUI provides interface to register, delete or edit the information regarding a device given to a personal.

4.4.5.2 Business Layer

Buisness layer modules are discussed below

4.4.5.2.1 ZigBee Network Controller

ZigBee network controller will control all the interaction with ZigBee devices on the network. The main functions include

a) **Network Interaction**

All the interaction with ZigBee devices in getting device locations is handled here.

b) Parsing

Parsing of strings received from ZigBee devices and presenting them in a meaning full form to rest of the system. This includes extracting EUI64, NODE ID and GPS provided location from the received string.

4.4.5.2.2 System Controller

Account Controller will handle all the requests from the upper modules and pass the below for retrieval or storage. This module acts as the backbone of system because all the interaction between Data and their respective utilizing modules is conducted.

The main operations of Account Controller are

a) Authentication

Base Station Operators and mobile user will use this functionality of Account Controller to get them authenticated with the system.

b) Add/Delete/Edit ZigBee Devices

ZigBee device particulars are added/deleted and edited in database using this module.

4.4.5.3 Data Access Layer

The connection with database is contained here. Using this module all the data is stored and retrieved from database. Microsoft LINQ library will be used to make connection with database.

4.4.5.4 Data Layer

Database implemented in Microsoft SQL Server 2008. ERD is given in design section

4.5 System Design

HITOC design specification and description of routing protocol used is given in this section.

4.5.1 Routing Protocol Overview

ZigBee devices use AD-hoc On-demand Distance Vector (AODV) routing protocol. In order to find the destination device, it broadcasts out a route request to all of its neighbors. The neighbors then broadcast the request to their neighbors, until the destination is reached. Once the destination is reached, it sends its route reply via unicast transmission following the lowest cost path back to the source. Once the source receives the reply, it will update its routing table for the destination address with the next hop in the path and the path cost

4.5.1.1 AODV Specifications

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.

4.5.1.2 AODV Overview

Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. These message types are received via UDP, and normal IP header processing applies. So, for instance, the requesting node is expected to use its IP address as the Originator IP address for the messages. For broadcast messages, the IP limited broadcast address (255.255.255.255) is used. This means that such messages are not blindly forwarded. However, AODV operation does require certain messages (e.g., RREQ) to be disseminated widely, perhaps throughout the ad hoc network. The range of dissemination of such RREQs is indicated by the TTL in the IP header. Fragmentation is typically not required. As long as the endpoints of a communication connection have valid routes to each other, AODV does not play any role. When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. A route can be determined when the RREQ reaches either the destination itself, or an intermediate node with a 'fresh enough' route to the destination. A 'fresh enough' route is a valid route entry for the destination whose associated sequence number is at least as great as that contained in the RREQ. The route is made available by unicasting a RREP back to the origination of the RREQ.

1. Destination IP Address
2. Destination Sequence Number
3. Valid Destination Sequence Number flag
4. Other state and routing flags (e.g., valid, invalid, repairable,Being repaired)
5. Network Interface
6. Hop Count (number of hops needed to reach destination)
7. Next Hop
8. List of Precursors
9. Lifetime (expiration or deletion time of the route)

4.5.1.3 AODV Messages

Message format used by AODV protocol are given on next page

Route Request (RREQ) Message Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|D|U|   Reserved          |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Originator Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format of the Route Request message is illustrated above, and contains the following fields:

Table 4-1 Abberivations in message format

Type	1
J	Join flag; reserved for multicast.

R	Repair flag; reserved for multicast.
G	Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to
D	Destination only flag; indicates only the
U	Unknown sequence number; indicates the destination sequence number is unknown.
Reserved	Sent as 0; ignored on reception.
Hop Count	The number of hops from the Originator IP Address to the node handling the request.
RREQ ID	A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address.
Destination IP Address	The IP address of the destination for which a route is desired.
Destination Sequence Number	The latest sequence number received in the past by the originator for any route towards the destination.
Originator IP Address	The IP address of the node which originated the Route Request.

Originator Sequence Number	The current sequence number to be used in the route entry pointing towards the originator of the route request.

Route Reply (RREP) Message Format

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |R|A|    Reserved     |Prefix Sz|   Hop Count   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     Destination IP address                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                  Destination Sequence Number                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    Originator IP address                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           Lifetime                            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format of the Route Reply message is illustrated above, and contains the following fields:

Table 4-2 Abberivations in message format

Type	2
R	Repair flag; used for multicast.
A	Acknowledgment required.
Reserved	Sent as 0; ignored on reception.
Prefix Size	If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination.
Hop Count	The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP.
Destination IP Address	The IP address of the destination for which a route is supplied.
Destination Sequence Number	The destination sequence number associated to the route.

Originator IP Address	The IP address of the node which originated the RREQ for which the route is supplied.
Lifetime	The time in milliseconds for which nodes receiving the RREP consider the route to be valid.

