PERFORMANCE OF BLUETOOTH TECHNOLOGIES AND THEIR APPLICATIONS TO LOCATION SENSING

BY

Abhishek Pramod Patil

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

Department of Electrical and Computer Engineering

2002

ABSTRACT

PERFORMANCE OF BLUETOOTH TECHNOLOGIES AND THEIR APPLICATIONS TO LOCATION SENSING

BY

Abhishek Pramod Patil

Location-aware computing is regarded as a key feature of many future mobile applications, especially with the convergence of wireless technologies and mobile systems. GPS serves well for most outdoor applications, but it cannot be used in indoor location sensing. Several approaches have been proposed for indoor location sensing; such as infrared sensing, radio frequency, ultrasonic, and scene capture analysis. Each of these methods has their own disadvantages. Some are expensive to implement, while others are not very accurate. This thesis examines some of the recent commodity wireless technologies, especially Bluetooth, to find alternatives and strategies for indoor location sensing. Note that both Bluetooth and WLAN are not designed for indoor location sensing. Bluetooth devices are able to set up wireless ad-hoc connections in order to exchange all kinds of information in nearly every situation. Besides being small and low on power consumption, Bluetooth devices would soon become a day-to-day commodity making them cheap and omnipresent in office-like environments. The thesis concludes by proposing a model consisting of Bluetooth and other wireless technologies for location sensing in office environments, shopping malls and day care centers.

to my parents

ACKNOWLEDGMENTS

First and foremost, I would like to deeply thank my thesis advisor Dr. Lionel Ni for his continual guidance and support during this work. I would like to thank my parents and my brother for their unconditional love and encouragement. I am also grateful to the members of the ELANS lab especially Pei, Bernie, Yiu, Smitha and Yunhao for exchanging ideas and helping me throughout. And finally, thanks to all my friends who have assisted me with this work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES[1]

[1] Images in this thesis are presented in color.

1 Introduction

The location of people and objects relative to their environment is a crucial piece of information. Indoor location sensing is beginning to find many applications other than asset tracking and security. The more traditional applications might be as simple as tracking the location of a valuable shipping carton or detecting the theft of a laptop computer, or as complex as helping someone to find his or her way around an unfamiliar building. Some of the more recent additions to this set of applications would include shopping malls customizing advertisements so that they address a person watching them or standing next to them. Lets say for example imagine you are in a shopping mall and an advertisement screen calls you by your name and tells you about a new brand of some item on sale or about a discount offer on a particular item that you regularly purchase. Hospitals and day care centers can use indoor location sensing to locate the nearest doctor in case of an emergency. Offices can implement telephone redirection depending on where a person is located so that they don't miss any important calls.

1.1 **Research Motivation**:

Current technologies, such as GPS or differential GPS, can help locate people or objects as long as they are outdoors, where the signals from the 24 orbiting GPS satellites may be received. However, there is a latent demand for a similar system that works indoors, where the physics of radio propagation rules out the reception of GPS's weak microwave signals. The concept of indoor location sensing has been around for quite a while. Although there have been some prior researches in recent years exploring techniques for location sensing inside buildings, many questions remain before a viable in-door location-sensing system is available.

Some of the older technologies use costlier equipment. In other case, they are difficult to install or require a person to carry or wear a device that is part of the sensory network. In case of RFID technology for example, the cost of two readers is about $3000. The system also requires the user to carry an RF tag along with him so that the readers can sense his/her presence. In order to find a solution to this problem, we examined different commodity wireless technologies (like WLAN and Bluetooth) that are ubiquitous in an office-like environment so that we can make use of an existing infrastructure. As we would see in the later part of this thesis, Bluetooth turns out to be a good replacement to the existing indoor location sensing technologies although it is not designed for indoor location sensing.

1.2 **Thesis Organization**:

The Related Works chapter of this report talks about some previous work done in the area of indoor location sensing. The chapter on RFID gives a detailed description about a system, called LANDMARC, being implemented at the ELANS lab by the SWIM team. This project implements indoor location sensing with the use of RFID. Although LANDMAC makes use of the old RFID approach, the concepts and the methodology developed in this project can be used for many other location sensing techniques irrespective of the technology used and hence it is discussed here.

The chapter following LANDMARC gives a brief idea about the recent developments in the wireless world. This part of the report covers Bluetooth in more detail and explains how Bluetooth devices detect the presence of another device in its vicinity and form a network on the fly. The section following Wireless Technologies gives a brief description of the equipment used for carrying out the various performance measurements and interference experiments. The chapter following it gives details about the experiments carried out to study the performance of different wireless technologies and how they interfere with each other.

The experimental results clearly show that Bluetooth is more resistant to interference than other wireless technologies of today. Bluetooth technology is getting popular and cheaper and almost all the handheld devices and cellular phones now come with a Bluetooth version. Bluetooth ASIC chips are under production and once mass-produced, would bring the cost down to $5 or less. Besides this, Bluetooth devices can detect each other and form an ad-hoc network without the user's intervention. All these factors make Bluetooth a good replacement to the existing indoor location sensing technologies.

The chapter on location sensing presents several models and configurations with Bluetooth as a replacement to the earlier technologies used for indoor location sensing. The model consists of Bluetooth as the core sensors and an 802.11a network for communication with the location server and the Bluetooth access point. The last chapter outlines a few promising directions for future work.

2 Related Work

Over the years, many different researchers and research groups have looked into the area of indoor location sensing. AT&T Olivetti Research Laboratory's Active Badge is the pioneering work on this area based on infrared technology [1]. However, due to the line-of-sight requirement and short-range signal transmission, researchers realized infrared technology is not a very good solution for this problem. In recent years, most of the researches have been adopting the radio frequency (RF) technology for this purpose instead. Examples are RADAR project by Microsoft Research [2], SpotON done at University of Washington [3]. Like the RADAR project, Project Aura done at Carnegie Mellon University also tries to utilize the IEEE 802.11 wireless technology for location sensing in addition to its use as a network infrastructure [4]. Other projects also include Active Bats system by AT&T Research Laboratory using ultrasonic technology [5], the Cricket Indoor Location System at MIT with a combination of ultrasonic and RF technologies [6], TinyOS RF motes by UC Berkeley [7], and the Cooltown project by Hewlett Packard [8].

2.1 **RADAR**:

RADAR [2] is a radio-frequency (RF) based system for locating and tracking users inside buildings. RADAR operates by recording and processing signal strength information at multiple base stations positioned to provide overlapping coverage in the area of interest. It combines empirical measurements with signal propagation modeling to determine user location and thereby enable location aware services and applications. We present experimental results that demonstrate the ability of RADAR to estimate user location with a high degree of accuracy.

The main advantage of the RADAR system is its simplicity and ease of setting it up. Since the system leverages on the signal strength and signal to noise ratio available from the WaveLAN network interface, it requires very few base stations and uses the same infrastructure that provides general wireless networking in the building. The difficulty is that the object being tracked must support a WaveLAN NIC, which may be impractical on small or power constrained devices. In addition, it is not trivial to generalize this approach to multi-floored buildings or three dimensions. Besides, signal behavior in an indoor environment is unpredictable and depends on various factors as we shall see in Section 5.6. In the system proposed in this thesis, the concept of reference tags is used which is a work around to solve the problem of randomness in signal characteristics in indoor environment. The RADAR system can position an object in a 3-4m circle with 50% probability, which is one major disadvantage of the system.

2.2 **Cricket**:

Cricket [6] uses a combination of RF and ultrasound technologies to provide a location-support service to users and applications. Wall and ceiling-mounted beacons are spread through the building, publishing information on an RF signal operating in the 418 MHz AM band. With each RF advertisement, the beacon transmits a concurrent ultrasonic pulse. Listeners attached to devices listen for RF signals, and upon receipt of the first few bits, listen for the corresponding ultrasonic pulse. When this pulse arrives, they obtain a distance estimate for the corresponding beacon. The listeners run maximum-likelihood estimators to correlate RF and ultrasound samples (the latter are simple pulses with no data encoded on them) to pick the best one.

The main advantage of the Cricket system is its accuracy – 30cm. It scales well as the number of devices increases. Its decentralized architecture makes it easy to deploy. However, the infrastructure involves installing and coordinating a lot of devices. The system makes use of ultrasonic devices, which are expensive and difficult to handle. The ultrasonic devices need to be synchronized so that their beacons don't interfere. This requires additional RF infrastructure further increasing the cost.

2.3 **SpotON**:

SpotON [3] is a new tagging technology for three dimensional location sensing based on radio signal strength analysis. SpotON researchers have designed and built hardware that will serve as object location tags, part of a project called SpotON. SpotON tags use received radio signal strength information (RSSI) as a sensor measurement for estimating inter-tag distance. Using many collocated nodes, the measured positional accuracy can be improved through algorithmic techniques and erroneous distance measurements caused by signal attenuation (e.g., by metal objects in the area) can be automatically factored out.

The main contribution of this paper was to come with a design and analysis of hardware meant for location sensing only. Another good thing about SpotON project is that it aims to gather real-world information not available using simulation techniques. However, using algorithmic techniques to remove errors dues to signal variation may not be the best solution. As mentioned in Section 5.6 signal variation in indoor environment is random and depends on several factors. With the concept of reference tag, the system proposed in this thesis, tried to overcome the problem of dynamic random variation in signal strength in indoor environment.

2.4 TinyOS:

TinyOS [7] RF motes are small networked sensors with a 4 MHz Atmel processor and a 916.50 MHz RF wireless transceiver. This project, examines location sensing and systems issues for a location-sensing infrastructure. It also presents a thorough empirical analysis of the networking capabilities of the TinyOS RF motes. The study consisted of capturing more than 15,000 sensor readings and analyzing how signal strength, packet loss, and byte corruption were affected by factors including pair-wise distance and environment. This analysis is used to build a model of the RF signal strength.

2.5 Aura:

The Aura [4] project makes use of the wireless network infrastructure at Carnegie Mellon University for determining a user's location both indoors and outdoors while on campus, and at a higher resolution than GPS. It employs a table-based lookup for triangulation of a user's location. The system makes use of existing wireless infrastructure, which is a major advantage. However, as mentioned earlier, signal strength in indoor environment varies randomly and cannot be used for distance calculation. Signal propagation in indoor environment depends on factors like movement of people, placement of cubicle partitions, furniture, etc.

3 Location-Sensing using RFID

LANDMARC [9] (Location Identification based on Dynamic Active RFID Calibration) is one of the projects undertaken by the SWIM (Sensory and WIreless Mobile) team at ELANS (Experimental laboratory of Advanced Networks and Systems in the Department of Computer Science and Engineering at Michigan State University). In this project, we try to develop and experiment with a prototype indoor location-aware system using RF devices. Variation in RF signal strength reception due to the dynamic environment and the device itself makes location sensing a more difficult task. In LANDMARC, we maintain up-to-date references by using plenty of inexpensive tags instead of having additional costly RF readers. This section of the report tries to give a brief description of the LANDMARC system.

3.1 What is RFID?

A basic Radio Frequency Identification (RFID) [10] system consist of three components – The antenna or a coil, a transceiver with decoder and an RF tag electronically programmed with unique information.

The antenna system emits radio signals to activate the tag and read and write data to it. Antennas are the link between the tag and the transceiver, which controls the system's data acquisition and communication. The electromagnetic field produced by an antenna can be constantly present when multiple tags are expected continually. If constant interrogation is not required, a sensor device can activate the field.

Often the antenna is packaged with the transceiver and decoder to become a reader, which can be configured either as a handheld or a fixed-mount device. The reader emits radio waves in ranges of anywhere from an inch to about 100 feet or more, depending upon its power output and the radio frequency used. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit and the data is passed to the location-sensing computer for processing.