Route Error (RERR) Message Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |N|          Reserved           |   DestCount   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Unreachable Destination IP Address (1)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Unreachable Destination Sequence Number (1)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|  Additional Unreachable Destination IP Addresses (if needed)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Additional Unreachable Destination Sequence Numbers (if needed)|
```

+-+

The format of the Route Error message is illustrated above, and

Contains the following fields:

Type	3
N	No delete flag; set when a node has performed a local repair of a link, and upstream nodes should not delete the route.
Reserved	Sent as 0; ignored on reception.
DestCount	The number of unreachable destinations included in the message; MUST be at least 1.
Unreachable Destination IP Address	The IP address of the destination that has become unreachable due to a link break.
Unreachable Destination Sequence Number	The sequence number in the route table entry for the destination listed in the previous Unreachable Destination IP Address field..

The RERR message is sent whenever a link break causes one or more destinations to become unreachable from some of the node's neighbors.

Route Reply Acknowledgment (RREP-ACK) Message Formats

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type   4

Reserved   Sent as 0; ignored on reception.

4.5.1.4 AODV Routing:

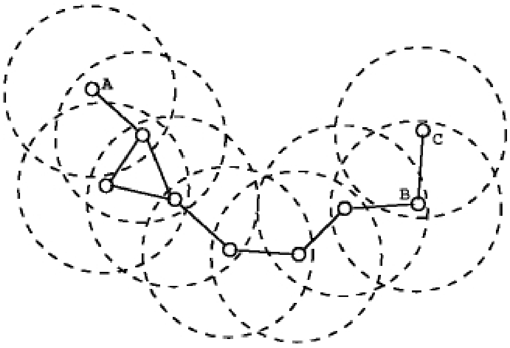

Figure 4-5 AODV Routing

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks.

In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time.

When a link fails, a routing error is passed back to a transmitting node, and the process repeats.

Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

This protocol is being followed in HITOC

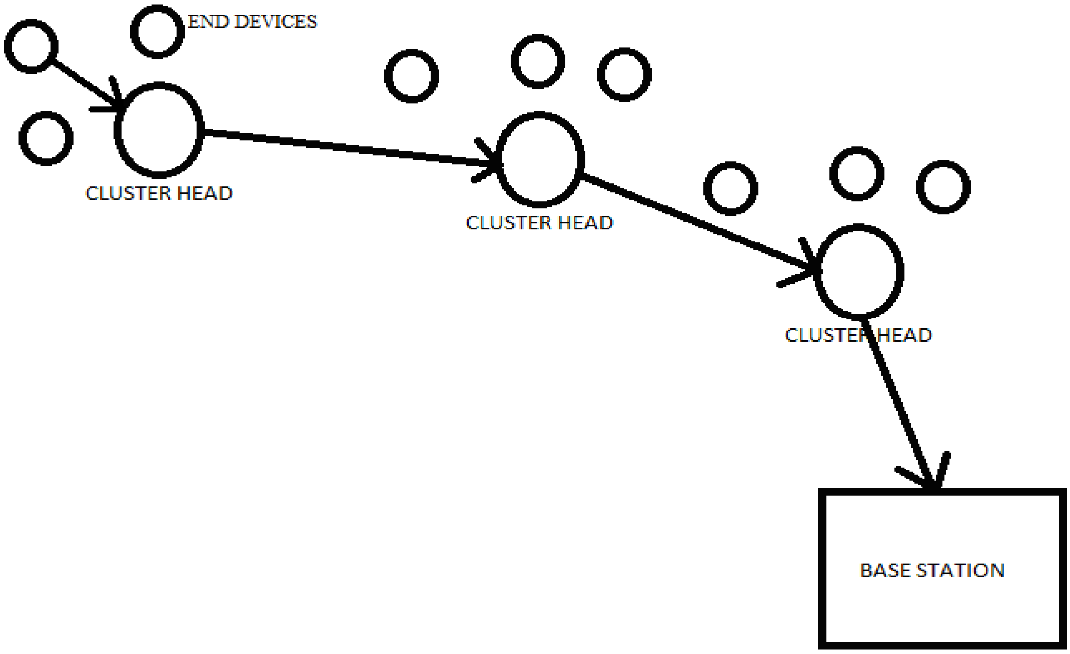

Figure 4-6 AODV Protocol utilization in ZigBee Network

4.5.2 Use Case Diagram

Use Case Diagram shows missions or stakeholder goals. The detailed requirements may then be captured as contractual statements.

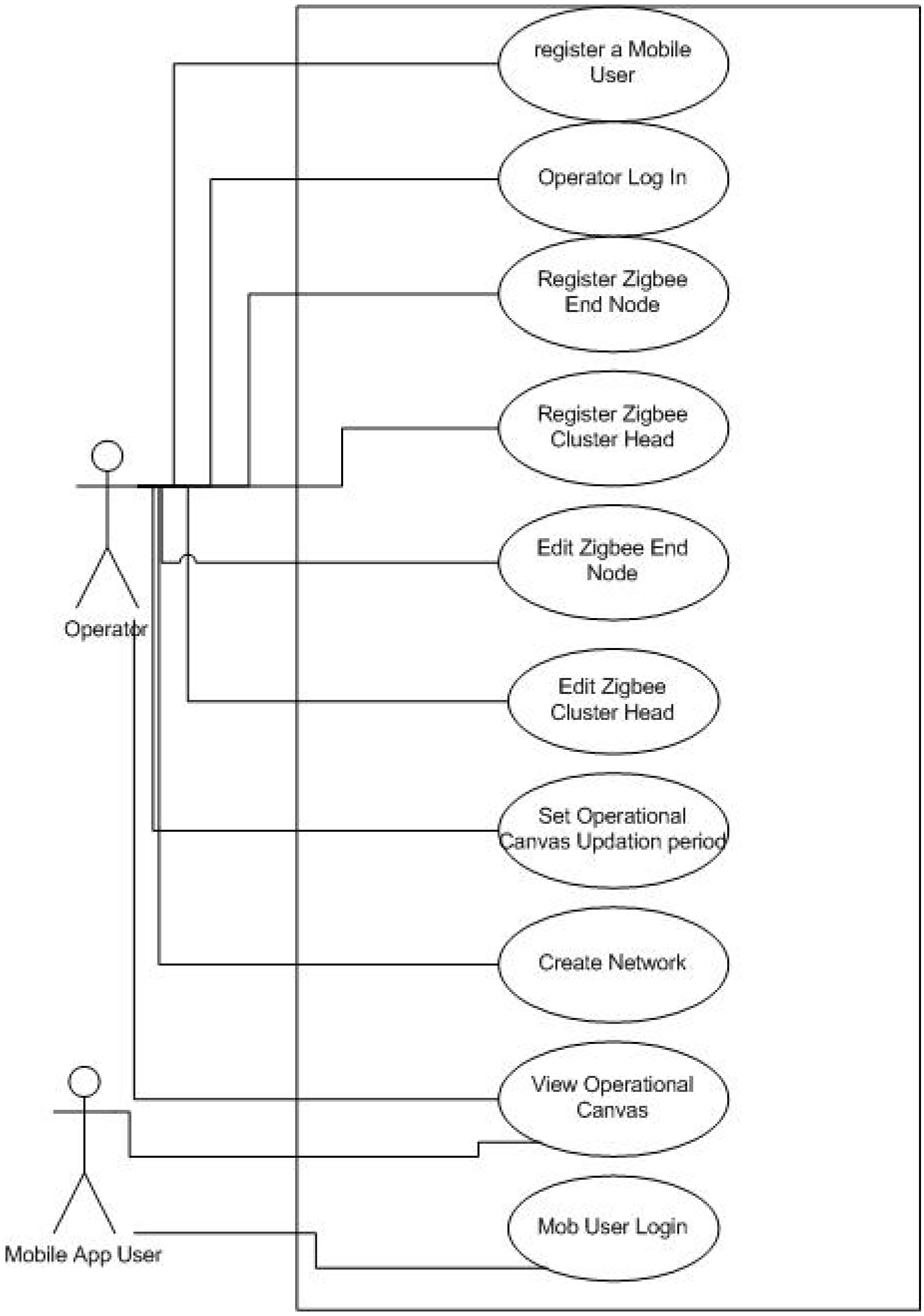

Figure 4-7 HITOC Use Case Diagram

Specification of use cases is given below

a) Operator Login:

Actor: Operator

Provides Login functionality to the base station user with authentication.

b) Register ZigBee End Node:

Actor: Operator

Provides the functionality to add particulars about a ZigBee end device and personal assigned with it.

c) Register ZigBee Cluster Head:

Actor: Operator

Provides the functionality to add particulars about a ZigBee cluster head device and personal assigned with it.

d) Edit ZigBee End Node

Actor: Operator

Provides the functionality to edit particulars about a ZigBee end node device and personal assigned with it.

e) Edit ZigBee Cluster Head

Actor: Operator

Provides the functionality to edit particulars about a ZigBee cluster head device and personal assigned with it.

f) Set Operational Canvas Updation Period:

Actor: Operator

Provides functionality to set updation period after which a stimulus is generated by base station to update personal locations.

g) Create Network:

Actor: Operator

Provides functionality for operator to create a network at start of an operation.

h) View Operational Canvas:

Actor: Operator, Mobile Application User

Provides a user friendly view of the operational canvas to operator and mobile application user.

4.5.3 Sequence Diagrams

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams typically are associated with use case realizations in the Logical View of the system under development.

4.5.3.1 Operator Login

This sequence diagram is describing the “operator login” use case.

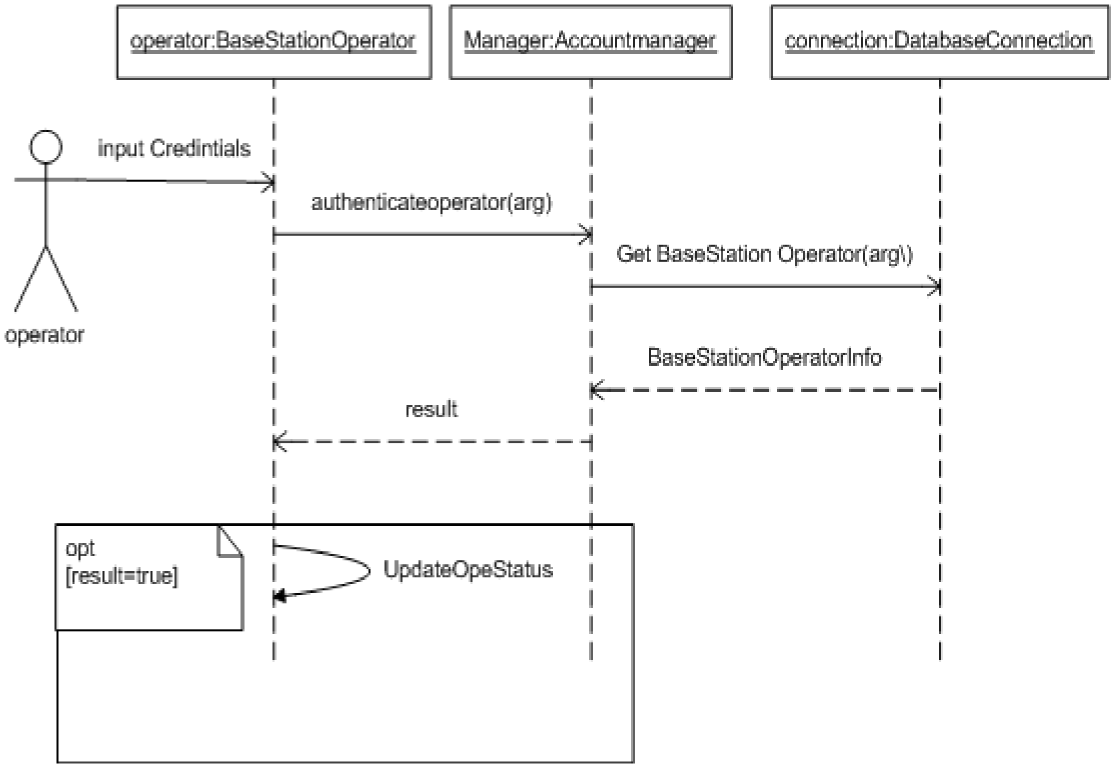

Figure 4-8 Operator Login

4.5.3.2 Register ZigBee End Node

This sequence diagram is describing the “Register Zigbee End Node” use case.

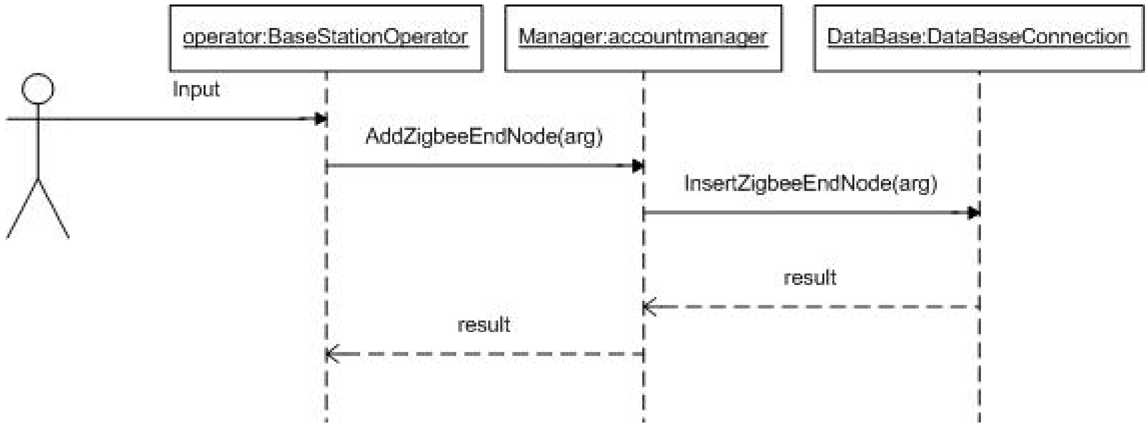