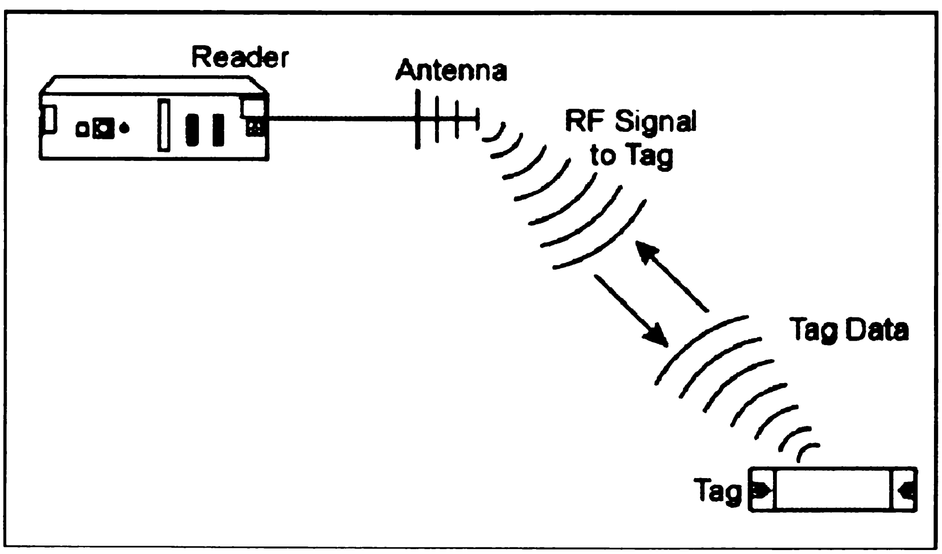


Figure 3.1: Active tag System.

RFID tags come in a wide variety of shapes and sizes depending on the application. RFID tags are categorized as either active or passive. An active RFID tags is powered by an internal battery and are typically read/write. An active tag's memory size varies according to application requirements. The battery-supplied power of an active tag generally gives it a longer read range. The trade off is greater size, greater cost, and a limited operational life.

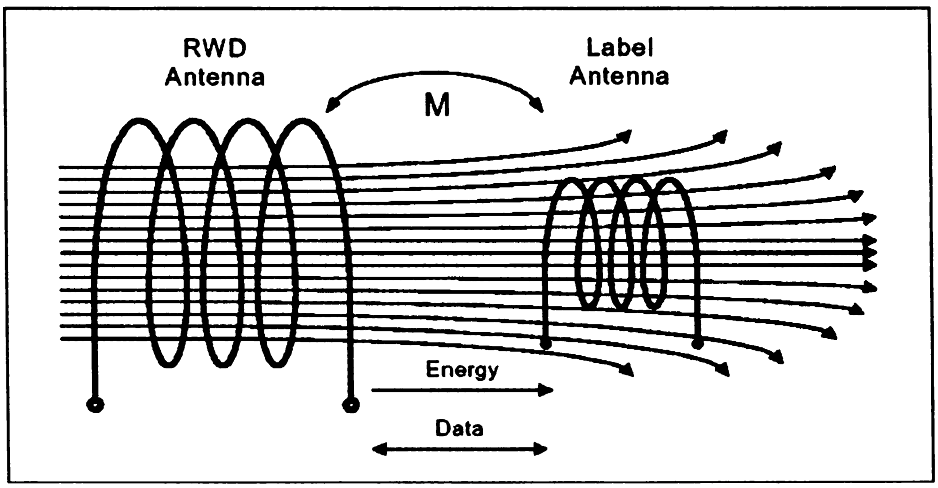


Figure 3.2: Basic Principle of inductive passive RFID system

Passive RFID tags operate without a separate external power source and obtain operating power generated from the reader. As a result, passive tags are much lighter than active tags, less expensive, and offer a virtually unlimited operational lifetime. The trade off is that they have shorter read ranges than active tags and require a higher-powered reader. Read-only tags are typically passive and are programmed with a unique set of data that cannot be modified. Read-only tags can be though as a replacement to barcodes.

Their frequency ranges also distinguish RFID systems. Low-frequency (30 KHz to 500 KHz) systems have short reading ranges and lower system costs. They are most commonly used in security access, asset tracking, and animal identification applications. High-frequency (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) systems, offering long read ranges (greater than 90 feet) and high reading speeds, are used for such applications as railroad car tracking and automated toll collection. However, the higher performance of high-frequency RFID systems incurs higher system costs.

3.1.1 Advantage of using RFID

The significant advantage of all types of RFID systems is the no contact, non-line-of-sight nature of the technology. Tags can be read through a variety of substances such as snow, fog, ice, paint, crusted grime, and other visually and environmentally challenging conditions, where barcodes or other optically read technologies would be useless. RFID tags can also be read in challenging circumstances at remarkable speeds, in some cases responding in less than 100 milliseconds. The read/write capability of an active RFID system is also a significant advantage in interactive applications such as work-in-process or maintenance tracking. Though it is a costlier technology (compared with barcode), RFID has become indispensable for a wide range of automated data collection and identification applications that would not be possible otherwise.

3.2 Infrastructure

The LANDMARC system consists of two physical components, the RF readers and RF tags (Figure 3.3). The reader decides the tag's location based on the Received Signal

Strength (RSS) from the tag. As the reader only reports whether a tag is in its detection range, the system is also said to be a proximity location sensing system. Following we describe some of the physical properties of both the readers and the tags.

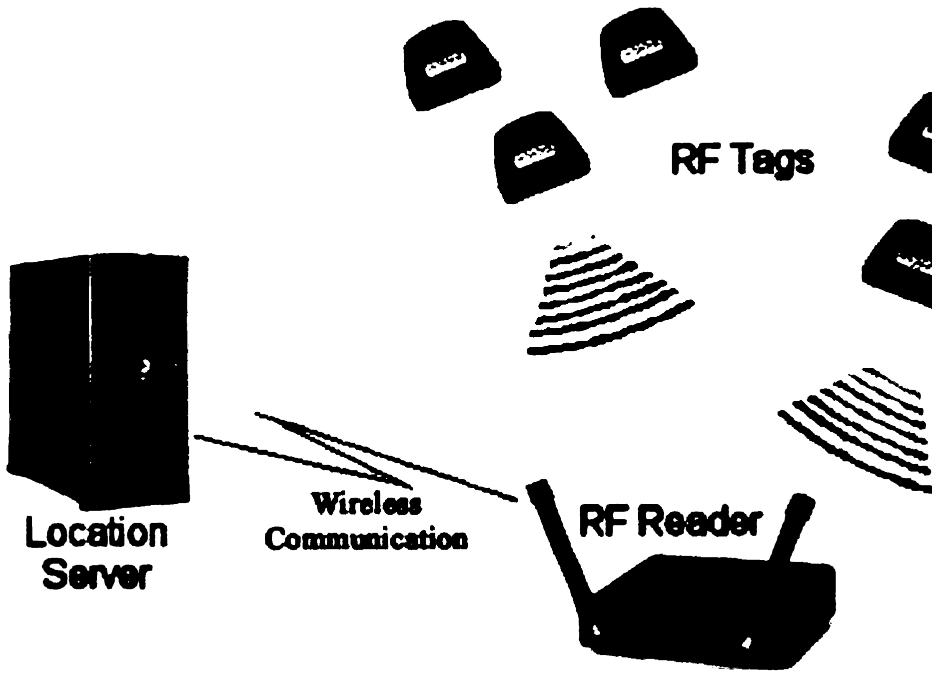


Figure 3.3: RFID location sensing infrastructure[11].

RF Reader

Operating frequency: 308 MHz

Reporting interface: Ethernet or IEEE 802.11b wireless network

Detection range: 150 feet (can be increased to 1000 feet with special antenna)

Online range control: provide digital control of readers' read range via providing configuration software and·API (8 incremental read ranges)

Simultaneous identification (collision avoidance): can detect up to 500 tags in 7 seconds

RF Tag

Unique ID: each tag is pre-programmed with a unique 7-character ID for identification by reader

Battery life: 3-5 years

Transmission rate: every 7 seconds

3.2.1 Dataflow

After the signal received at the RF readers, the readers then report the information to "TagTracker Concentrator LI" (a software program/API provided by RF Code, Inc.) via wired or wireless network, which can handle up to 10 readers. Moreover, the software also acts as a central configuration interface for the RF readers. For example, it can be used to adjust the detection range and rate of the readers. After the information from the readers is processed by the TagTracker Concentrator LI, the processed location information can be buffered locally as file on the same machine or transmitted via network socket (configurable in the API). Figure 3.4 shows the dataflow in the RFID prototype system.

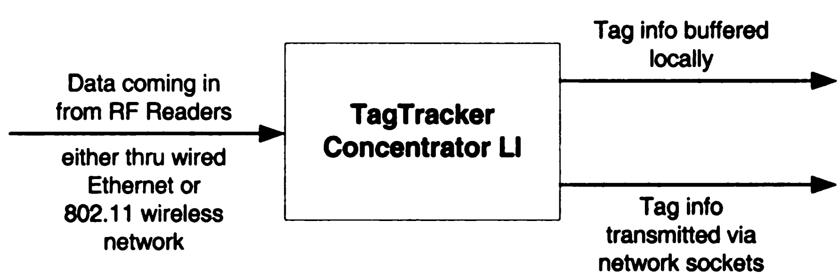


Figure 3.4: Dataflow in RFID prototype system

3.3 Prototype Setup Procedures

In brief, the prototype environment consists of a sensing network that helps the location tracking of mobile users/objects within certain granularity and accuracy, and a wireless network that enables the communication between mobile devices and the resources-rich Internet/Intranet. Figure 3.5 shows the overall system infrastructure.

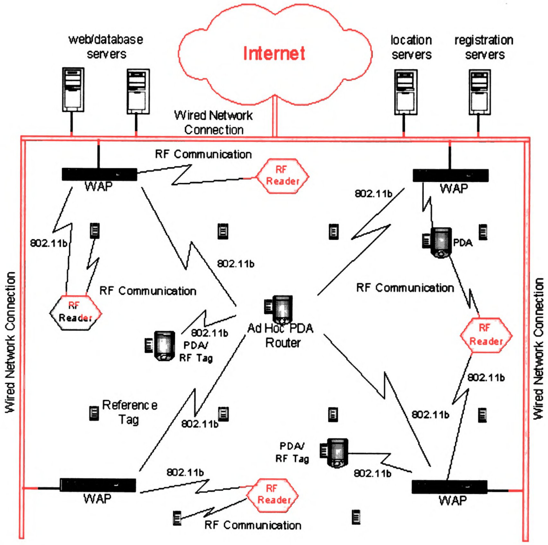


Figure 3.5: Overall system infrastructure[9].

3.3.1 Location Sensing Networks

An Indoor Location sensing environment consists of two networks:

- Sensory Network – to locate a mobile user or an object within a certain accuracy or granularity
- Wireless Network – all the mobile devices to communicate amongst themselves and the resource rich internet/intranet.

The sensing network primarily includes the RF readers and RF Tags. The RF Reader has a range of up to 150 feet (which can be extended to 1000 feet with a special antenna) and can identify 500 tags in 7.5 seconds with the collision avoidance. With the API supplied that communicates with the readers, the system can report tag in a range from 8 different ranges that is a function of distance from the reader. As an active tag system, the RF tag emits signal, which consists of a unique 7-character ID, every 7.5 seconds for identification by the readers. The tag is powered by a button-cell battery and claimed to have a 2-5 years battery life and it operates at the frequency of 303.8 MHz that doesn't require the FCC licensing.

The other major part of the infrastructure is the wireless network that allows communication between mobile devices like PDAs and the Internet. In addition, it also acts as a bridge between the sensing network and the other part of the system. As the reader is equipped with the capability of communicating wirelessly using IEEE 802.11b wireless network, all the tag information gathered on readers is sent over to the supplied API sitting on a specific server (the location server). This feature doesn't have the trouble of having a wire-connection to the readers, thus reducing the possible restrictions of where the readers could be placed. And the wireless network will serve as the fundamental framework of all the communication in the infrastructure.

3.3.2 Concept of Reference Ids

In section 5.6, we shall see that signal variation in an indoor environment is random and depends on many factors. Movement of people, placement of cubicle partition, furniture etc, contribute to this randomness.

To offset these environmental changes, we use the concept of reference IDs where, we uniformly distribute RF-tags over the area of interest. In contrast to having more readers in place to increase the accuracy, the LANDMARC system employs the idea of having extra tags instead to help the location calibration. These tags serve as reference points in the system (like landmark in our daily life). By placing these reference tags at fixed location, the system will always contain the most up-to-date reference. Therefore, each time when we want to track down an object with the tag, we can compare the detected range of that tag to those of the reference tags to make the decision. This approach helps offset some of the environmental factors that contribute to the variations in detected range because now the reference tags are subjected to the same effect in the environment as the tags to be located and we can dynamically update the reference information for lookup based on the detected range from the reference tags in real-time.

Thus, a much more accurate and close to real-time location sensing can be achieved with this much more flexible and dynamic approach. Not to mention the lower cost by relying more on inexpensive tags than having additional costly readers, the LANDMARC system can also be easily adopted to different environments with no training phase required.

3.4 Experiment with LANDMARC

3.4.1 Methodology

With the same setup as the preliminary testing, we have 4 RF readers along with 32 tags setup in our lab. However, this time, we use half of the tags as reference tags while the other 16 as objects being tracked. Layout and positioning of the readers and tags is shown in Figure 3.6. The readers are all configured with continuous mode (continuously reporting the tags that are within the specified range) and a detection-rang of 1-8 (meaning the reader will scan from range 1 to 8 and keep repeating the cycle with a rate of 30 seconds per range).

With the setup, the data is collected via socket from the TagTracker Concentrator LI and are logged to provide further offline analysis. Offline processing is necessary instead of real-time so that we can apply different approaches to see how well it performs based on the same set of data. For this test, the data is collected over a period of 24 hours.

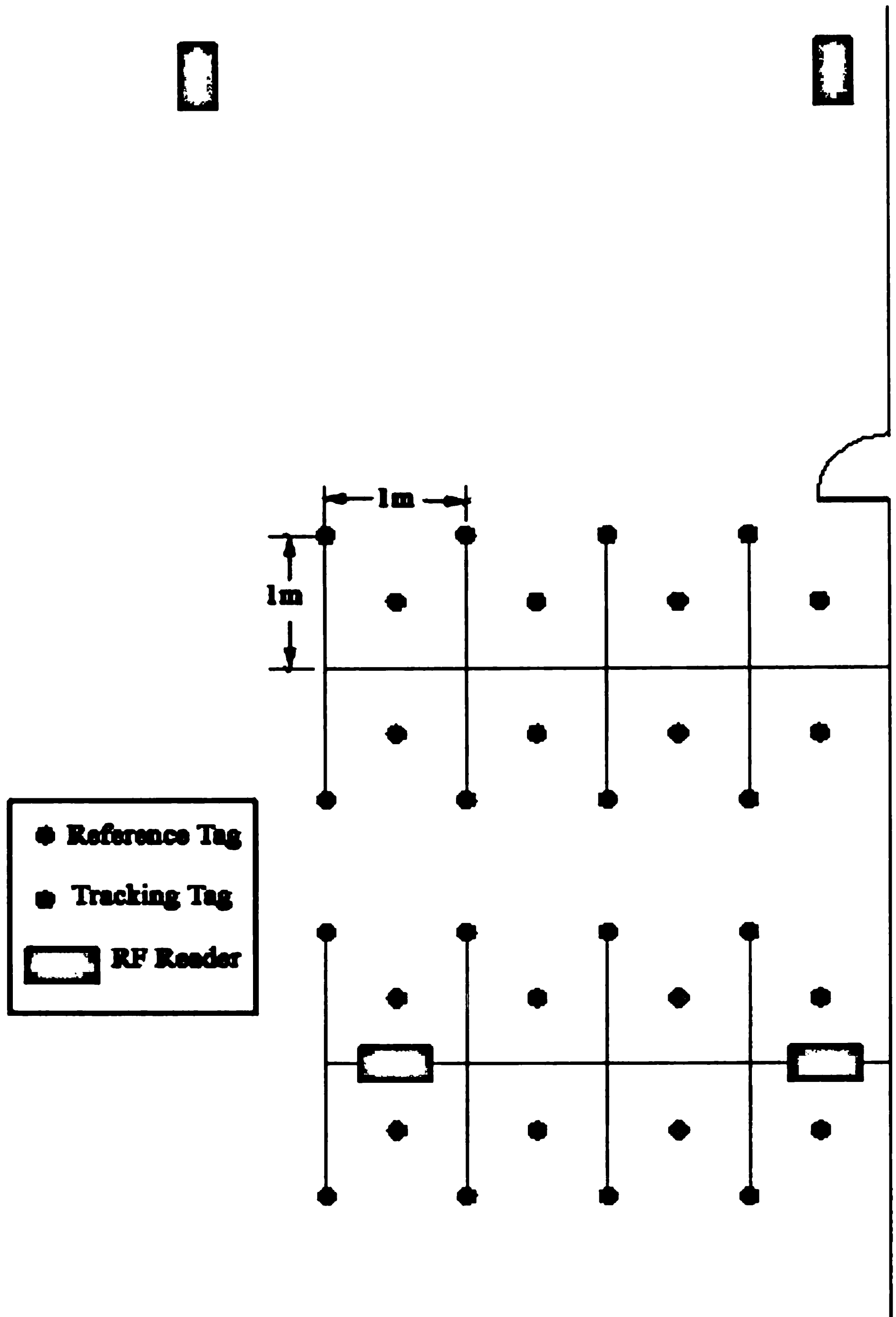


Figure 3.6: RF readers and tags layout for the experiment

As we will see in the later section, we can use a similar approach when we use Bluetooth devices in place of readers and the tags.

4 Wireless Technologies and Experimental Setup

This section gives a brief description about the recent developments in the wireless world. It starts by describing various 802.11x technologies and then proceeds on to Bluetooth, which is the main focus of this paper.

4.1 802.11x

In 1990, the IEEE 802 Executive Committee established the 802.11 Working Group to create a wireless local area network (WLAN) standard. The standard specified an operating frequency in the 2.4GHz ISM (Industrial, Scientific, and Medical) band. Seven years later, the group approved IEEE 802.11 as the world's first WLAN standard with data rates of 1 and 2 Mbps. Afterwards the committee began work on another 802.11 extension that could satisfy future needs. Within 24 months, the working group approved two higher rate physical layer extensions to 802.11. The two extensions were designed to work with the existing 802.11 MAC layer (Medium Access Control), with one being the IEEE 802.11a - 5.2GHz, and the other IEEE 802.11b - 2.4GHz. Recently 802.11g was announced, which operates at 2.4 GHz and uses OFDM.

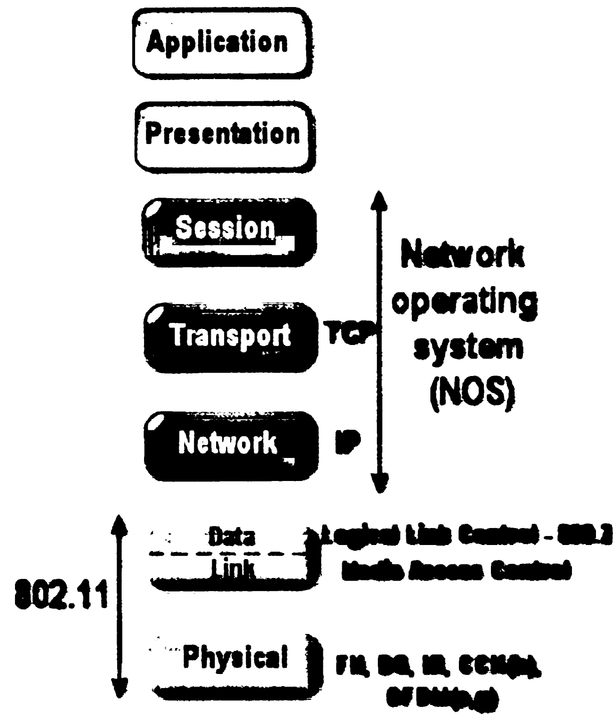


Figure 4.1: Protocol stack for 802.11x system[12].

4.2 802.11b

The 802.11b protocol operates in the unlicensed 2.4GHz ISM band, using DSSS (direct-sequence spread-spectrum) transmission. Data is transmitted on BPSK and QPSK constellations. Maximum data rate is about 11 Mbits/s with fallback rates of 5.5, 2 and 1 Mbits/s, depending on distance, noise and other factors. Range can be up to 100m, but this too is dependent on the environment. In a protocol view (Figure 4.1), 802.11b only modifies the bottom 2 layers of the 802 model, PHY & MAC, (OSI layers 1: Physical & 2:DataLink). Any LAN application, network operating system, or protocol, including TCP/IP and Novell NetWare, will run on an 802.11-compliant WLAN as easily as they run over Ethernet.

4.3 802.11a

The recently ratified 802.11a standard establishes a new unlicensed frequency band for wireless networking and increases throughput for networks to 54 Mbps. Much of the increase comes from use of the orthogonal frequency division multiplexing (OFDM) modulation technique. The standard uses the unlicensed national information infrastructure (UNII) frequency band. Wireless networking applications are just beginning to employ this band, which is split into three noncontiguous frequency segments.

UNII-1 is in the 5.2 GHz range.

UNII-2 is in the 5.7 GHz range.

UNII-3 is in the 5.8 GHz range.

A common misconception is that 802.11a came first. 802.11b does represent the second generation of wireless networking, but 802.11a actually represents a third generation. There are two major differences between 802.11a and 802.11b:

- The type of modulation. 802.11a uses orthogonal frequency division multiplexing (OFDM) to enable efficient use of available bandwidth.
- The carrier frequency. 802.11a uses the 5.2 GHz band, while 802.11b uses the 2.4 GHz band.

The following figure shows the fall-back rates for 802.11a & 802.11b with increase in distance.

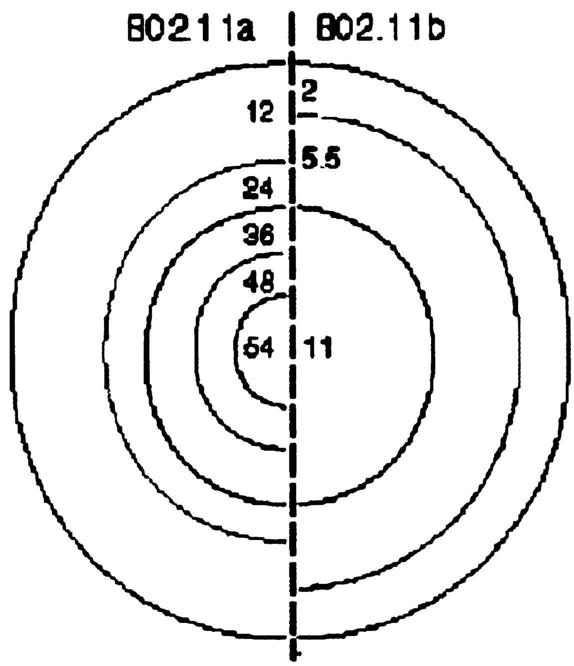


Figure 4.2: Fall-back data rates for 802.11a & 802.11b[2].

4.4 802.11e

The 802.11e committee is working to establish Ethernet quality of service (QoS) characteristics within 802.11 wireless LANs. Note that this effort applies to all 802.11 implementations (b, a, and g). The standard is expected to link the wired Ethernet QoS (802.1p) and the wireless world.

4.5 802.11g

The 802.11g standard, which has also been known as 802.11b-extended, seeks to increase the data throughput of the 2.4-GHz ISM frequency band. The standard has not yet been ratified, largely because of competing modulation techniques. Recently, members of the working group have agreed that the OFDM modulation technique will be required, but that packet binary convolution coding (PBCC) can be used as an alternative. This breaks

[2] All values are signaling rate in Mbps. (Not all data rates shown)

a significant technical holdup to ratification, but debate still rages regarding 802.11g's necessity now that 802.11a promises similar gains in a largely unused frequency band. 802.11g would provide initial throughput of 32 Mbps with the potential to grow to 54 Mbps and beyond.

4.6 802.11i

Originally focused on 802.11b systems, the 802.11i committee is developing new data security protocols for use in all 802.11 systems. The original standard included a wired equivalency protocol (WEP) with two key structures, 40 and 128 bits long.