Figure 4-9 Register ZigBee End Node

4.5.3.3 Register ZigBee Cluster Head

This sequence diagram is describing the “Register Zigbee Cluster Head” use case.

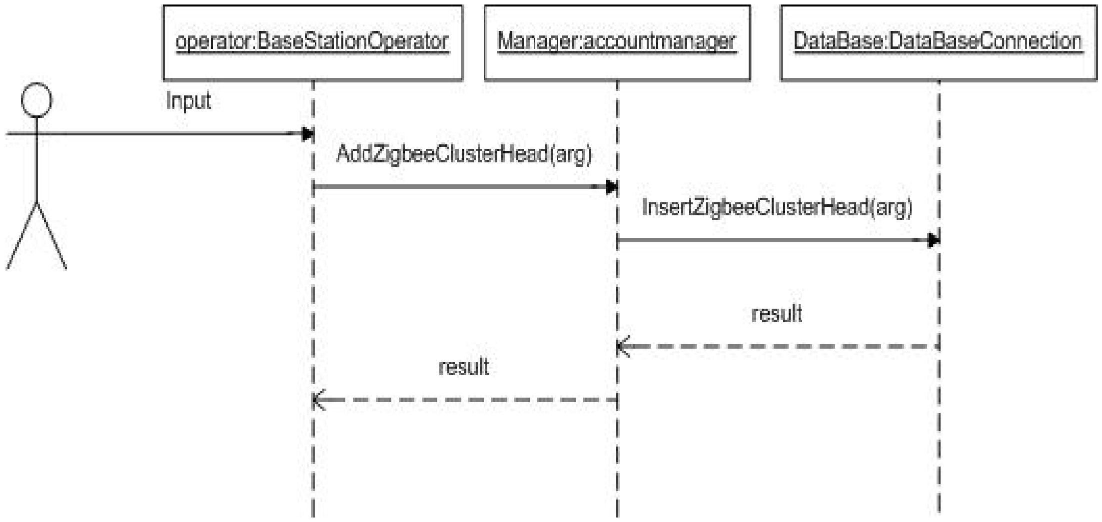

Figure 4-10 Register ZigBee Cluster Head

4.5.3.4 Edit ZigBee End Node

This sequence diagram is describing the "Edit Zigbee End Node" use case.

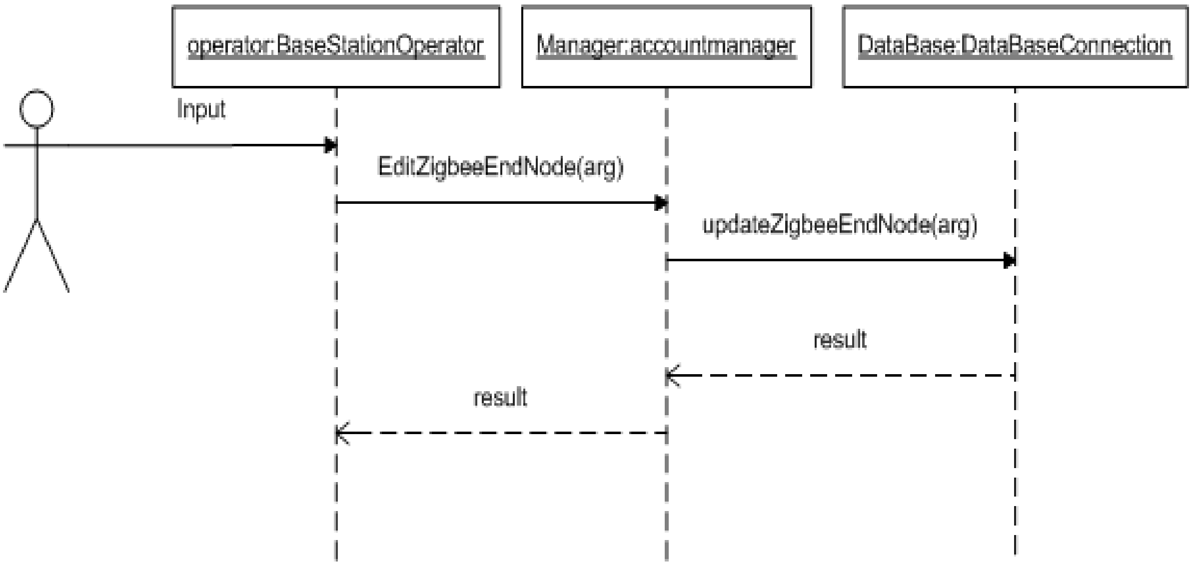

Figure 4-11 Edit ZigBee End Node

4.5.3.5 Edit ZigBee Cluster Head

This sequence diagram is describing the "Edit Zigbee Cluster Head" use case.

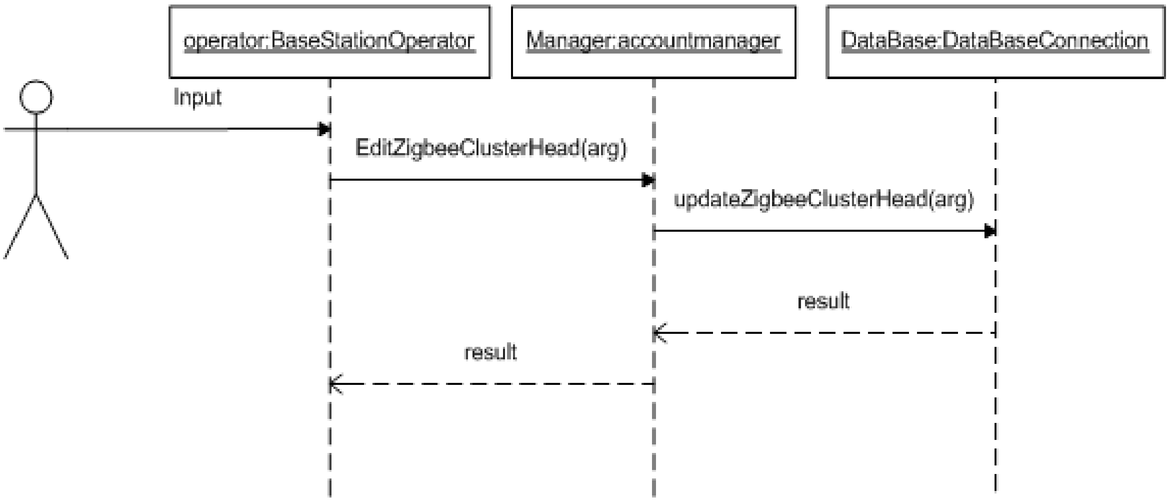

Figure 4-12 ZigBee Cluster Head

4.5.3.6 Set Operational Canvas Updation Period

This sequence diagram is describing the “Set Operational Canvas Updation Period” use case.

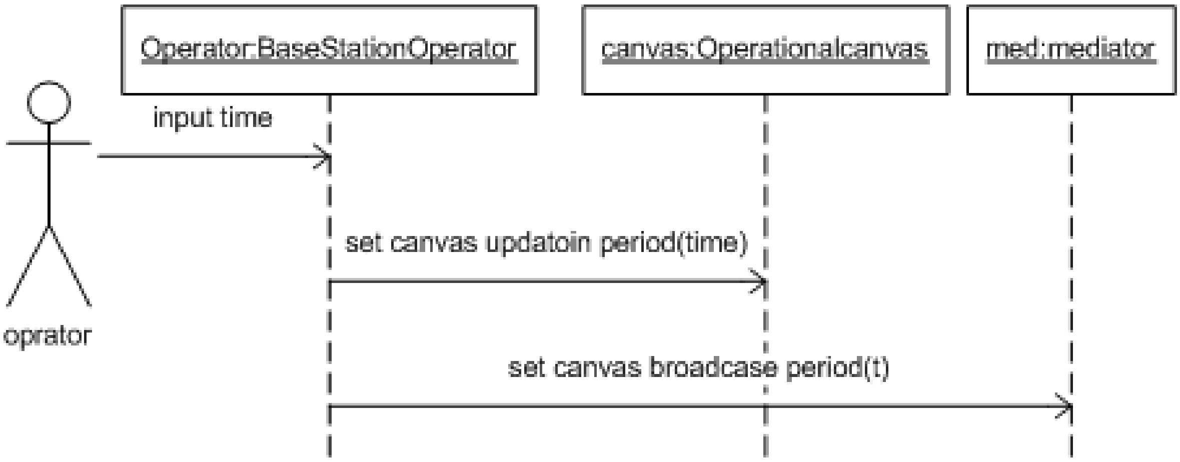

Figure 4-13 Set Operational Canvas Updation Period

4.5.3.7 Create Network

This sequence diagram is describing the “Create Network” use case.

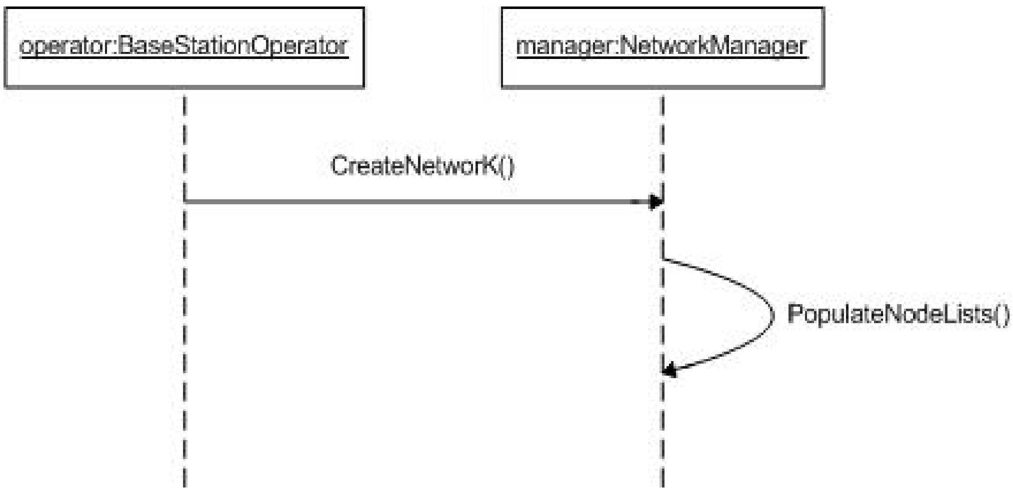

Figure 4-14 Create Network

4.5.3.8 View Operational Canvas Base Station Operator

This sequence diagram is describing the “View Operational Canvas” use case.

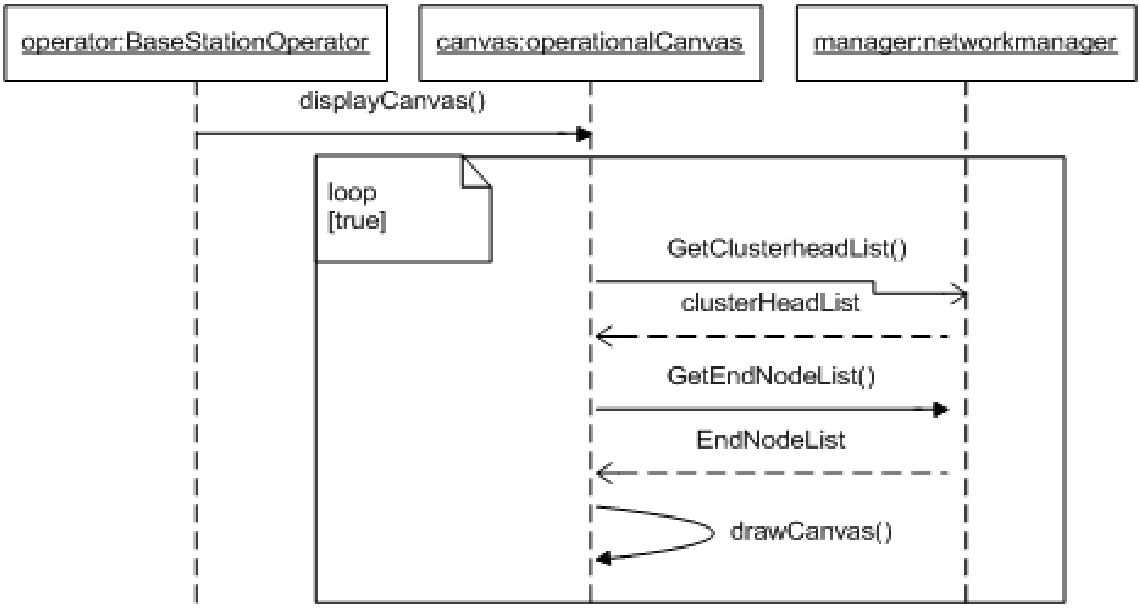

Figure 4-15 View Operational Canvas Base Station Operator

4.5.4 Class Diagram:

This is the class diagram of HITOC System. This is a type of static structure diagram that describes the structure of a HITOC by showing the system's classes, their attributes, operations and the relationships among the classes.

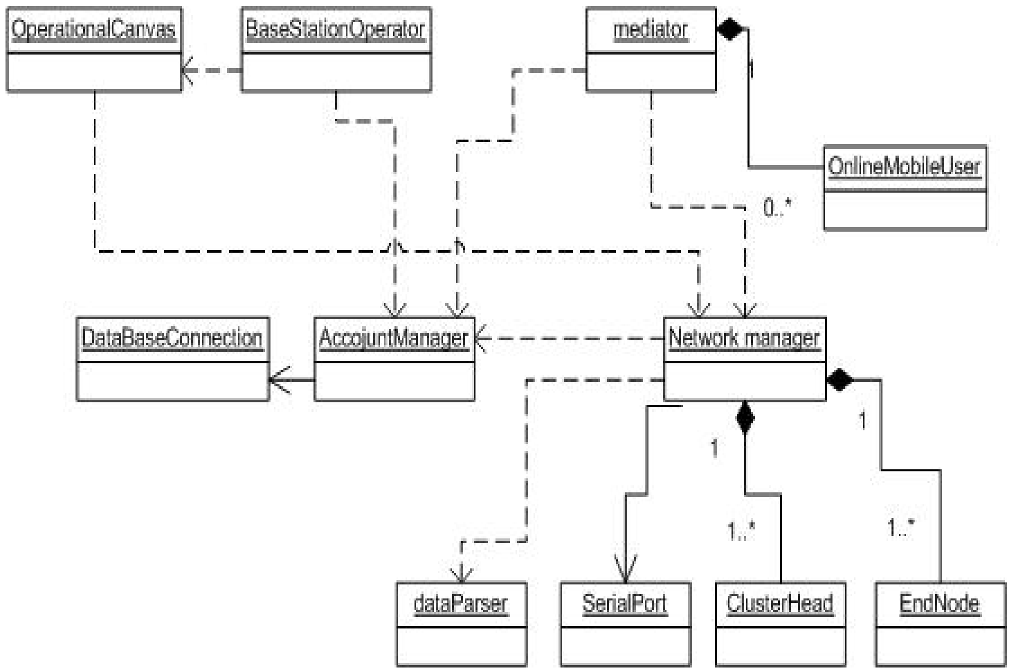

Figure 4-16. Class diagram of HITOC

4.5.5 Design Pattern used in HITOC Design

Singleton design pattern has been used in the design of HITOC**.** It is used when a system only needs one instance of a class, and that instance needs to be accessible in many different parts of a system, you control both instantiation and access by making that class a singleton.

In HITOC there are three such classes (Operational Canvas, AccountManager and NetworkManager) which have to be instantiated just once during execution of HITOC.

Implementation of Singleton Pattern

To implement Singleton pattern we have to make one private static data member of bool type and one public static Method of Singleton class. Public static Method will ensure availability of single instance of Singleton class.

This is the UML class diagram of Singleton pattern.

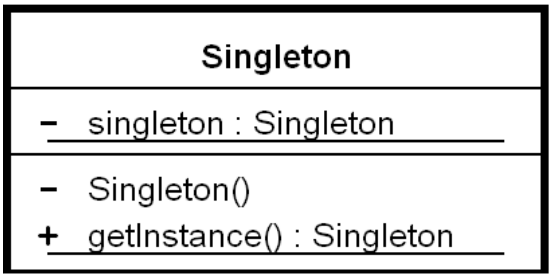

Figure 4-17 Singleton Pattern

4.5.6 Individual Classes Definitions

In this section individual class are defined with their attributes and operations. These classes are from the class diagram given in fig 4-16.

a) Base Station Operator

Base Station operators username and status are maintained in this class.

Attributes and methods of Base Station operator are illutrated in Fig# 4-18

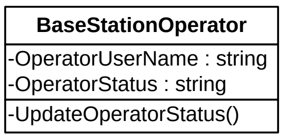

Figure 4-18. Base Station Operator Class Diagram

b) Operational Canvas

Operational canvas view state and updation period is maintained in this class.

Attributes and methods of Operational Canvas are illutrated in Fig# 4-19

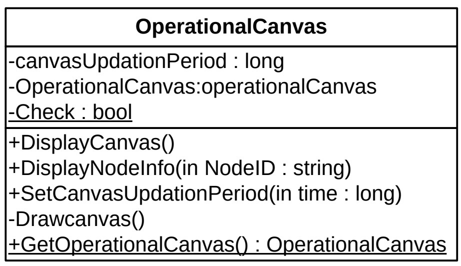

Figure 4-19. Operational Canvas Class Diagram

c) Mediator

Mediator class will broadcast operational canvas to registered mobile devices. It also listens for new mobile user requests. Attributes and methods of Mediator are illustrated in Fig# 4-20

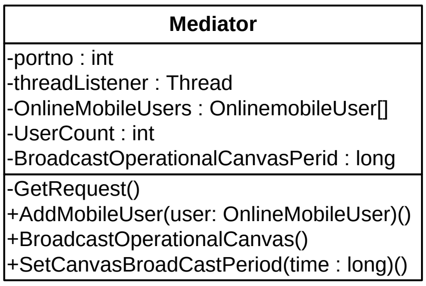

Figure 4-20. Mediator Class Diagram

d) Account Manager

Authentication of users and addition of ZigBee devices to the system is maintained here. Attributes and methods of Account Manager are illustrated in Fig# 4-21

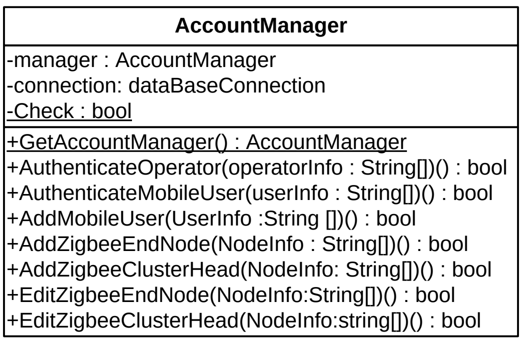

Figure 4-21. Account Manager Class Diagram

e) Database Connection

Connection with Microsoft SQL Server 2008 database and insertion, updation, deletion and retrieval of records from database are carried out through this class methods. Attributes and methods of Database Connection are illustrated in Fig 4-22.