4.7 802.11h

The 802.11h committee is developing a uniform standard for power usage and transmission power from 802.11 radios. The need for this committee is being driven by requirements for enhanced battery life and in-country EIRP compliance for travelers. Emphasis on this committee is just beginning; therefore, there is much to accomplish. The committee expects to ratify the standard by late-2002.

4.8 Bluetooth

The development of the Bluetooth industry standard started late in the winter of 1998 when Ericsson, IBM, Intel, Nokia, and Toshiba formed the Bluetooth Special Industry Group (SIG) to develop and promote a global solution for short range wireless communication operating in the unlicensed 2.4 GHz ISM band.

The Bluetooth wireless technology serves as a replacement of the interconnect cables between a variety of personal devices, including notebook computers, cellular phones, personal digital assistants (PDAs), digital cameras, etc. The Bluetooth wireless technology would function as the universal low cost, user friendly, air interface that will replace the plethora of proprietary cables that people need to carry and use to connect their personal devices. While personal devices typically communicate based on the RS-232 serial port protocol, proprietary connectors and pin arrangements make it impossible to use the same set of cables to interconnect devices from different manufactures, and sometimes even from the same manufacturer. The primary focus of the Bluetooth wireless technology is to provide a flexible cable connector with reconfigurable pin arrangements permitting several personal devices to interconnect with each other.

Bluetooth wireless technology offers to the personal connectivity space the benefits of omni-directionality and the elimination of the line of sight requirement of RF-based connectivity. The personal connectivity space resembles a communications bubble that follows people around and empowers them to connect their personal devices with other devices that enter the bubble. Connectivity in this bubble is spontaneous and ephemeral and can involve several devices of diverse computing capabilities, unlike wireless LAN solutions that are designed for communication between devices of sufficient computing power and battery capabilities.

4.8.1 Bluetooth properties

The main properties of the Bluetooth wireless communication technology are:

1. Low-cost, low power radio transceiver chip (0.5 square inches).
2. Price of Bluetooth module will be approx. $15-20 in the near future and the goal is to approach $5 or less.
3. A low nominal range of Bluetooth radio (10 meters) for saving battery power.
4. Extended range with external power amplifier (100 meters).
5. Operation in the globally available and unlicensed.

4.8.2 Technicalities:

A Bluetooth radio operates on the license-free 2.4 GHz ISM band and is compliant with FCC part 15 regulations for intentional radiators in this band. The Bluetooth radio transmission uses a packet switching protocol with FHSS (Frequency Hopping Spread Spectrum). The hop frequency is 1600 hops per second. The frequency spectrum is divided into 79 hops of 1 MHz bandwidth each. Thus, eventually, Bluetooth devices occupy 79MHz, but at any specific moment, only 1 MHz is occupied. Each of these hops goes to a slot that is 625us long, (packets can last 1,3 or 5 slots, but the hop frequency remains the same for each packet).

Frequency hopping is used to reduce interference and enhance security. The frequency-hopping scheme is combined with fast ARQ (Automatic Repeat Request), CRC (Cyclic Redundancy Check) and FEC (Forward Error Correction). A binary radio frequency modulation and simple link layer protocols reduce the complexity and the costs of the radio chip. Bluetooth provides a nominal data rate of 1 Mbit/s.

4.8.3 Bluetooth Networking

When several Bluetooth devices are in close vicinity of each other, they form a piconet. One piconet consists of 1 master and up to 7 slaves where the master-slave principle is used to initiate and control the traffic between devices in a piconet. The master is responsible for defining and synchronizing the frequency hop pattern in his piconet. All packets are exchanged between a master and its slaves within a piconet. There is no direct master-master or slave-slave communication. A device can be a slave in several piconets but be a master in only one piconet. Bluetooth piconets can coexist in time and space independently of each other. Furthermore, a single device may be a member of several piconets, a case referred to as scatternet in Bluetooth parlance.

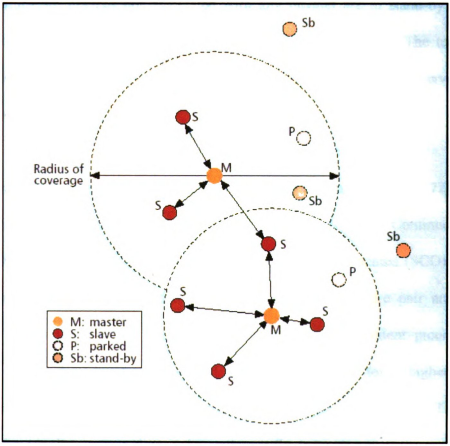


Figure 4.3: Bluetooth Piconet [13].

A piconet is formed in an ad hoc manner without any infrastructure assistance, and it lasts for as long as the creator of it needs and is available to communicate with other devices. The terms master and slave are relative to a particular existing piconet. To identify each slave, the master of a piconet assigns a locally unique active member address to the slaves participating in active communications in the piconet. The master regulates and controls who transmits and when. While up to seven slaves may be actively communicating in a piconet at one time, additional devices may be registered with the master and be invited to become active whenever necessary. These additional devices are called parked. A master can have up to 200 Bluetooth devices (in its vicinity) in parked mode. Bluetooth devices not associated with any piconet are in stand-by mode. Any Bluetooth device can perform the role of a master and/or a slave. The terms are not assigned to the radio units at manufacture time. A Bluetooth radio may serve either as a master or as slave at different times.

A single Bluetooth unit may send/receive at a maximum data rate of 721 kbit/s or a maximum of 3 voice channels (of 64 Kbit/s each with CVSD – Continuous Variable Slope Delta Modulation). Both a Synchronous Connection Oriented (SCO) link and an Asynchronous Connectionless (ACL) link for each master-slave pair are supported. Within the same Bluetooth radio range, separate and independent piconets may be formed. These may build up so-called scatternets to allow for a higher number of Bluetooth devices being active and/or for a higher aggregate bandwidth. The Bluetooth radios come in three power classes, depending on the transmit power:

- Class 1 radios transmit power of 20 dBm (100 mW).
- Class 2 radios transmit power of 4 dBm (2.5 mW).
- Class 3 radios transmit power of only 0 dBm (1 mW).

Due to the power and cost constraints of the various personal devices that use Bluetooth radios, class 3 and class 2 radios are expected to be the ones mostly used.

4.8.4 Bluetooth Device discovery

A Bluetooth device can discover other devices by the inquiry process. A master in INQUIRY state hops 3,200 times per second according to a 32-channel inquiry hopping sequence. At the same time, a slave in INQUIRY SCAN state changes its listening frequency every 1.28 seconds, along the same sequence.

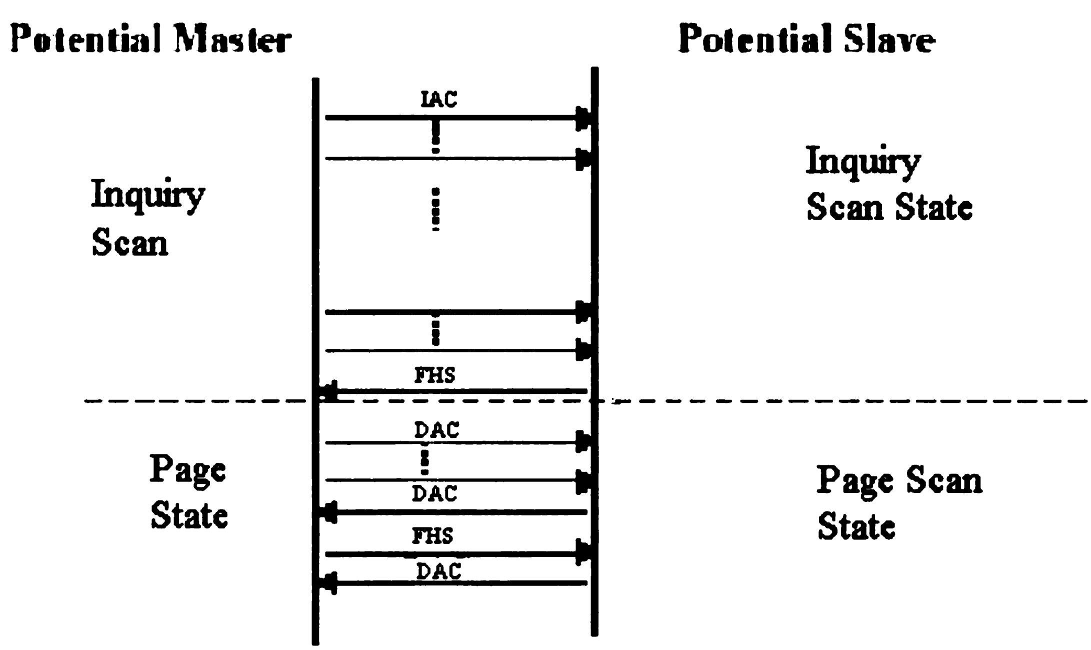


Figure 4.4: Bluetooth link formation process[14].

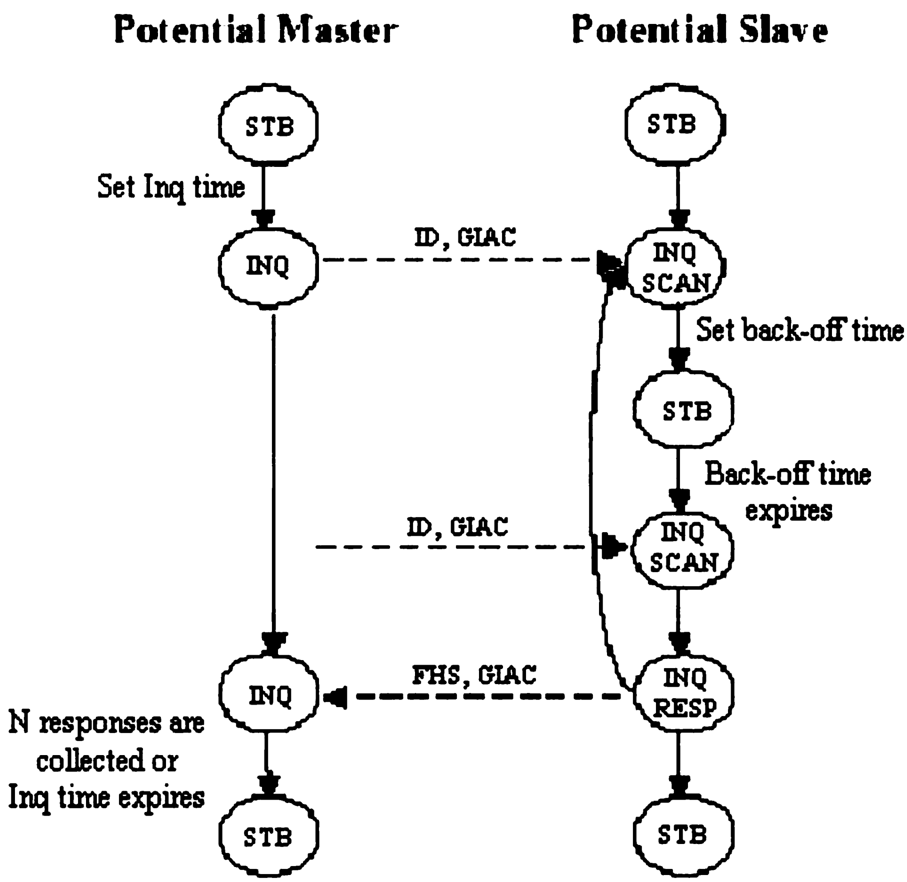


Figure 4.5: State transition during the Inquiry process[14].

If the inquiry process succeeds, the master learns the address (which is unique for each Bluetooth device) and the clock of the slave. In the page process, the master in PAGE state contacts the slave with a 32-channel page hopping sequence, which is a function of the slave's address and (estimated) clock. Similarly, the PAGE SCAN slave hops with the period of 1.28s along the same sequence. After the master and the slave are connected, they communicate with a hopping sequence over all 79 channels at the rate of 1600 hops per second. This hopping sequence is determined by the master's clock and address.

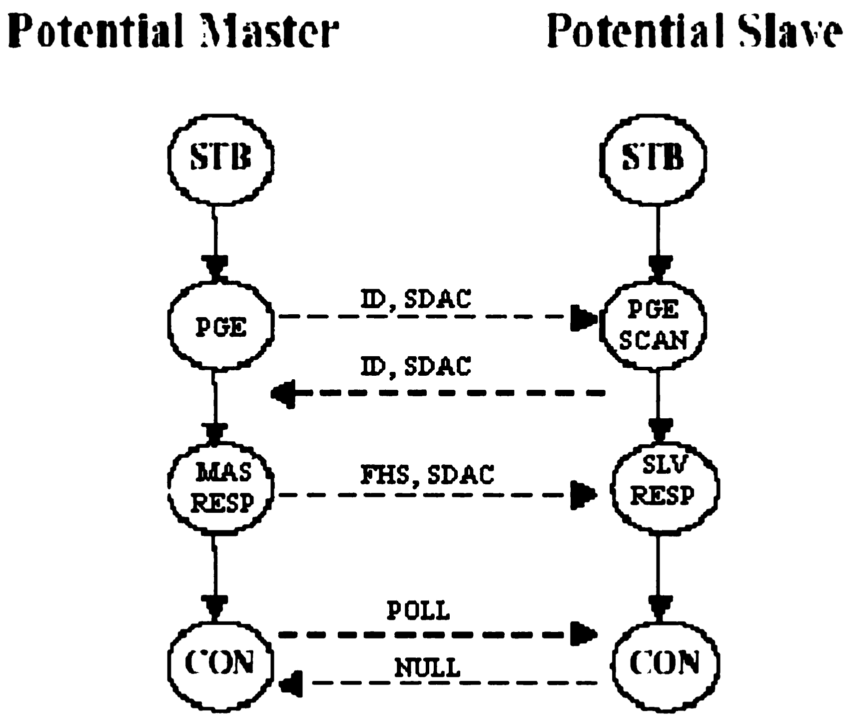


Figure 4.6: State transition during the Page process[14].

The following sections of this chapter give a brief description of the equipment used in the experiment and the lab layout.

4.9 Compaq iPAQ H3800 series Pocket PC[15]

For almost all the experiments, the Compaq iPAQ H3780 was used. The H3800 series iPAQs comes with inbuilt Bluetooth for wireless link to Bluetooth phones, printers, and PCs. The Bluetooth manager feature can be used to search for other Bluetooth devices and form bonding or share files with them.

The figures below are some screen shots from PoceketPCPassion site [15]. It show the Bluetooth interface provided in the iPAQ.

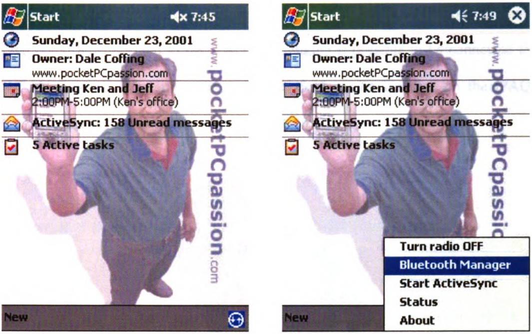


Figure 4.7: Bluetooth enabled iPAQ (Bluetooth icon on the lower right corner)

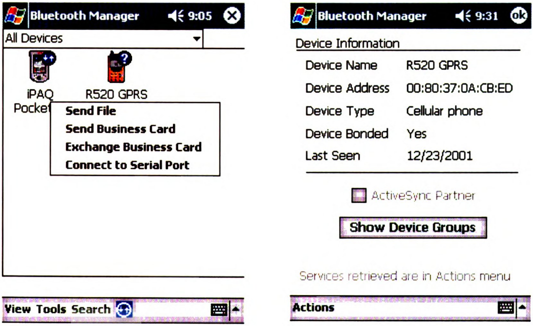


Figure 4.8: Creating bonds and exchanging information with other Bluetooth devices those lie in the vicinity.

With the use of an additional expansion pack, a D-Link or an Orinoco wireless card could be connected to the iPAQ thus making it possible to be connected to WLAN network. The appropriate software needs to be installed on the iPAQ before it can be used to access the WLAN network.

Figure 4.9: CF Expansion pack.

4.10 3COM Wireless Bluetooth USB adapter (Model No. 3CREB96)[16]

Figure 4.10: 3COM Wireless Bluetooth USB Adapter.

The 3COM wireless USB adapter makes it possible to 'Bluetooth enable' a PC or a laptop. Like the iPAQs, this was used with a number of PC/laptops to communicate with other Bluetooth devices during the experiments. The software interface lets the user know about other Bluetooth devices in the vicinity. It can even tell the class of the device viz - desktop computer or a laptop or a handheld. Through the interface, the user can create bonds with other Bluetooth enabled devices and exchange files.

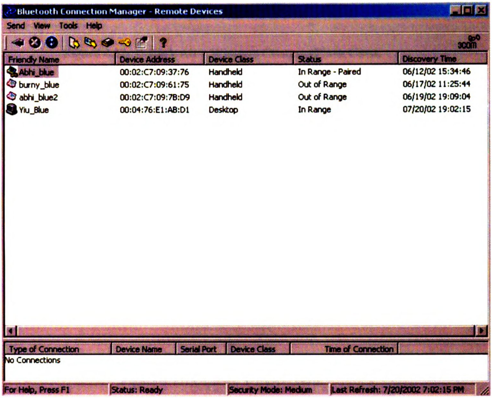


Figure 4.11: Screen shot of 3COM Bluetooth connection manager.

4.11 D-Link Air – Wireless CompactFlash card[17]

The D-Link DCF-650W is a wireless compact flash type II card that is IEEE 802.11b compliant. The DCF-650W provides a solution to connect PDAs such as the Compaq iPAQ and Casio 125 to an existing IEEE 802.11b wireless network. The D-Link card was used in all experiments involving 802.11b and iPAQ.

Figure 4.12: D-Link Air - Wireless CompactFlash Card.

4.12 Orinoco (Lucent) Wireless 802.11b Silver card[18]

Figure 4.13: Orinoco Wireless card.

The ORINOCO PC card can be used to wireless enable PCs and Laptops or even PDA having appropriate expansion slots and software. The card provides high-speed wireless networking at 11 Mbit/s, and secure Internet access for laptop and desktop computers, as well as a wide range of mobile client computing devices. The standard level, Silver PC Card, has wired equivalent privacy (WEP), using a 64-bit key. The Gold card has 128-bit key. For all experiments described in this report, the Silver card was used.

4.13 Orinoco USB Client[18]

The Agere System ORINOCO USB Client provides high-speed (11 Mbit/s) wireless Internet Access and networking for USB enabled desktops. Users can have wireless connectivity simply by plugging the USB Client into a spare USB connector and installing the software on a desktop PC or notebook. The USB Client supports wired equivalent privacy (WEP), using a 64-bit key.

Figure 4.14: Orinoco USB Client.

4.14 A Laptop (with Orinoco Client Manager software [18])

A laptop with Orinoco Client Manager software installed on it was used in the experiment. The client manager software can be configured to monitor and log the activities of a particular link. All the logs in the experiments were carried out for about three minutes (180sec). But for accuracy reasons, only 150 seconds were considered (not considering the first and the last 15 secs). The client manager software also gives a graphical representation of the signal variation in time. The signal variation and the log also record the variation at the remote partner.

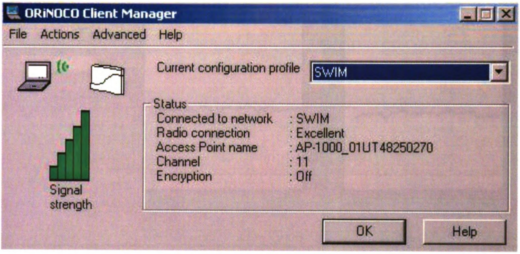


Figure 4.15: Orinoco Client Manager

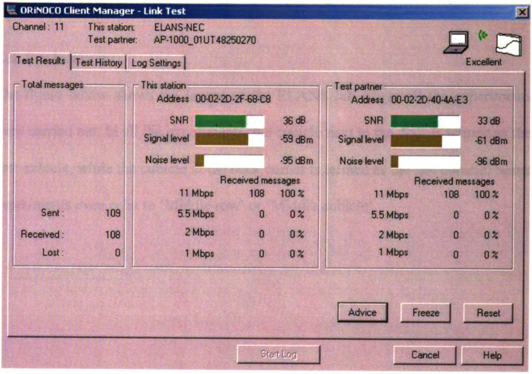


Figure 4.16: Orinoco Client Manger – Link Test

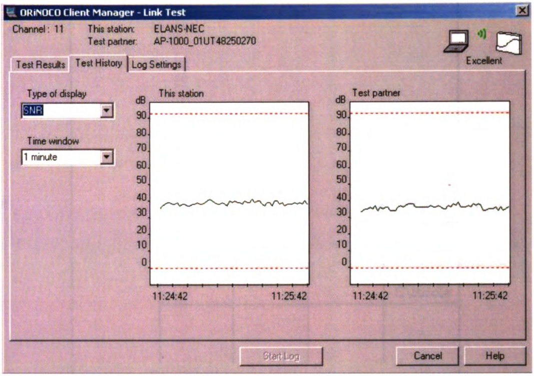


Figure 4.17: Orinoco Client Manger – Link Test (signal variation in time)

4.15 Lab Environment:

The figure below shows the layout of the ELANS lab where all the experiments were carried out. In all the experiments, the cubicle next to the door is termed as the first cubicle, while the cubicle in the back corner is termed as the last cubicle. Some experiments even refer to 'Middle row' or 'Middle cubicle'.