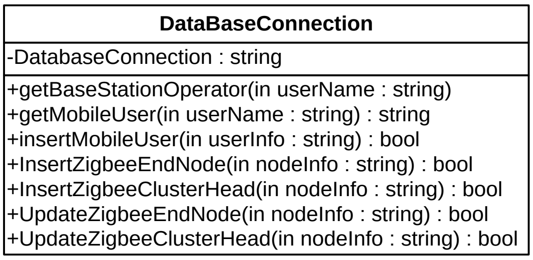

Figure 4-22. Database Connection Class Diagram

f) Network Manager

Interaction with network nodes is carried out through this class methods. Attributes and methods of Network Manager are illustrated in Fig# 4-23

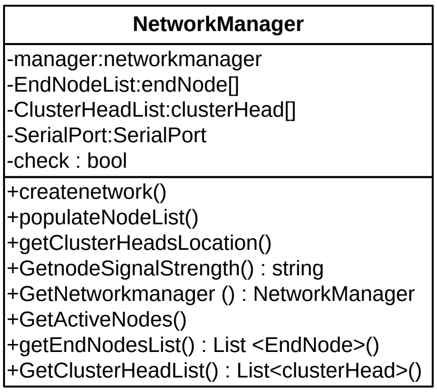

Figure 4-23. NetworkManager Class Diagram

g) Serial Port

Serial port access to control ZigBee sink device is maintained in Serial port class. Attributes and methods of Serial Port are illustrated in Fig#4-24

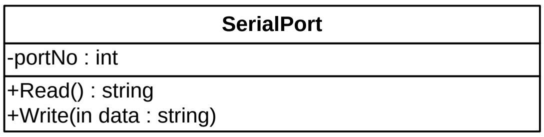

Figure 4-24. Cluster Head Class Diagram

h) Data Parser

Parsing of strings received from serial port are done to retrieve desired data using data parser methods. Attributes and methods of data parser are illustrated in Fig# 4-25

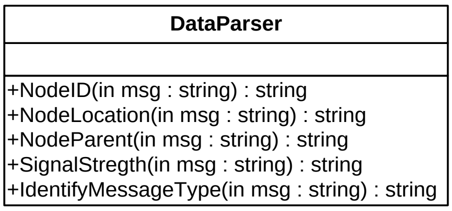

Figure 4-25. Cluster Head Class Diagram

i) End Node

This class specifies a ZigBee end node device. Attributes and methods of End Node are illustrated in Fig# 4-26

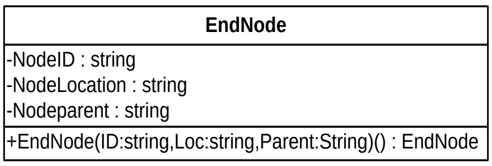

Figure 4-26. End Node Class Diagram

j) Cluster Head

This class specifies a ZigBee cluster head device. Attributes and methods of Cluster Head are illustrated in Fig# 4-27

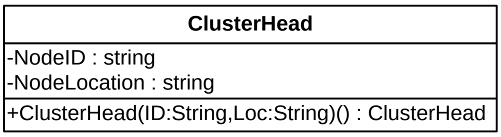

Figure 4-27. Cluster Head Class Diagram

5. ERD of HITOC

ERD of HITOC includes four entities Operator, Mobile App User, Zigbee Cluster Head and Zigbee End Node.

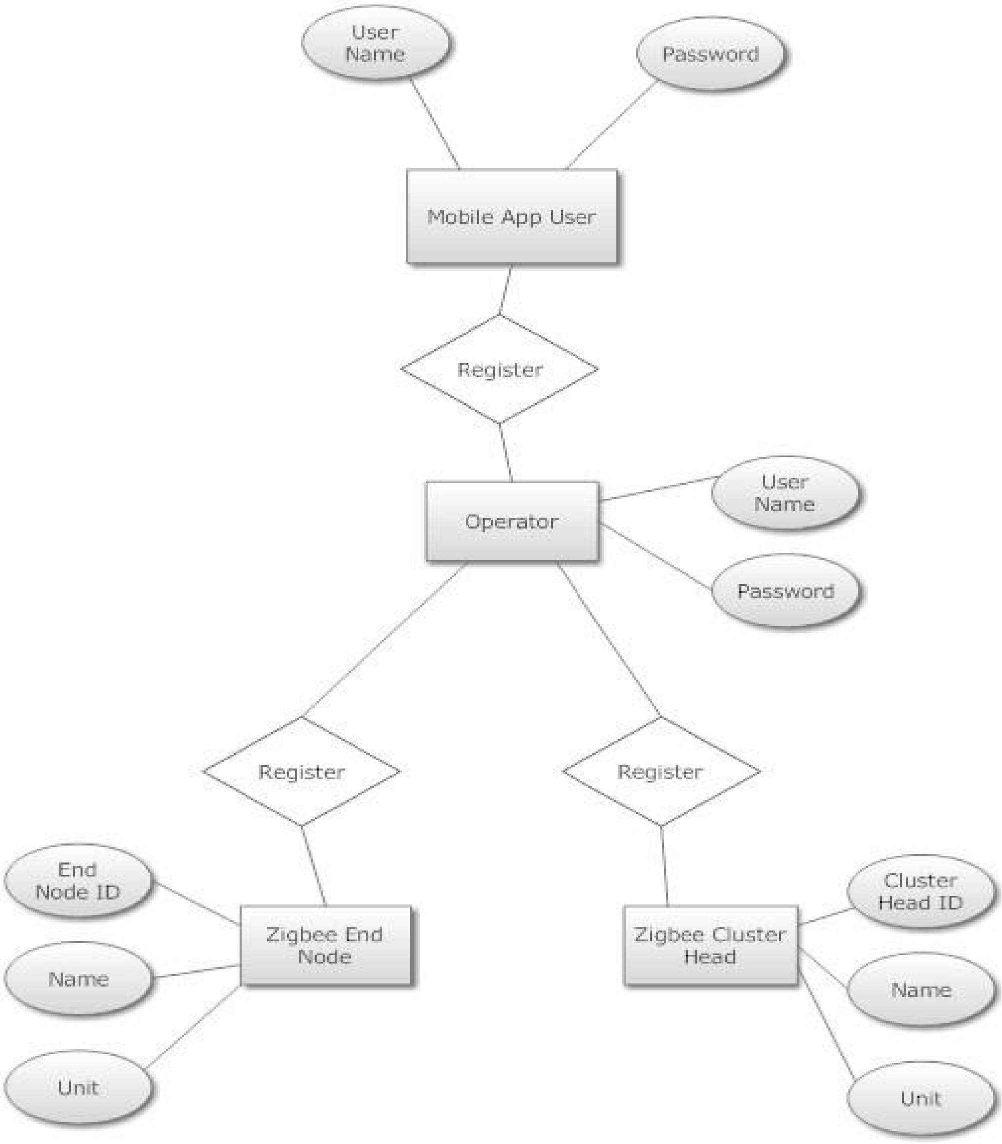

Figure 2-28. ERD of HITOC

5 Chapter

Implementation

5.1 Introduction

The previous chapter discussed the design; inner details of the class attributes and methods, Use case diagram etc. Based on that design this chapter will concentrate on the implementation details of the system.

We have categorized implementation details into Location Tracking, routing protocol and Handy Tool for Identification and Tracking on Operational Canvas (HITOC) application. Therefore, in the remaining of this section implementation details regarding these modules have been presented.

5.2 Device Registration

Each Zigbee device has to be registered before it has to be operational and given to any operational participant. Registration means store the records of a device the information of the person to whom it will be allocated during an operation. Each Zigbee device has a 64 bit unique identifier which is used to uniquely distinguish a device. Zigbee device record is saved into database against that 64 bit id. In our case there are two type of devices

1. Zigbee Cluster Head

2. Zigbee End Node

5.2.1 Zigbee Cluster Head Registration

As Zigbee Cluster Head is an entity so a table in the database is generated to store the records of all the cluster heads which consists on the following attributes

1. Cluster Head ID

2. Name of person

3. Rank

4. Unit No

Cluster Head ID serves as the primary key to distinguish a record.

5.2.2 Zigbee End Node Registration

As Zigbee End node is also an entity so a table in the database is generated to store the records of all the end node devices which consists on the following attributes

1. End Node ID

2. Name of person

3. Rank

4. Unit No

End Node ID serves as the primary key to distinguish a record.

5.3 Zigbee Network Formation

When devices are registered they become operational and can be used in the operation. After that an establish network command is initiated from the base station to form the network. ZigBee devices use AD-hoc On-demand Distance Vector (AODV) routing protocol. In order to find the destination device, it broadcasts out a route request to all of its neighbors. The neighbors then broadcast the request to their neighbors, until the destination is reached. Once the destination is reached, it sends its route reply via unicast transmission following the lowest cost path back to the source. Once the source receives the reply, it will update its routing table for the destination address with the next hop in the path and the path cost.

5.3.1 Create Network

```
public EstablishNetwork(String port)
        {
            InitializeComponent();
            markerAccessCechk = false;
            SP = port;
            clusterHead = new ClsterHead();
            endNodeList = new List<EndNd>();
            overLay1 = new GMapOverlay(gMapControl1, "overLay1");
            endNodeMarkerList = new List<CustomeMarkerGreen>();

            CH = "000D6F0000D5CD45";

            serialPort.BaudRate = 19200;
            serialPort.PortName = SP;
            serialPort.ReadTimeout = 60000;
            serialPort.Open();
            serialPort.Write("at+en\r");

            timer.Tick += new EventHandler(timer_Tick);
            timer.Interval = 30000;
            timer.Enabled = true;

        }
```

5.3.2 Scan network thread code-snippet

```
void ScanNetworkThread()
        {
            try
            {
                clusterHead = new ClsterHead();
                if (endNodeList.Count > 0)
                    endNodeList.Clear();
                count = 0;
                serialPort.DiscardInBuffer();
                serialPort.Write("at+sn\r"); // AT command
                String temp = serialPort.ReadLine();
                Thread.Sleep(2000);
                int i = 0;
                while (i < 10)
                {
                    if (serialPort.BytesToRead > 0)
                    {
                        temp = serialPort.ReadLine();
                        if (temp.Length > 6)
                        {
                            if (temp[0] == 'S')
                            {
                                String[] arr = temp.Split(new Char[] { ',' });
                                if (arr[1] == CH)
                                {

                                                        clusterHead.nodeID = arr[1];
                                    clusterHead.networkID = arr[2];
                                    if (serialPort.BytesToRead > 0)
                                        temp = serialPort.ReadLine();
                                }
                                else
                                {
```

```
                        EndNd node = new EndNd();
                        node.nodeID = arr[1];
                        node.networkID = arr[2];

                        if (serialPort.BytesToRead > 0)
                            temp = serialPort.ReadLine();

                        endNodeList.Add(node);
                        count++;
                    }
                }
            }
        }

    }
}
catch (Exception ex)
{

}
}
```

5.3.3 Close network Code

```
private void btnCloseNetwork_Click_1(object sender, EventArgs e)
    {
        serialPort.Write("at+dassl\r");
        serialPort.Close();
        if(mainThread!=null)
            mainThread.Abort();
        this.Close();
    }
```

5.4 Location Tracking of operational participants

Once network is formed and becomes operational then we need to capture the location of the individuals that are participant of the network.

5.4.1 Location Capturing

Zigbee Cluster Head device is equipped with the GPS receiver to get its location in the form of latitude and longitude. Cluster Head device reads data from the GPS and stores it in its memory register. Then all the cluster head devices are visited to get their location. Once location data is arrived at base station in form of a string then it is parsed to get the actual location. Besides the cluster head devices there are end node devices as well. Their location is captured according to their parent cluster head devices. Parent node of an end node is identified then distance of the end node from its parent cluster head is calculated on the basis of signal strength drop at the parent node.

Location is captured continuously after a period of time and shown on the map to keep it updated.

5.4.2 Location Plotting

Once location is captured and available at base station then it has to be plotted at the Google map to show it graphically to the user. For the purpose Google map API is used in the project which takes the input in the form of latitude and longitude and show that location on the map. That location is represented by a marker.

```
void ShowMarkers()
    {
        try
        {
            if (clusterHead.nodeID != null)
            {
                serialPort.DiscardInBuffer();
                serialPort.Write("ats3c?\r");
                Thread.Sleep(200);
```

```
String temp = "";

if (serialPort.BytesToRead > 0)

{

    temp = serialPort.ReadLine();

}

if (serialPort.BytesToRead > 0)

    temp = serialPort.ReadLine();

if (temp.Length > 7)

{

    String[] arr = temp.Split(new Char[] { ',' });

    clusterHead.latitude = Double.Parse(arr[0]);

    clusterHead.longitude = Double.Parse(arr[1]);

    PointLatLng p = new PointLatLng();

    p.Lat = clusterHead.latitude + 0.231642;

    p.Lng = clusterHead.longitude + 0.02482;



    while (markerAccessCechk)

    {
```

```
    Thread.Sleep(100);
}
if (marker != null)
{
    overLay1.Markers.Remove(marker);
}
marker = new CustomeMarker(p);
marker.ID = clusterHead.nodeID;
overLay1.Markers.Add(marker);
if (endNodeMarkerList.Count > 0)
{
    for (int j = 0; j < endNodeMarkerList.Count; j++)
    {
        overLay1.Markers.Remove(endNodeMarkerList[j]);
    }
    endNodeMarkerList.Clear();
}
if (endNodeList.Count > 0)
```

```
{
    for (int j = 0; j < endNodeList.Count; j++)
    {
        PointLatLng p1 = new PointLatLng();
        p1.Lat = p.Lat - ((j + 1)/10000.0);
        p1.Lng = p.Lng - ((j + 1)/10000.0);
        if (j == 0)
        {
            p1.Lat = p.Lat - (1 / 10000.0);
            p1.Lng = p.Lng - (1 / 10000.0);
        }
        else if (j == 1)
        {
            p1.Lat = p.Lat + (1 / 10000.0);
            p1.Lng = p.Lng - (1 / 10000.0);
        }
        else if (j == 2)
        {
```

```
    p1.Lat = p.Lat + (1 / 10000.0);
    p1.Lng = p.Lng + (1 / 10000.0);
}
else if (j == 3)
{
    p1.Lat = p.Lat - (1 / 10000.0);
    p1.Lng = p.Lng + (1 / 10000.0);
}
else if (j == 4)
{
    p1.Lat = p.Lat;
    p1.Lng = p.Lng - (2 / 10000.0);
}
else if(j==5)
{
    p1.Lat = p.Lat + (2 / 10000.0);
    p1.Lng = p.Lng;
}
```

```
    else if (j == 6)
    {
        p1.Lat = p.Lat;
        p1.Lng = p.Lng + (2 / 10000.0);
    }
    else
    {
        p1.Lat = p.Lat - (j / 10000.0);
        p1.Lng = p.Lng - (j / 10000.0);
    }
    if (j < count)
    {
        CustomeMarkerGreen node = new CustomeMarkerGreen(p1);
        node.ID = endNodeList[j].nodeID;
        endNodeMarkerList.Add(node);
        overLay1.Markers.Add(node);
    }
}
```

```
        }
    }
}
else
{
    while (markerAccessCechk)
    {
        Thread.Sleep(100);
    }


    if (marker != null)
    {
        overLay1.Markers.Remove(marker);
    }
    if (endNodeMarkerList.Count > 0)
    {
        for (int j = 0; j < endNodeMarkerList.Count; j++)
        {
```