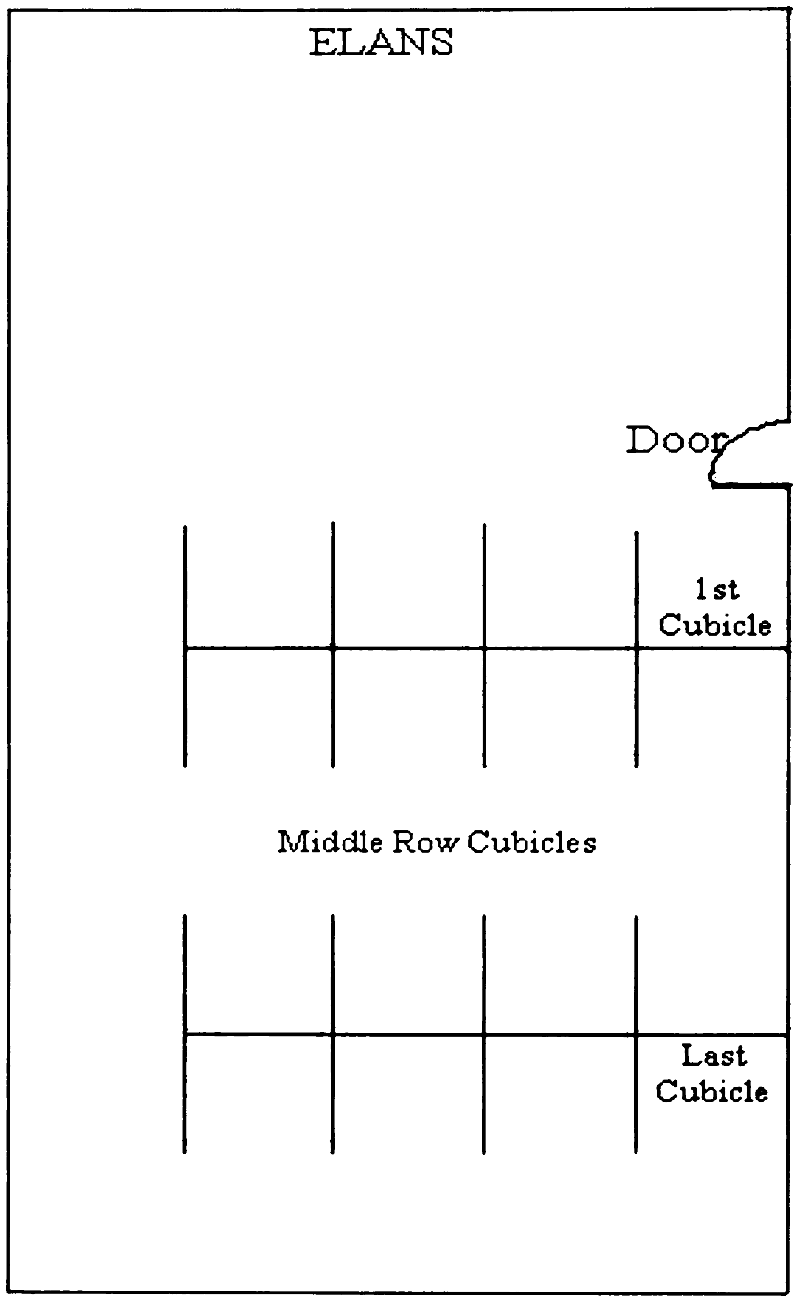


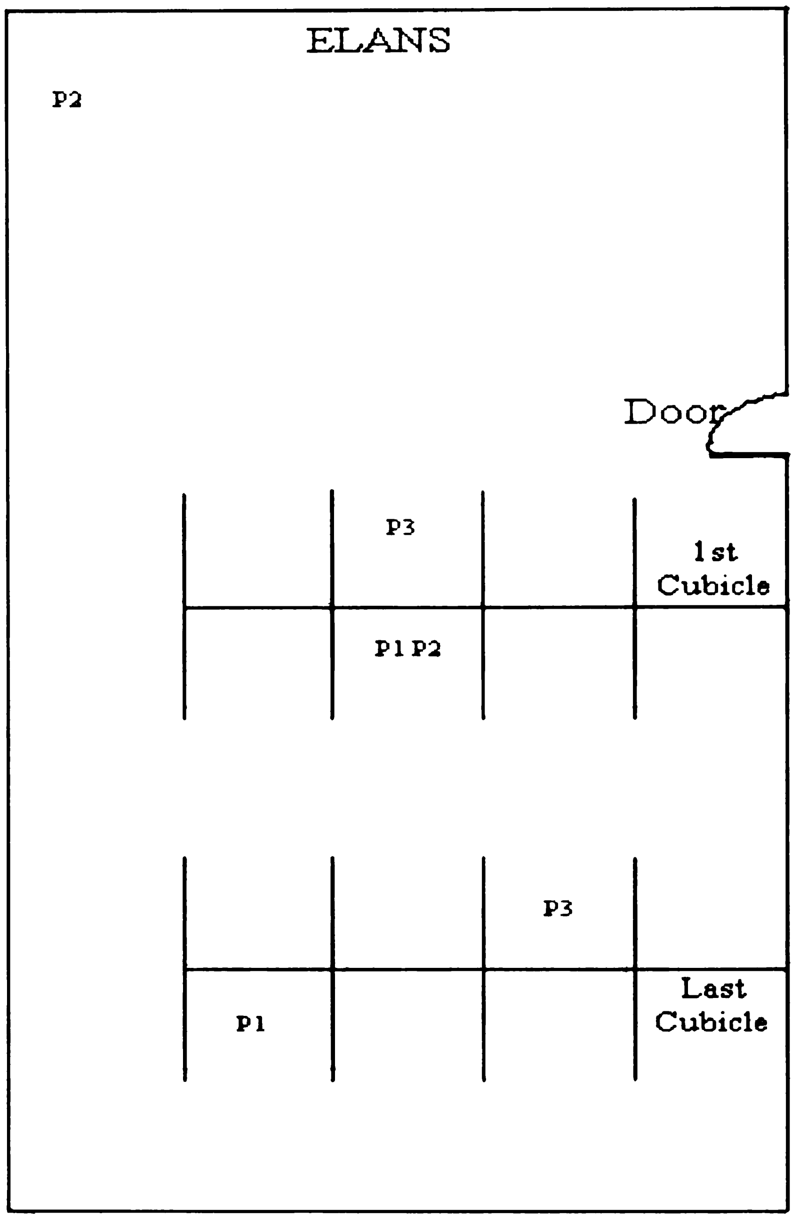
Figure 4.18: Layout of ELANS lab (EB1100 MSU)

5 Performance Evaluation of Wireless Technologies

This chapter describes the various experiments carried out at the ELANS lab with the aim to study how one wireless technology affects another. We examine the interference effect and how it affects the throughput. The experiments can be divided in to four sets:

1. The effects of 802.11b devices on other 802.11b devices,
2. The effect of Bluetooth on 802.11b,
3. The effect of 802.11b on Bluetooth and,
4. The effect of Bluetooth on Bluetooth.

5.1 Experiments to check the influence of 802.11b devices with other 802.11b devices



P1 – Position of first Pair (used in Case 1, 2 & 3)
P2 – Position of second Pair (used in Case 2 & 3)
P3 – Position of third Pair (used in Case 3)

Figure 5.1: Layout of ELANS lab showing position of various 802.11b devices in an experiment to check the interference between different 802.11b devices

5.1.1 Case1: Single pair of 802.11b devices present in the environment – No Interference:

An iPAQ with D-Link card and a laptop with Orinoco card are configured to ping each other over the same channel. The Orinoco client manager on the laptop is used to log the data. As mentioned earlier, the data logging was carried out for 3mins (180sec); but for accuracy reason, the first & the last 15secs are ignored. Thus the log of 150secs is considered. Since there is only one pair involved in this experiment, it represents the case where there is no interference present. The figures below show the result:

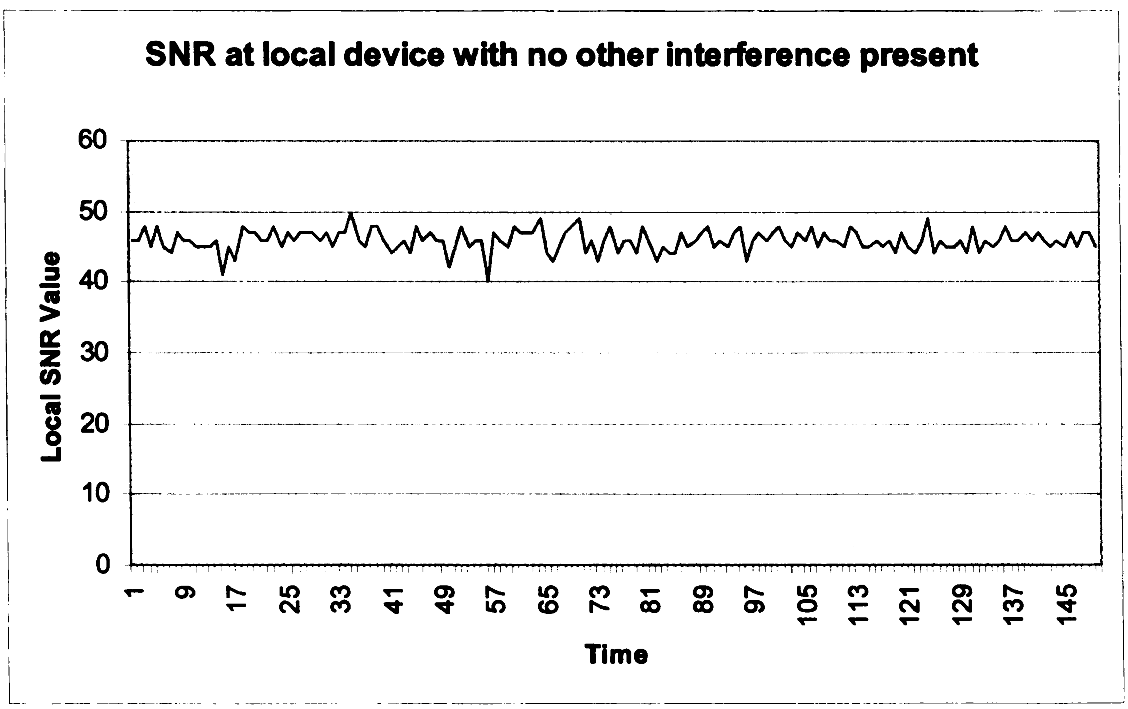


Figure 5.2: SNR value at Laptop (Local device) when Laptop & iPAQ placed away from each other with NO other interference present

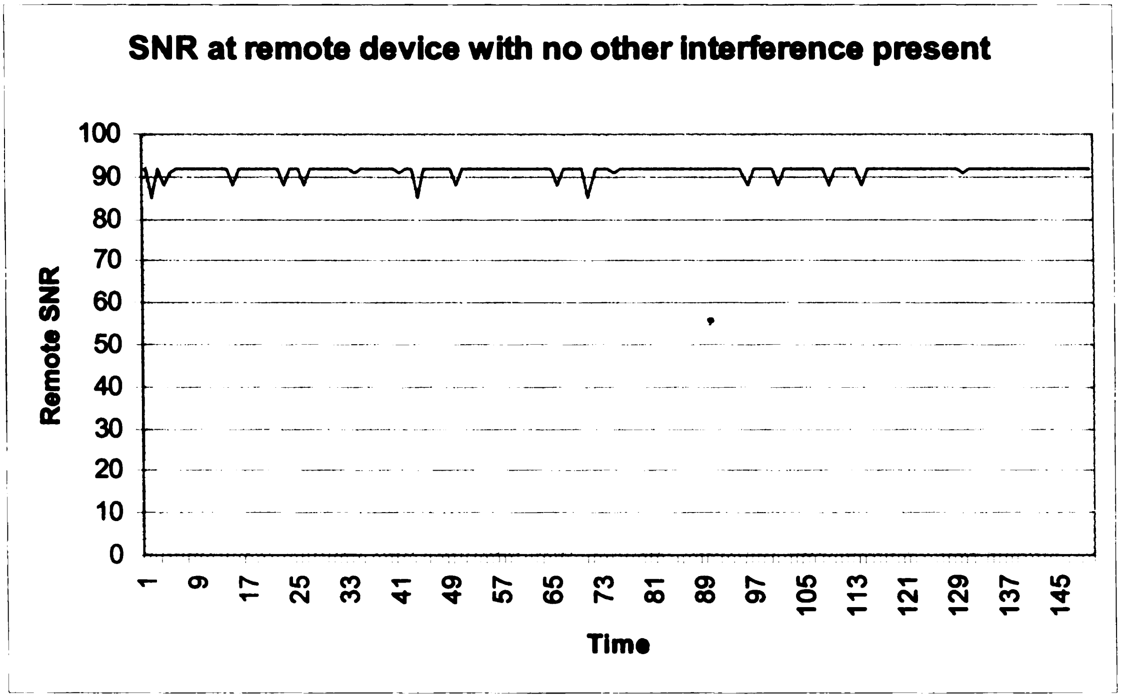


Figure 5.3: SNR value at iPAQ (Remote device) when Laptop & iPAQ placed away from each other with NO other interference present

Observation:

With no interference is present, the signal strength stays stable over a given range.

5.1.2 Case 2: Two Pair of 802.11b devices in the environment:

Another iPAQ with D-Link card and an Orinoco USB client on a PC are added to the setting in Case 1. They are configured so that they communicate over the same channel as the earlier configuration. Thus there is another pair of 802.11b devices now present over the same network as the earlier case. The Orinoco client manager on the laptop is used to log the data at the local and the remote devices. Like the earlier case, again only 150 sec are considered for accuracy. The figures below show the result:

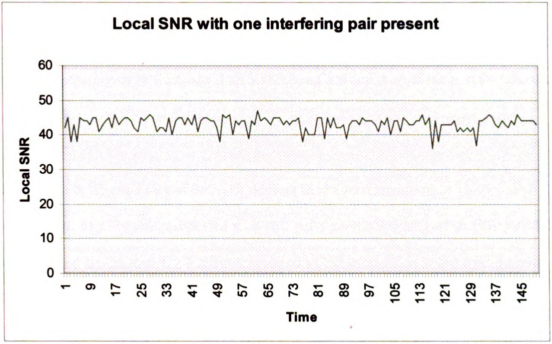


Figure 5.4: SNR at the laptop (local) when another pair of 802.11b devices is present in the same network.