```
                    overLay1.Markers.Remove(endNodeMarkerList[j]);
                }
                endNodeMarkerList.Clear();
            }
        }
    }
    catch (Exception ex)
    {
        //MessageBox.Show("Show Markers Exception");
    }
}
```

5.5 Device Identification

One objective of the system is to identify the person to whom zigbee device is handed over. For that purpose device unique 64 bit identifier is used which is captured from the response message of the device and matched in the database to find the record of registered device. User has been given the facility to identify the individual by clicking on a marker on the map. When he clicks on the marker the information of that person is shown to the user.

5.6 Summary

The implementation of final product has been explained in this chapter. Implementation of the routing protocol and the HITOC has been explained in detail. For complete detailed Code Please see the given CD.

6 Chapter

Testing

6.1 Introduction

Most important issue related to any project is to ensure that the quality of the product is high and it is efficient therefore testing of the software is conducted. In Software projects special importance is given to the testing and it is one phase of Software development life cycle, no software project is completed without testing. The HITOC project is no exception. Testing techniques which are used in testing of HITOC to obtain the high quality product are discussed in this chapter.

6.2 Testing Techniques and Levels

Testing of the software projects involve different levels of testing to make sure that the software which is being developed is error and fault free. HITOC has different modules which were developed separately depending up on the functionalities. Therefore testing of all the modules has to be done and testing while integrating all the modules. The different levels at which testing was done are discussed here.

6.2.1 Unit testing

Unit testing involves the testing of each module at the completion and sometimes during the development of the module. The testing of each module is carried out on the basis of the defined data sets. HITOC was divided in to four different modules that are Getting & Transmitting location, Network Creation, Multi hop routing protocol and HITOC (Software Application).

6.2.1.1 Getting & Transmitting Location

The unit testing of the module is done by taking the original location through google maps. There was a slight variation in the expected and actual output. The result of unit testing showed that the location measured by GPS had some slight difference from the actual location. The reason was that because we had used a self made(given by college authorities) GPS which was not so accurate So a correction factor is added in to the received location.GPS module was integrated with baseStation and the data sent b GPS was received successfully.

6.2.1.2 Network Creation

In this module creation of zigbee network was tested. Sink device is in broadcast mode when turned on. A number of end node devices were checked whatever they create network or not. Only those devices which were not in the 100 m range of any other end device were cut off, rest made network successfully. The path taken by every device’s data was also visible.

6.2.1.3 Multi Hop Routing Protocol

The multi hop routing protocol is the most important module of the HITOC because it deals with the transfer of data from the different nodes to the sink node. The testing was carried out by placing the nodes at varying distances from each other and the sink. The contents of the packets received were observed to ensure that correct data reached the sink. The testing process revealed that communication deteriorated if the distance between nodes was above 100 meters. Also communication faltered when there were many obstructions between communicating nodes.

Certain delays are caused in the cases of node relocation, adding a new node to the network, removing a node from the network. Also a delay is caused during a multi hop transmission at intermediate nodes. All of the above mentioned delays were in the range of 3-4 seconds.

6.2.1.4 HITOC Application

This is the software application of the system which displays the data coming from different devices to the sink node. It also process data map the location on operational canvas.

In order to test the application the network was set up and then it was tested for different events. The application was tested for changes in network configuration and for renaming of zigbee nodes.

6.2.2 Integration Testing

Integration testing is the type of testing which is performed when different modules of the system are combined to form a whole system. This testing level ensures that the system is stable and performs as expected after integrating the individually tested modules. The modules as mentioned above and the precious chapters were integrated and tested. The results produced were satisfactory to the fact that the system correctly reported events and multi-hop routing was operational. All modules communicated with each other as expected. Upon receipt by the sink, the data was successfully read by the HITOC and respective data was generated.

6.2.3 System Testing

System testing is the level of testing which comes when the whole system has been developed and integrated. The complete system was tested in different places with different conditions to verify that those conditions do not disrupt the performance of the system. The testing was carried out both indoors and outdoors. The only significant finding was that the coverage area of the network was more outside than inside the buildings.

6.3 Software Test Cases

6.3.1 Test Case 1

Test Case Description: Aim to design this test case is to test that whether base station operator is able to login to system or not.

Prerequisite Requirements: Login form should be visible, username and password text boxes should be available with appropriate text captions, login button should be available.

TC ID	Test Case Name	Actions/Steps	Results
TC1	Test Base Station Login Functionality	Write Username	Username is accepted
		Write Password	Password is accepted
		Press Login Button	Login button pressed and new form is appeared if username and password is correct otherwise it shows an error message.

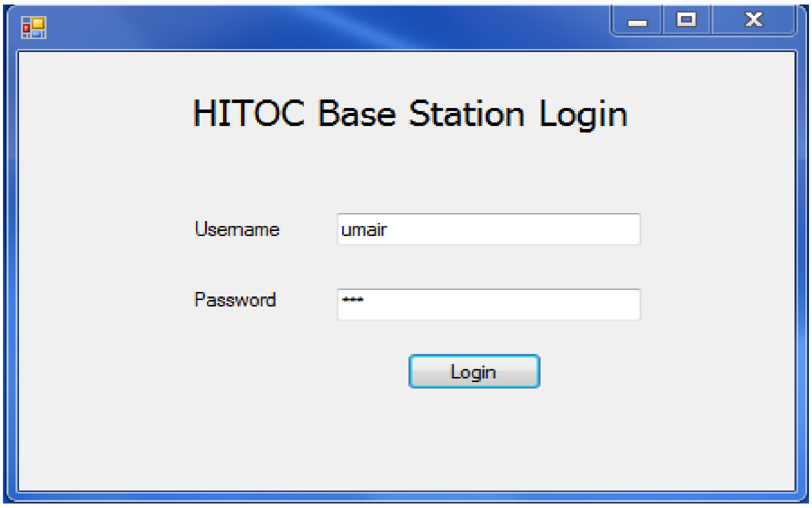

Figure 6-1

Summary: Figure 6-1 shows that Test Case 6.3.1 has been successfully tested.

6.3.2 Test Case 2

Test Case Description: The purpose of this test case is to check that base station operator should be able to establish zigbee network.

Prerequisite Requirements: Establish network form should be visible, Sink device should be attached to the system and Establish network button should be available with appropriate text caption.

TC ID	**Test Case Name**	**Actions/Steps**	**Results**
TC2	Test Zigbee Network Establishment	User selects com port of Zigbee Sink Device	Appropriate Com port is selected
		User presses Establish button	Zigbee Network is established and new form is appeared

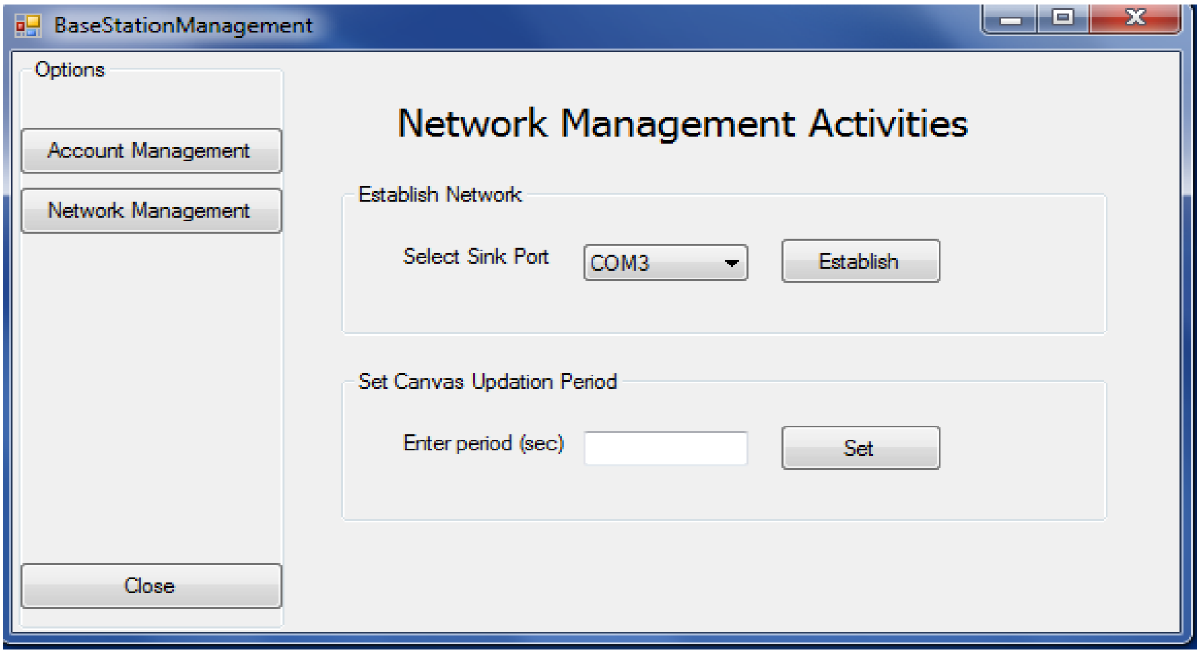

Figure 6-2

Summary: Figure 6-2 shows that test case 6.3.2 has been successfully tested.

6.3.3 Test Case 3

Test Case Description: The purpose of this test case is to test established zigbee network functionality which includes testing of addition and removal of network nodes from the zigbee network.

Prerequisite Requirements: Zigbee network should be established and end node device should be in the range of network.

TC ID	Test Case Name	Actions/Steps	Results
TC3	Test established Zigbee Network functionality	User switch on a zigbee device	Zigbee device joins the network and appears as a marker on the map at base station as a part of the network
		User switch off a Zigbee device	Zigbee device leaves the network and disappears on the map

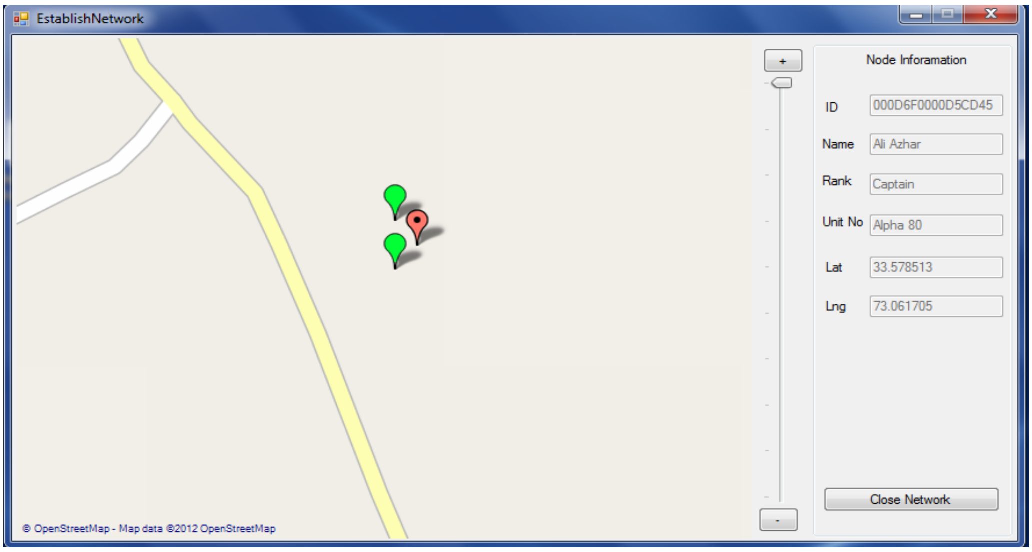

Figure 6-3

Summary: Figure 6-3 shows that test case 6.3.3 has been successfully tested.

6.3.4 Test Case 4

Test Case Description: The purpose of this test case is to verify the identification of the zigbee end node. Identification means name, rank etc. of the individual holding the zigbee device.

Prerequisite Requirements: Zigbee network should be established and the device you want to identify should be part of the network and visible on the map at the base station.

TC ID	Test Case Name	Actions/Steps	Results
TC4	Test identification of the zigbee end node	User should bring the cursor at the marker of the targeted device on the map	Cursor should be on the marker and changes from arrow to hand symbol which indicates that it is ready to be clicked
		User clicks on the marker	System shows the information of the marker of the zigbee end node in the

			window at the right hand side

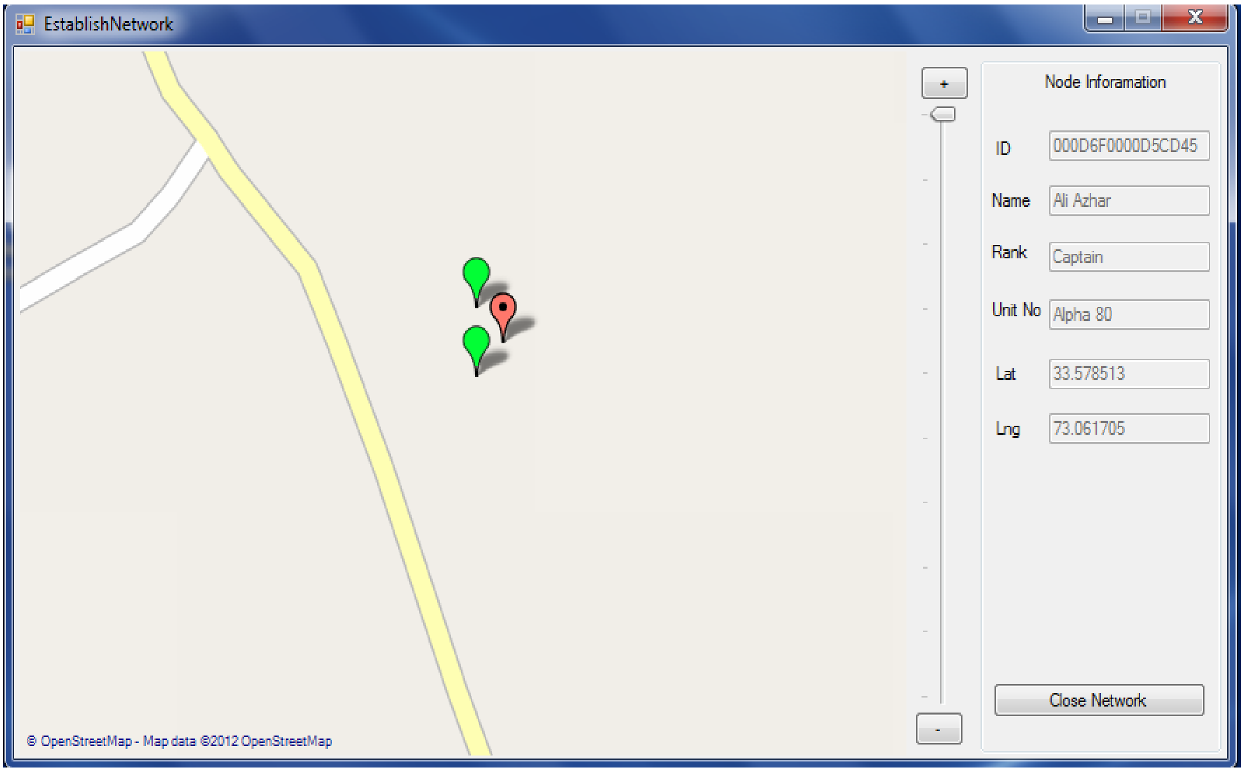

Figure 6-4

Summary: Figure 6-4 shows that test case 6.3.4 has been successfully tested.

6.3.5 Test Case 5

Test Case Description: The purpose of this test case is to verify that the system is exited successfully.

Prerequisite Requirements: System should be in running mode.

TC ID	Test Case Name	Actions/Steps	Results
TC5	Test the closing the system	User presses the close button	System closes all the sub applications, background threads and leaves all the captured resources

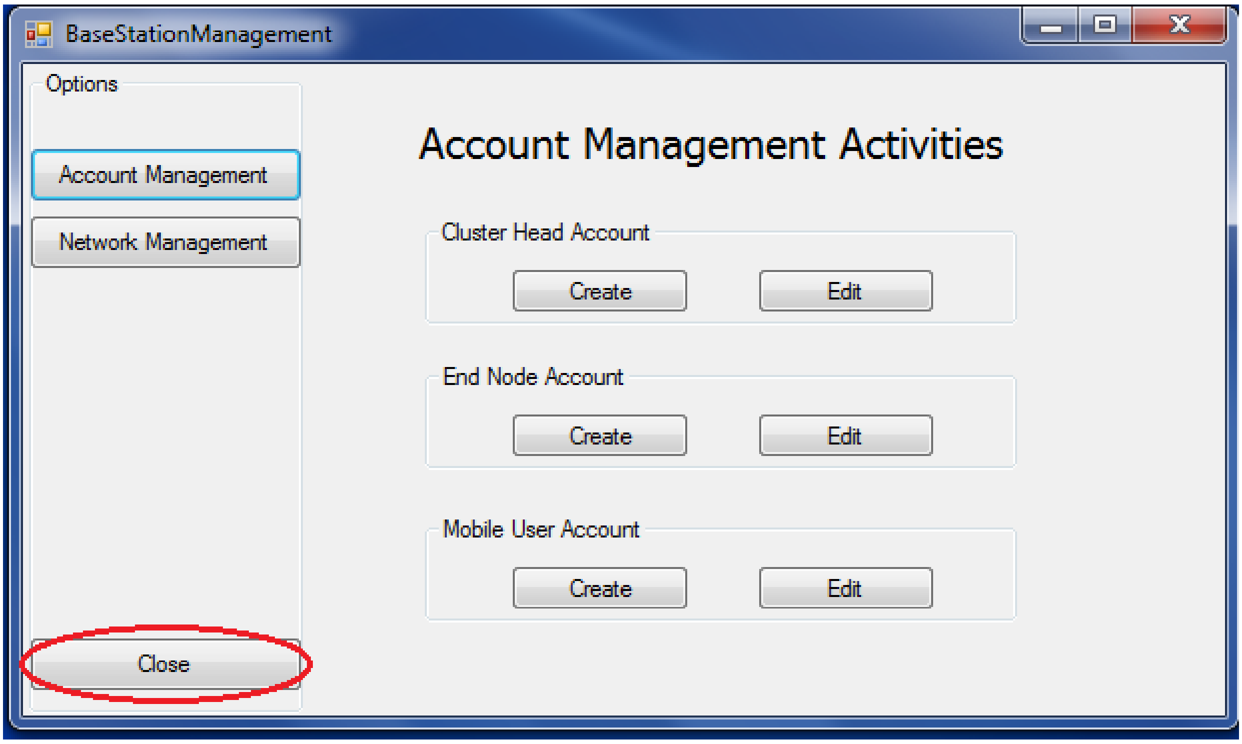

Figure 6-5

Summary: Figure 6-5 shows that test case 6.3.5 has been successfully tested

6.4 Hardware Test Case

Three types of tests were performed on ZigBee modules to assure reliable performance. These tests were performed using Windows HyperTerminal running on the base station to check ZigBee devices response.

1- Network Joining Test
2- Network Leaving Test
3- Range Test

6.4.1 Network Joining Test

The ZigBee devices were tuned with AT commands to check every 10 sec whether they are part of a network or not, if not, scan for the available network and join the best one.

Input	Expected Output	Actual Output
Start device with previous network available	The device should leave the previous network and then search for new one, in this case it should join the network after 10 seconds	The device joins the network at 10 seconds, 20 seconds or 30 seconds.
Start device with a new network	The device should leave the initial network and then search for new one, in this case it should join the network after 10 seconds	The device joins the network at 10 seconds, 20 seconds or 30 seconds at different occasions.
Shutdown network but keep device on and then create a new network	The device manufacturer stated that devices should join leave and join the new network with in a period of 1 minute	The devices didn't work as specified by the manufacturer. So we made an assumption that network is not going to be destroyed in the operational time.
The device goes out of reach	It should join the network again when it comes in the range of network within	The device joins the network at 10 seconds, 20 seconds or 30 seconds after coming back in

	10 seconds.	networks reach.

6.4.2 Network Leaving Test

Initially the ZigBee devices were tuned to search for the previous network they were the part of at startup, but this behavior was not suitable for HITOC so we tuned the devices with AT commands to leave the network it was initially part of at startup and then search for available networks after 10 seconds and join the best one.

Input	**Expected Output**	**Actual Output**
Start device with previous network available	The device should leave the previous network and then search for new one, in this case it should join the network after 10 seconds	The device left the initial network at startup and then joins the network at 10 seconds, 20 seconds or 30 seconds.
Start Device with no network	The device should leave previous network and stay unconnected	The device leaves previous network and stays unconnected
Start device with a new network	The device should leave the initial network and then search for new one, in this case it should join the network after 10 seconds	The device leaves the previous network at startup and then joins the new network at 10 seconds, 20 seconds or 30 seconds.

6.4.3 Range Test

ZigBee devices with external antennas connected works about 100 meters in open air and about 40 to 50 meters indoor. The devices without in internal built in antennas work 50 to 60 meters in open air and 20 to 25 meters indoor.

Input	**Expected Output**	**Actual Output**
Move external antenna attached devices in 100 meter outdoor radius of other devices	Device should remain in network	Device remains in network
Move external antenna attached devices beyond 100 meter outdoor radius of other devices	Device may go out of range	Device goes out of range
Move internal antenna devices in 50 to 60 meter outdoor radius of other devices	Device should remain in network	Device remains in network

Move internal antenna devices beyond 50 to 60 meter outdoor radius of other devices	Device may go out of range	Device goes out of range

6.5 Summary

Testing is one of the most important phases of software development life cycle because by testing one can ensure the quality and performance of the product as expected. Different testing approaches were applied on the HITOC to make system which lead to a more stable and correct version of the system.

7 Chapter

Result and Analysis

7.1 Introduction

HITOC is a real time application to provide accurate locations of personals in operational areas. It gets the location and transmit it to the base station where location is plotted on an operational canvas. The information of device bearer and devices is also visible on screen. The system provides all these services by using Telegesis device ETRX3 which communicates wirelessly to a central device where the HITOC Application is deployed.

7.2 Result

HITOC deals with safety and security issues which makes this system sensitive and important. The basic concept of the project is to facilitate organizations with displaying locations of the personals in the operational areas. The main objective of the project was achieved which is discussed in this section.

The main objectives of project was to develop a self configuring multi hop routing protocol for wireless communication, Identification and tracking of personals in the operational area and display the results on a screen at base station.

Each of the modules has been tested and results gathered. These are documented below

7.2.1 Getting, transmitting and showing node locations

GPS integration with HITOC, getting and transmitting location was the most important part of the project. GPS was provided by the department whose data format was studied deeply in order to extract the information which fulfilled our interests.

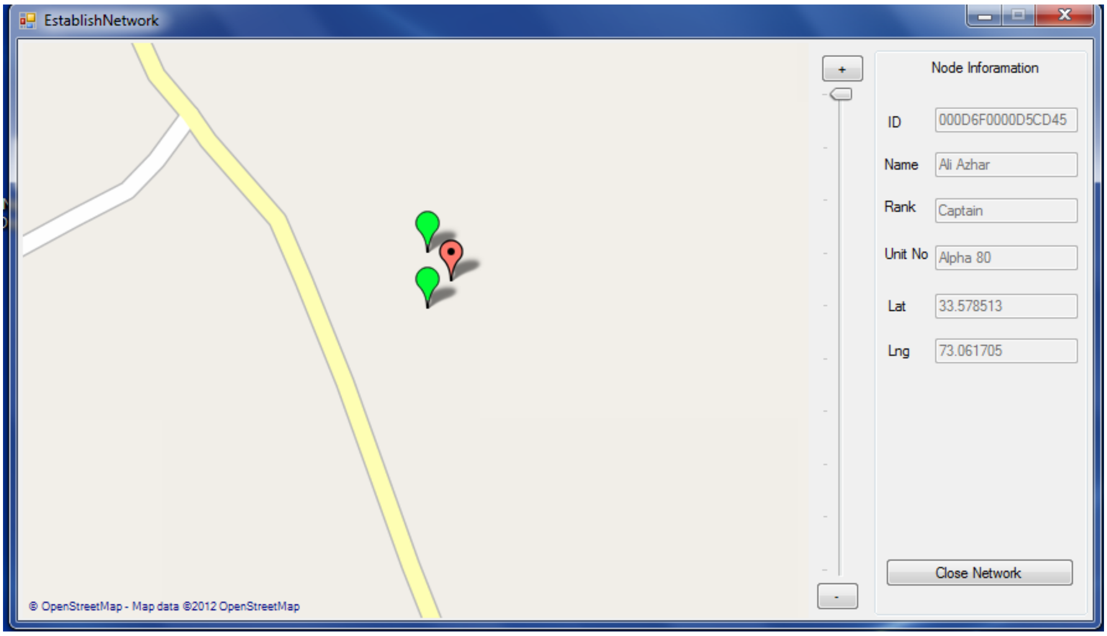

Figure7.1 Locations plotted

The figure 7-1 is showing three devices locations which were received at the sink node.

7.2.2 Multi Hop routing protocol

Multi hop routing is an important objective of the system because it involves the transfer of data from the end node to the sink node.

7.2.3 Configuring & Updating Nodes

Information associated with devices are configured and updated whenever a new operation is started.

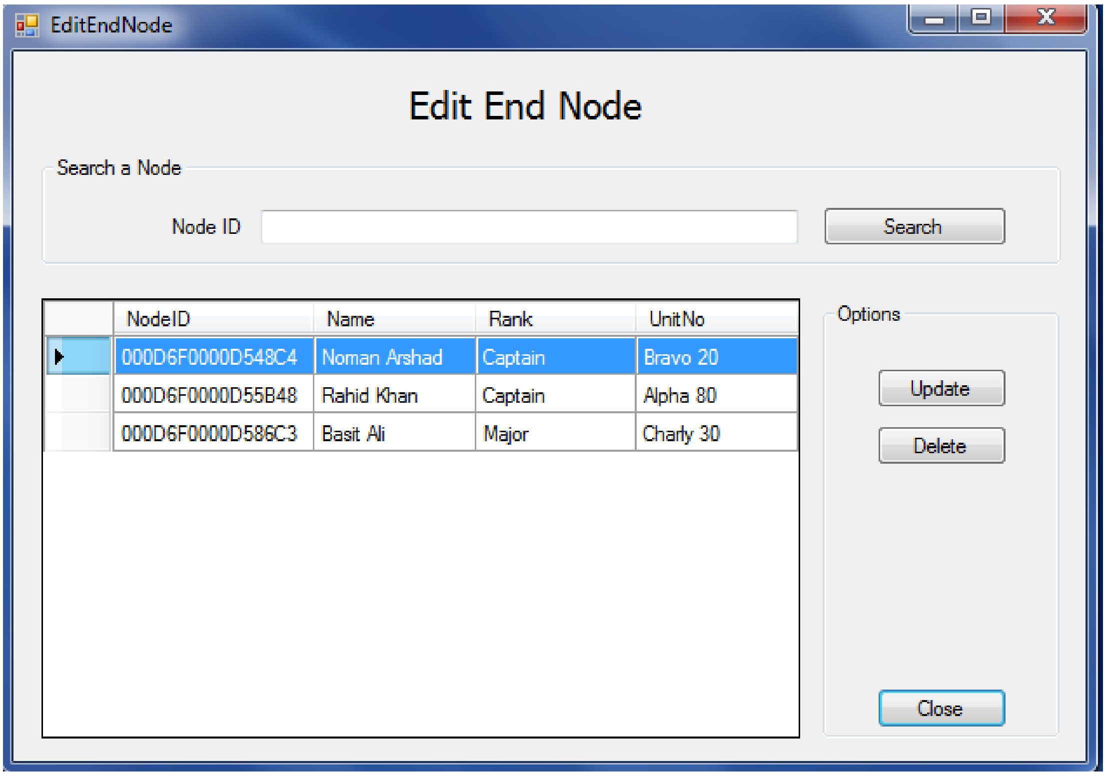

Figure 7.2 Edit End node

7.2.4 Network management

Here network is managed in order to create a zigbee network. User has to enter port No on which sink node is inserted in to the computer. The COM port can be viewed from device management of my Computer.

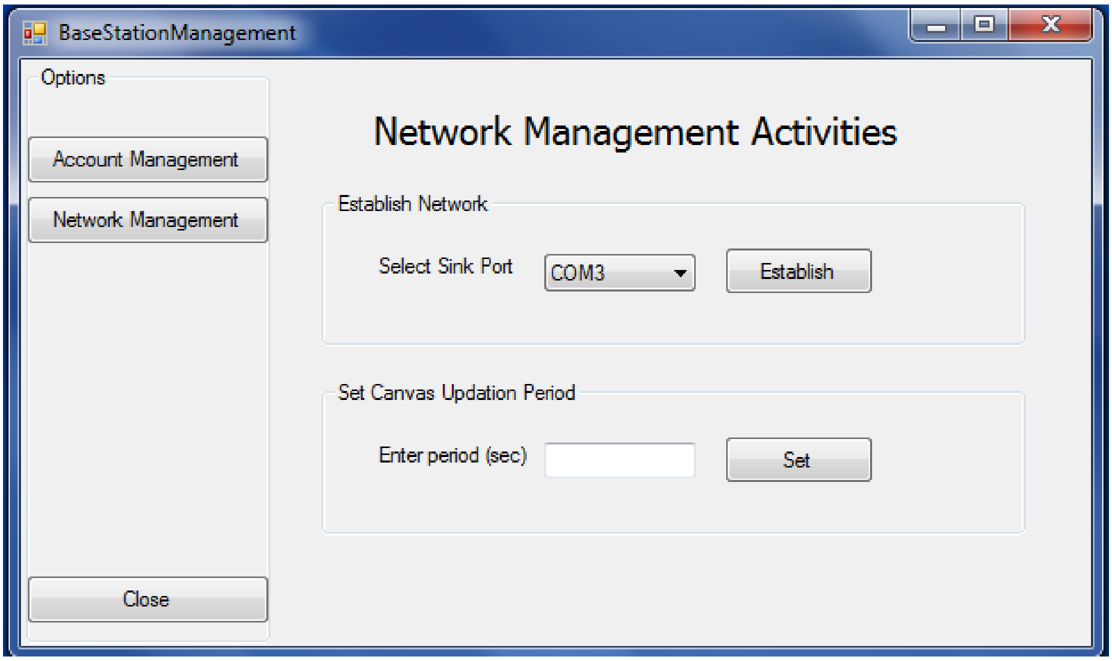

Figure7.3 Network management activities

7.3 Summary