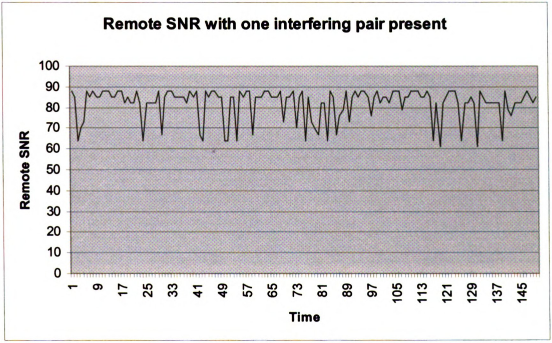


Figure 5.5: SNR at the iPAQ (remote) when another pair of 802.11b devices is present in the same network.

Observation:

When another pair is introduced in the same network, there is interference between the two causing the signal to fluctuate. The SNR shows a sharp drop at the point where there is collision between the two pairs.

5.1.3 Case 3. Three Pairs of 802.11b devices in the environment

This time the experiment is repeated with two pairs each consisting of an iPAQ with D-Link card and an Orinoco USB client connected to PC in addition to the configuration in Case 1. All the devices are configured so that they communicate over the same channel as the earlier configuration. The Orinoco client manager on the laptop is used to log the data at the local & the remote devices. The figures below show the results:

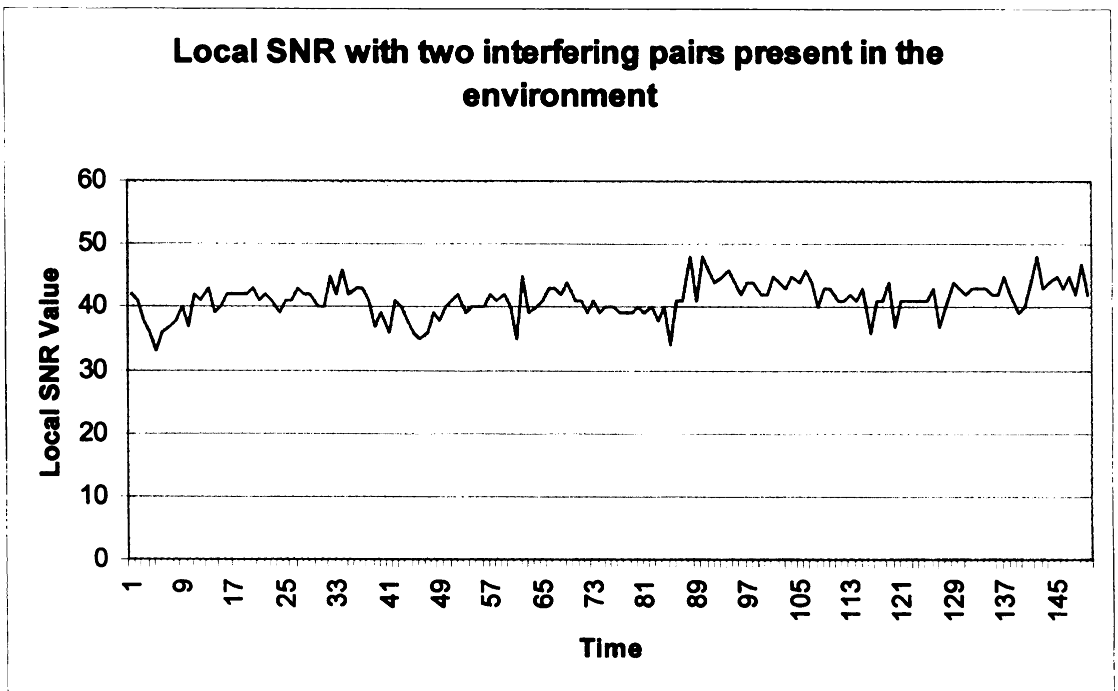


Figure 5.6: SNR at the Laptop (local) when two other interfering pairs of 802.11b devices are present in the same network.

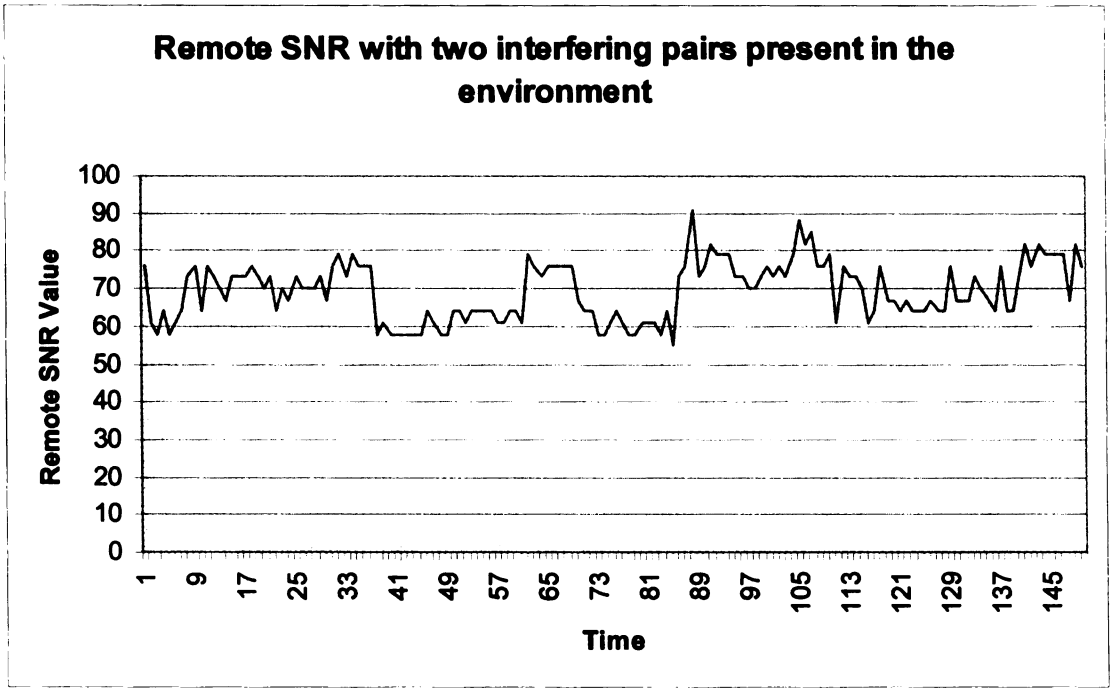


Figure 5.7: SNR at the iPAQ (remote) when two other interfering pairs of 802.11b devices are present in the same network.

Observation:

With two pairs present in the same network, the interference is much higher as can be seen from the graphs.

5.1.3.1 Explanation

The 802.11b standard defines 11 possible channels that may be used. Each channel is defied by its 'center frequency'. The center frequencies are at distances of 5MHz from each other. Since the high bandwidth (20dB) could give a signal as wide as 16MHz, multiple co-located networks channels have to be spaced out from another.

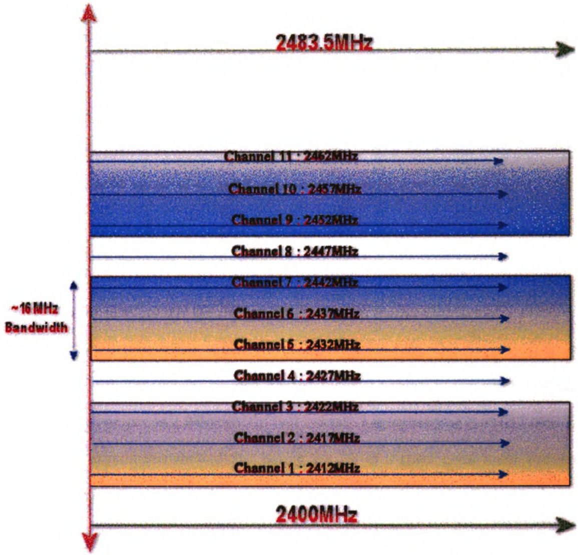


Figure 5.8: Channel spacing in 802.11b[19]

Thus, one 802.11b network could operate at any channel, but 2 co-located networks would have to have enough spacing, say channel 2 and 10, giving a minimum of 24 MHz in between them. Similarly, 3 co-located networks would have to choose from something like channels 1, 6 & 11, to ensure enough spacing. More than 5 co-located channels is not recommended.

5.1.3.2 Effect on Throughput

In theory, an 802.11b link should have an effective bandwidth of 11Mbps. But due to processing overhead, signaling information, stray interference, etc, the bandwidth is reduced to a lower value. When more devices operating over the same channel are added and all other factors remaining the same, the interference factor increases. The sharp drops in the SNR values in the graph show this. Collisions mean retransmission. Thus it can be said that as the number of devices are increased in the same network, effective bandwidth for a particular link drops.

To test the effect of one 802.11b device on another, we did a performance evaluation using netperf, benchmarking software available from HP [20]. The Netperf server was running on PIII-750MHz PC running RedHat Linux 7.3 using an Orinoco Silver card. While, the client ran on a PII-366MHz Dell Latitude Laptop running RedHat Linux 7.1. Our initial experiments showed that having the PC as a client gives lower values of throughput; possibly due to OS overhead and slower CPU speed on the laptop.

We also notice as seen from Figure 5.9 that the throughput is high when the UDP packet size used for testing is 1472 or multiples of that. The reason we believe this happens is because 1472 is the payload value for an Ethernet packet size. For all other values higher than 1472, there is fragmentation and for values lower than 1472, the packet size is not enough to keep the channel busy and there may be 'gaps' between successive test packets resulting in lower throughput values. Henceforth, for all experiments related to throughput calculations we have used 1472 as the packet size.

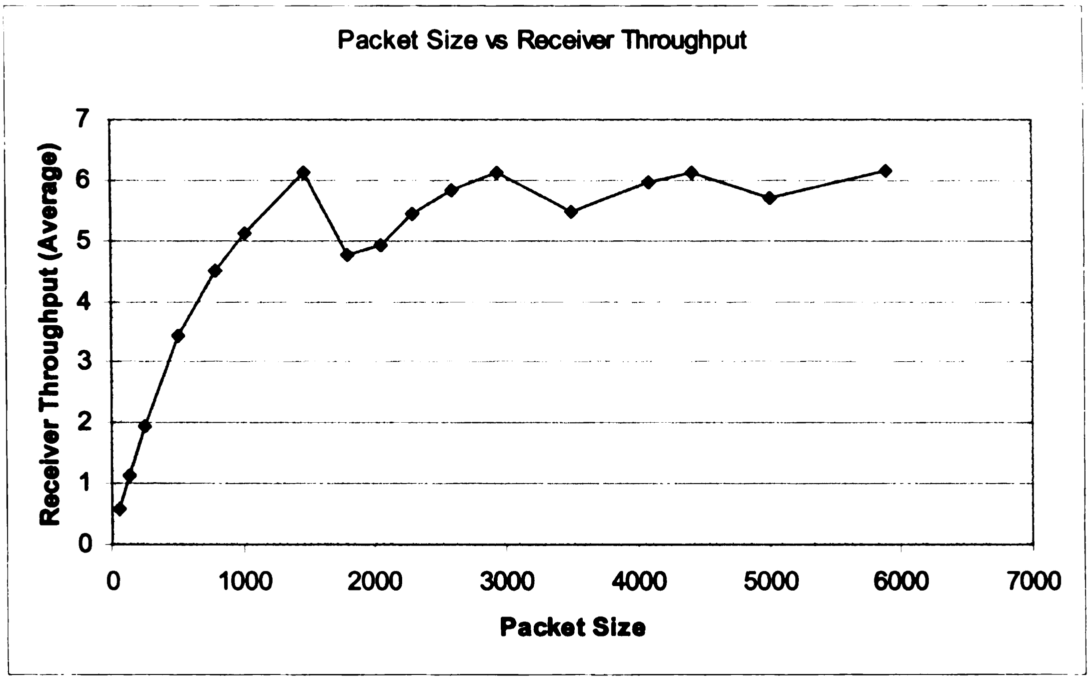


Figure 5.9: Graph of UDP packet size (in Netperf testing) versus throughput at the receiver.