The HITOC is an important system providing two essential functionalities in a single unit i.e. identification and tracking. An application has been developed to assist in monitoring i.e. HITOC, which responds to location data transmitted by zigbee devices. The wireless sensor network used to monitor the environment is cost effective as it uses low cost and low power hardware (telegesis ETRX3). In order to increase the coverage area of the network, a multi-hop routing protocol was implemented on these devices.

8 Chapter

Conclusion and Future Work

8.1 Introduction

This chapter describes the future scope of the project and the overall conclusion of the project. The project can be extended and few ideas are given in the chapter for the up gradation of the concept.

8.2 Future work

Following extensions would be quite helpful in extending usability of the system and make it more acceptable. These extensions would give Base Station personals very useful and viable information about personals in the operational environment.

Environmental Variables Extension

Environmental variables like temperature of personals and logistics to which a device is assigned can be reported using temperature sensors with the ZIgBee devices. Temperature sensors are inexpensive devices available to report temperature; their output can be relayed through the ZigBee to the Base Station.

Pulse Rate Sensor Extension

Pulse rate sensors can be attached to the ZigBee device to transmit pulse rate of personal who carries the device. Pulse rate sensors are a bit expensive but useful to know current health status of your personals.

Bi Directional Warning Signals

Bi directional warning signals would be vital incase of war scenarios, Base Station would be able to send warning signals to the ZigBee device holder and vice versa. On a ZigBee device warnings can be indicated through LED Flashes or buzzers.

Android Extension

Android application was initially a part of system but was scrubbed due to lack of time, however in future this smart phone application can be implemented to provide more flexibility in operational support.

8.3 Summary and Conclusion

This chapter documents the conclusions drawn after the completion of the HITOC. A section has also been dedicated to some of the future plans.

Identification and tracking are critical in all aspects of todays world, irrespective of whether human lives are involved or not. Even though stakes are higher if human life is at risk. Whatever the case compromise is not an option. In order to ensure management easily deployable and easy to afford solutions are required. HITOC Project is just one of those solutions. What makes this solution an effective one is that it is easily deployable with low cost. It can be used as basic tool for the identification and tracking of personals in operational areas i.e. warzone or disaster areas. The developed solution has been rigorously tested and the end results are satisfactory.

References

1. R. D. Team, “RPL: Routing Protocol for Low Power and Lossy Networks,” IETF ROLL WG, IETF Internet-Draft, 4 February 2009,draft-ietf-roll-rpl-00

2. Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das. "Ad Hoc On Demand Distance Vector (AODV) Routing." IETF RFC 3561

3. David B. Johnson, David A. Maltz, and Josh Broch. DSR: The Dynamic

   Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. in Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001

4. Telegesis ETRX-3 User manuals and data Sheets

5. http://www.adrc.asia/countryreport/NPL/NPLeng98/index.html

6. http://www.springerlink.com/content/vvp563ewkptnay6p/

Glossary

ETRX3- The ETRX3 series is the 3rd generation of advanced Zigbee modules from Telegesis

PA/LNA- Power Amplifier/Low Noise Amplifier

EM-357- Zigbee Module

ETRX2- Earlier Model of ETRX3

Hirose U.FL- Miniature coaxial RF connector for high-frequency signals up to 6 GHz manufactured by Hirose Electric Group in Japan.

RF- Radio Frequency

LRS- Long Range Surveillance

JTAG- Joint Test Action Group

AT Commands- Hayes Commands

APPENDIX

HITOC

USER’S MANUAL

WELCOME

Thank you for using the Handy Tool for identification and tracking on operational canvas.

This user’s manual is designed to be a reference for the operation of the HITOC.

Here you can find detailed operation information related to the HITOC.

Overview and Environment

The following sections give a brief overview of the HITOC and the minimum requirements needed to run the software

Overview

It is software that comes with hardware required for the Objectives of HITOC are

a. For army surveillance task our project application will assist them in tracking their peers (Soldiers, agents, informers).

b. For military ground operations task forces, this application is going to enable them to maintain contacts with their hosts and headquarters.

c. For military ground operations task forces as well as intelligence agencies, this application is going to enable single watch point of the complete operational view. For example it can be a base station where system is deployed showing the map of the complete zone.

d. For varied variety of users our application intends flexibility to view the entire zonal operation and its participant's location on SMART devices like PDA's. These palm top devices will access the map from Base Station via internet connection (GPRS, Edge). However in the absence of such smart application managing and tracking such critical operations is very tricky affair which is also prone to a large variety of risks leading to failure.

As nature of the system depicts that it is most suitable for the defense forces (Army, SSG, Police) in the war zones or it may also be used by the special agencies working in different catastrophes or disaster places.

Environment

OS: Windows XP /Vista/7.

CPU: 1 GHz or higher.

Memory: 1GB or higher for XP OS.

Displayer: 1024*768 or higher.

Other Software Requirements

TelegesisUSB_Driver(6.1)

Duly provided in package or can be downloaded from

www.telegesis.com

.NET Framework 4.0

Microsoft SQL Server 2008

Installations

The software can be executed directly by copying the concerned files onto the Base Station Server machine, no further installations are required.

.How to Use Software

This section describes the various features offered by the software and how to use these.

Login

The figure 3-1 shows the login screen where administrator can enter his assigned username and password to access further functionality of HITOC.

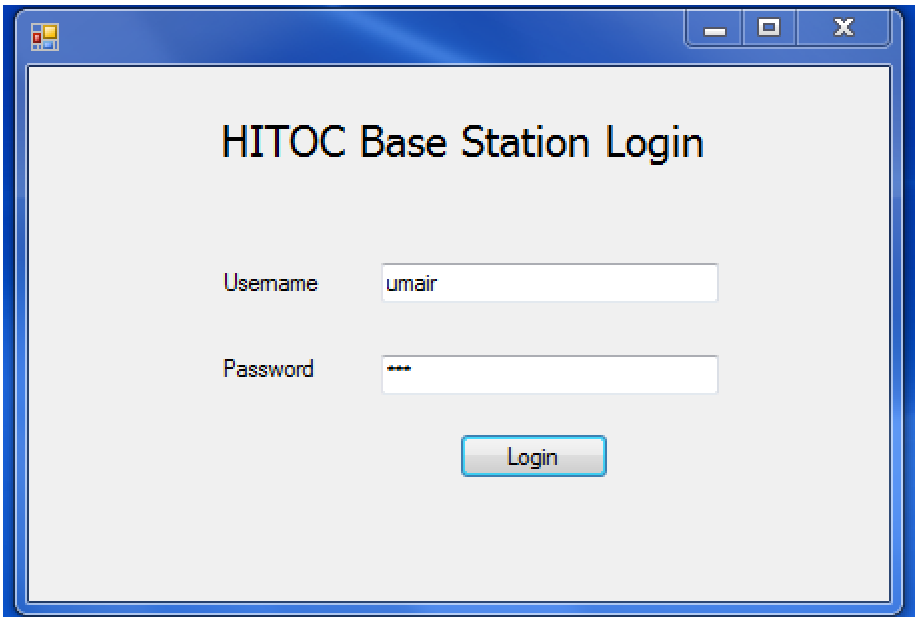

Figure 5 – 1 login

Account Management Activities

This screen allow you to create or edit clusterhead/end node and mobile user account.

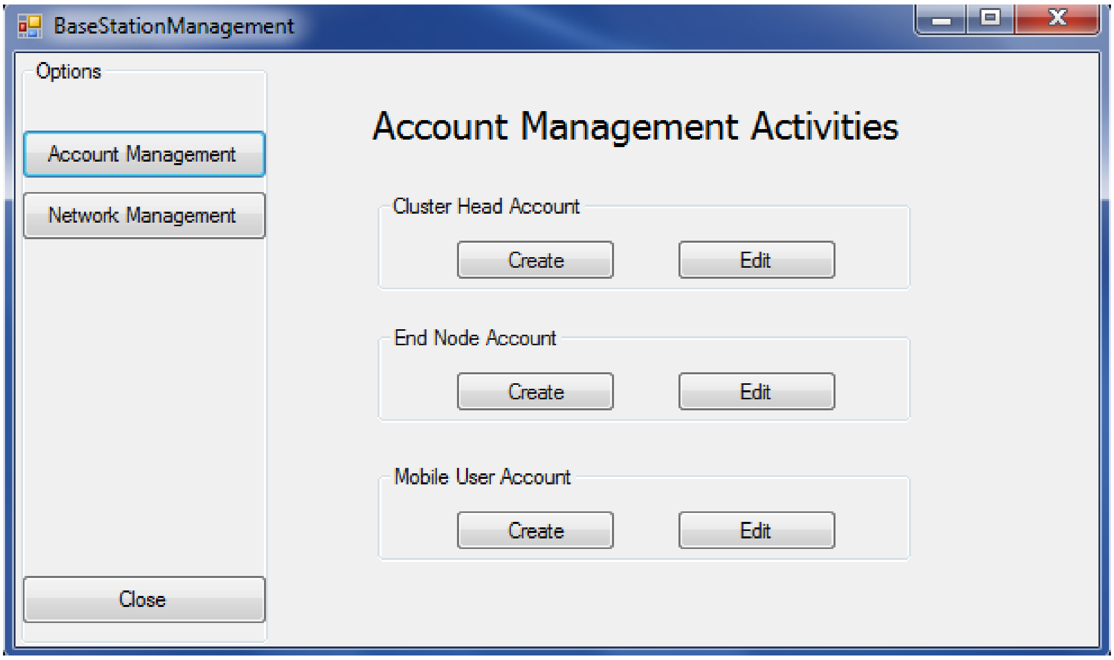

Figure 5 – 2 Account management activities

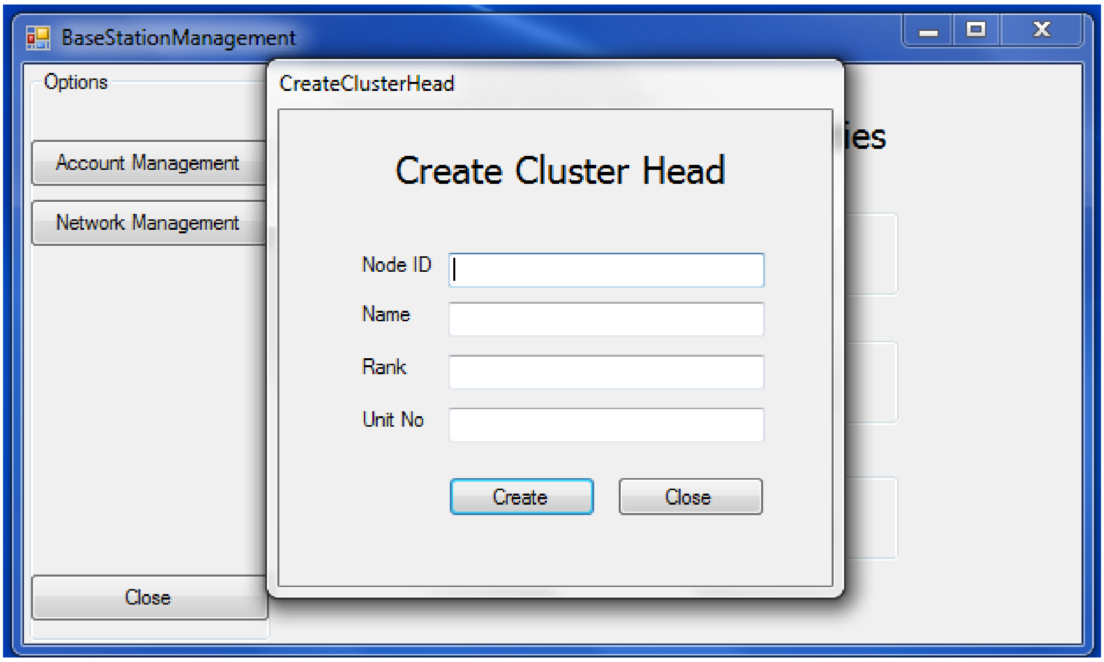

Figure 5 – 3 create cluster head

Node Id

This is the ID of zigbee device.

Name/Rank/Unit

This is the information of the personal to whom that device is being assigned.

Edit cluster Head

Here administrator can edit the information on cluster head when required i.e. if cluster head is assigned to a new personal or we change the zigbee device.

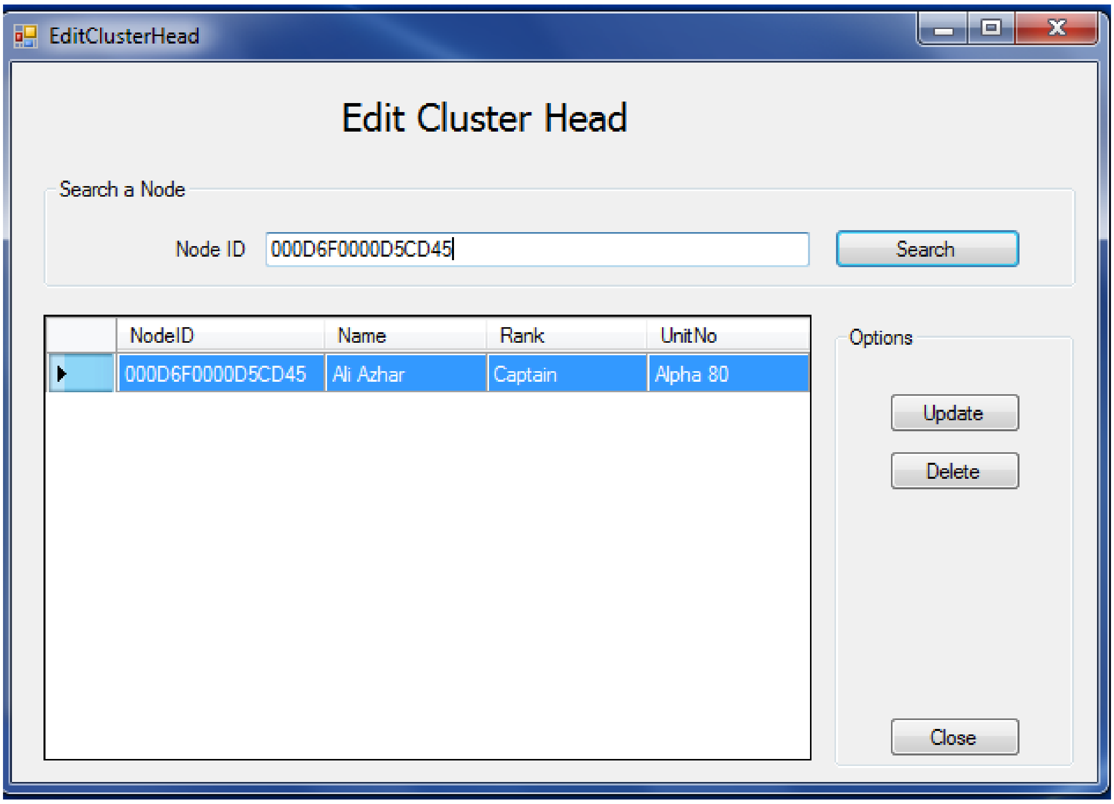

Figure 5 – 4 edit cluster head

Create End Node

End node creation is done here. Node ID, Name, Rank and unit information is needed

.

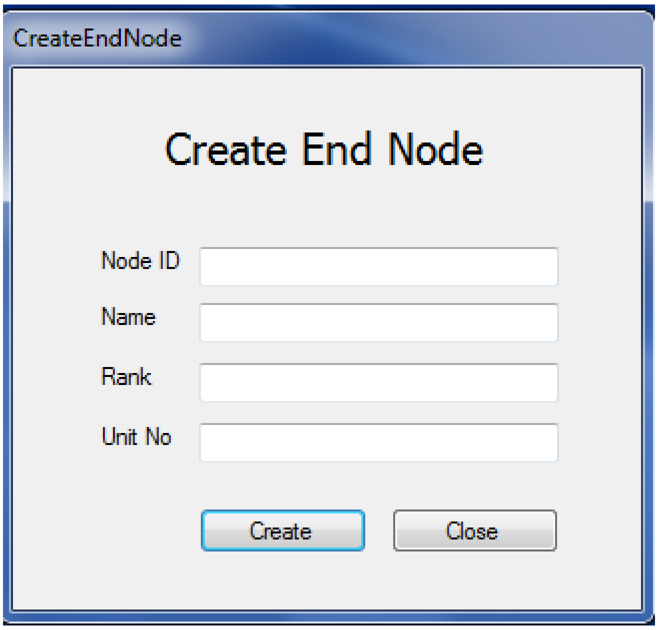

Figure 5– 5 Create End Node

Edit End Node

Here administrator can edit the information on end Node when required i.e. if end Node is assigned to a new personal or we change the zigbee device.

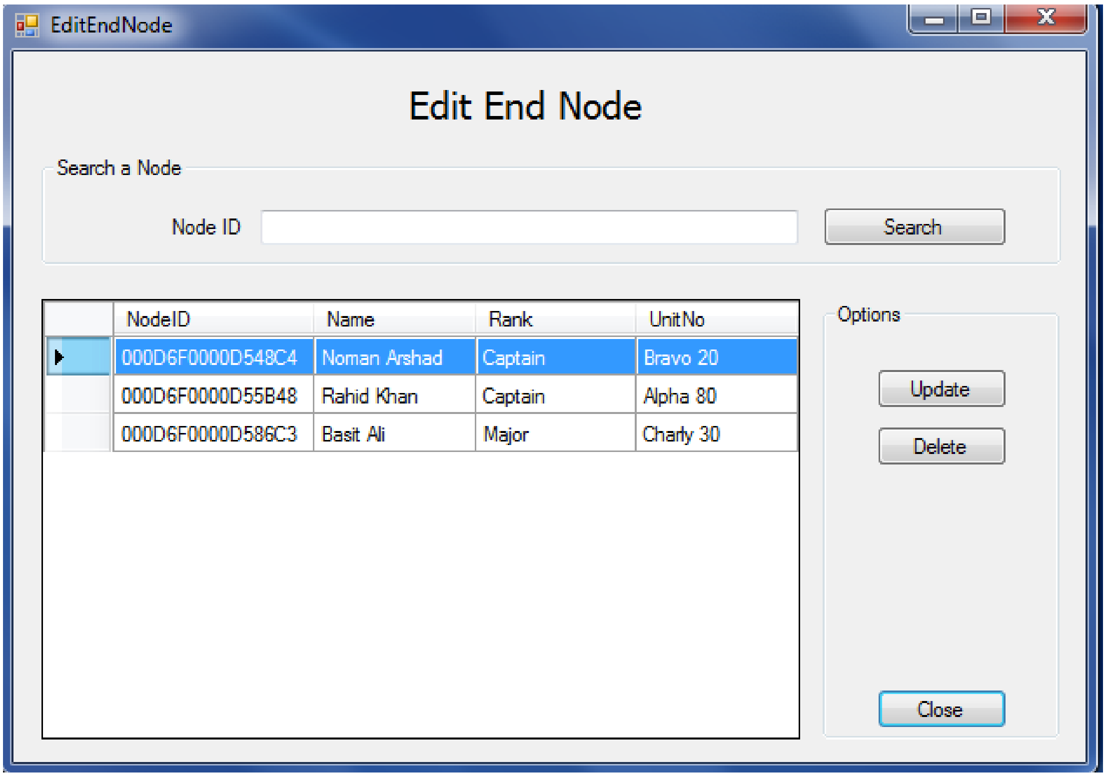

Figure 5– 6 Edit End Node

Network Management Activities

Here com port is defined where sink node is attached also the updation period of canvas is set.

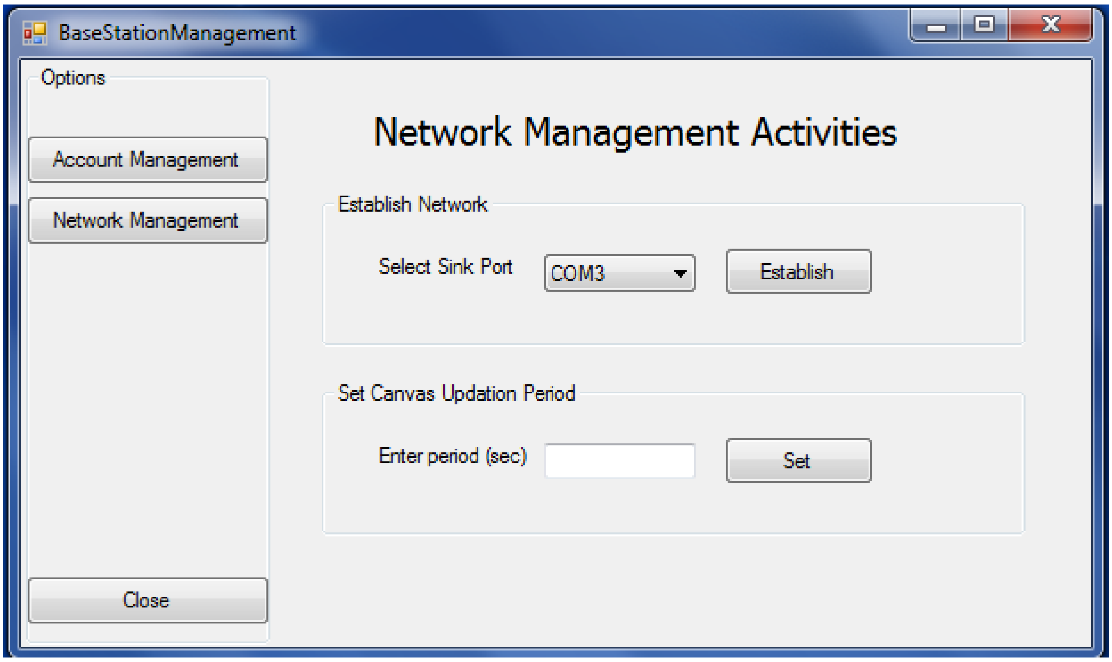

Figure 5 – 7 network managent activities

Operational Canvas

Operational Canvas is shown on successful operations. The personals are shown as markers on the map. marker can be clicked to see that personal information.

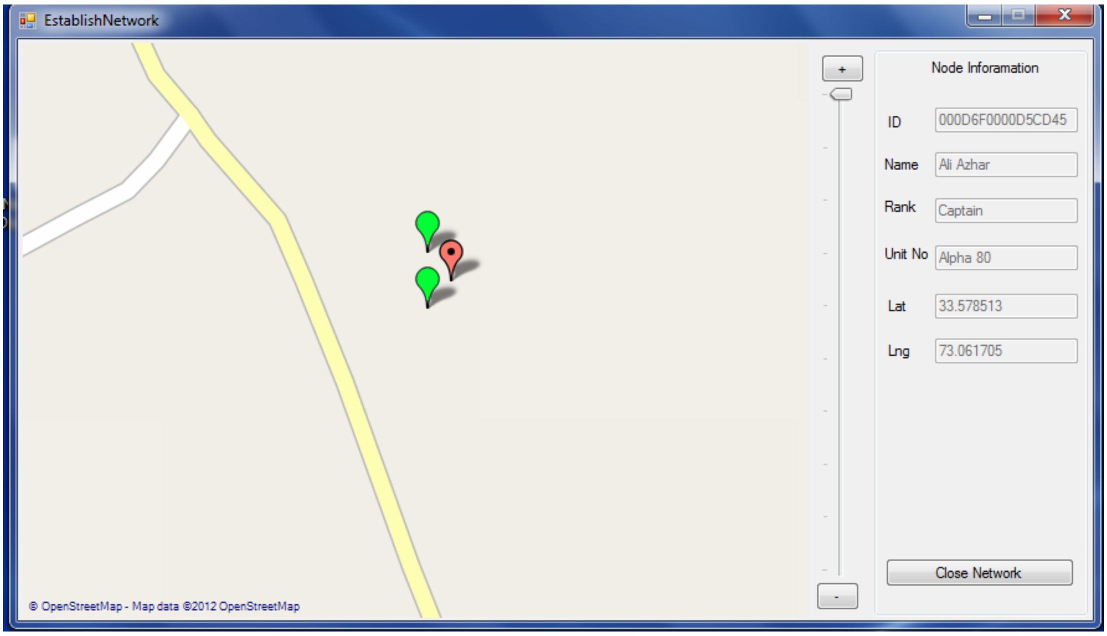

Figure 5-8 Operational Canvas