To test the effect of another 802.11b pair in the vicinity, we introduced a pair consisting of the Orinoco USB adapter on a PC and an iPAQ with a D-link card. To keep constant data traffic between the new pair, iPAQ was made to ping the PC constantly.

It was noticed that for smaller ping packet sizes, the new pair didn't have much effect on throughput of the earlier one. However, as the ping packet size increase, the effect of interference was more visible. The graphs below clearly show the effect. There were two sets of experiments that were conducted – one with the interfering pair very close to the test pair (Figure 5.10) and the other with the interfering pair at the distance of 7m with a cubicle partition in the middle (Figure 5.11). The receiver throughput values are average of three trials.

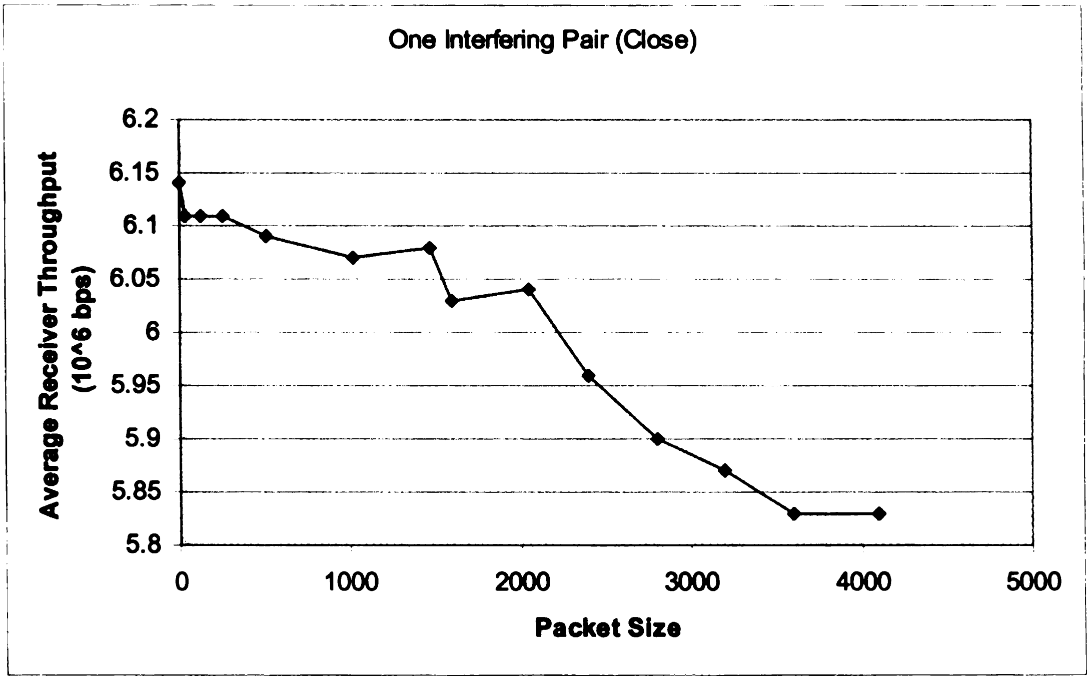


Figure 5.10: Graph showing the variation in the receiver throughput as the ping packet size in the interfering pair is increased (interfering pair very close to test pair).

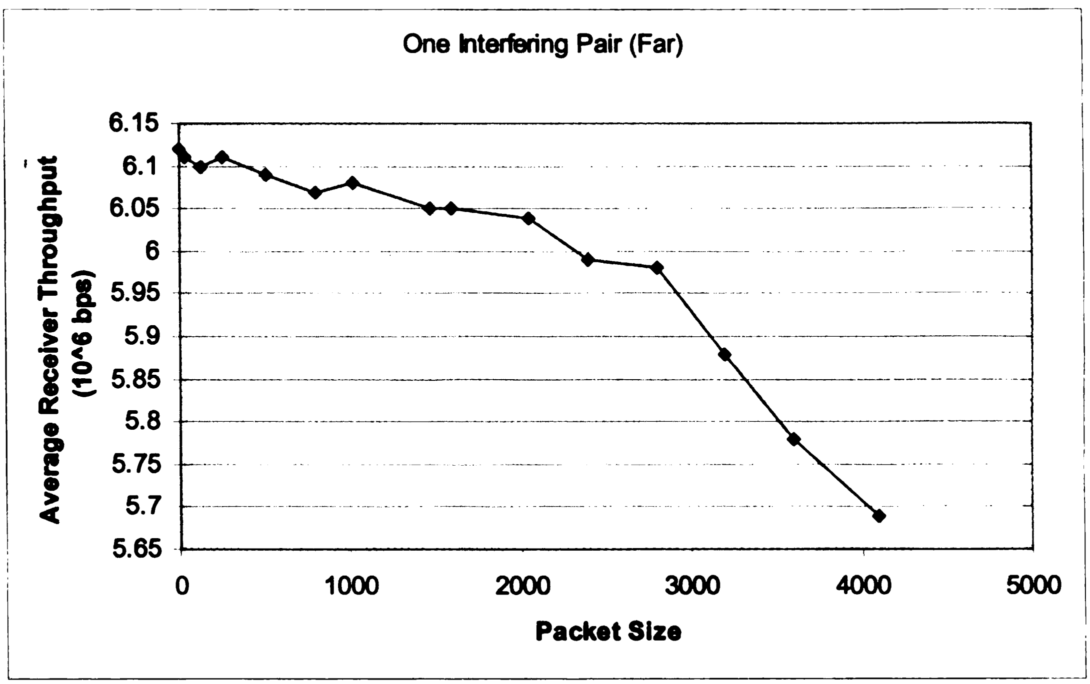


Figure 5.11: Graph showing the variation in the receiver throughput as the ping packet size in the interfering pair is increased (interfering pair away from test pair).

The effect of two other interfering 802.11b pairs is shown below:

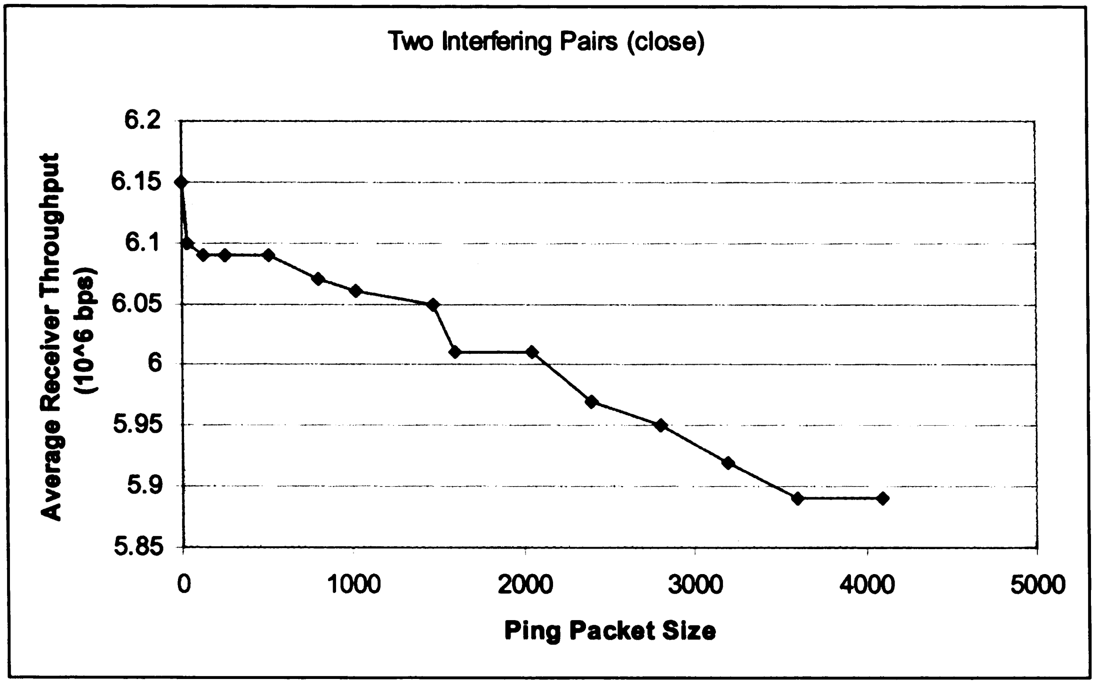


Figure 5.12: Throughput of 802.11b when two other interfering 802.11b pairs are kept in close vicinity.

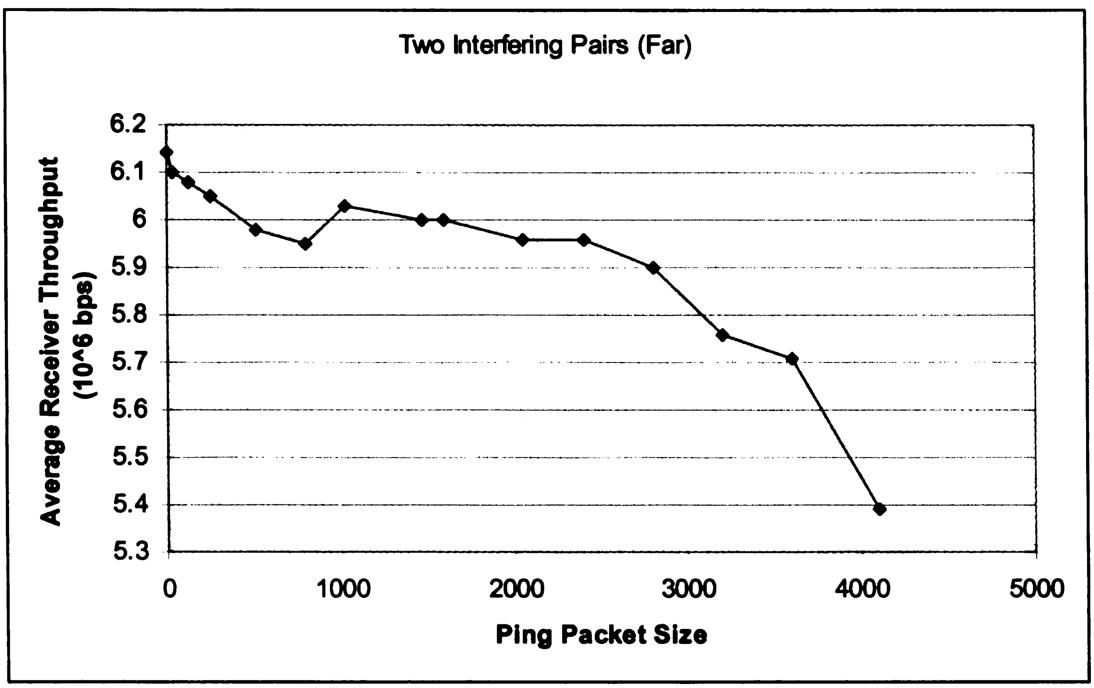


Figure 5.13: Throughput of 802.11b when two other interfering 802.11b pairs are kept at approx 7m from the test pair.

5.1.3.3 Location sensing & 802.11b

In the above experiments, all the devices were made to communicate over the same channel and hence the interference increased as the number of pair of communicating devices increased. In a location-sensing environment, all the sensors would be operating over the same frequency range. If 802.11b device were to act as a location sensor, then all the communication (location-sensing) between the 'unknown' 802.11b user devices and the sensor had to be on the same channel. The experiments above clearly show that this is not possible with 802.11b since there would be a lot of interference. Thus 802.11b would not be a good candidate for location sensing.

5.2 Experiments to study the interference of Bluetooth on 802.11b devices

5.2.1 Case 1: Interference with a single pair of Bluetooth device

In Case 1, we investigate interference between a pair of 802.11b and a single pair of Bluetooth devices.

We examined two scenarios in this case:

- Near – when Bluetooth and 802.11b are very close to each other.
- Far – when Bluetooth and 802.11b are very away from each other.

5.2.1.1 Near

In this case, a pair of Bluetooth and a pair of 802.11b devices was placed in the same cubicle. The laptop had the Orinoco Client manager running which logged the SNR for the different cases. As explained earlier, the data is logged for 180sec but only the 150sec in the middle are considered. The figures below show the result of the interference with Bluetooth present:

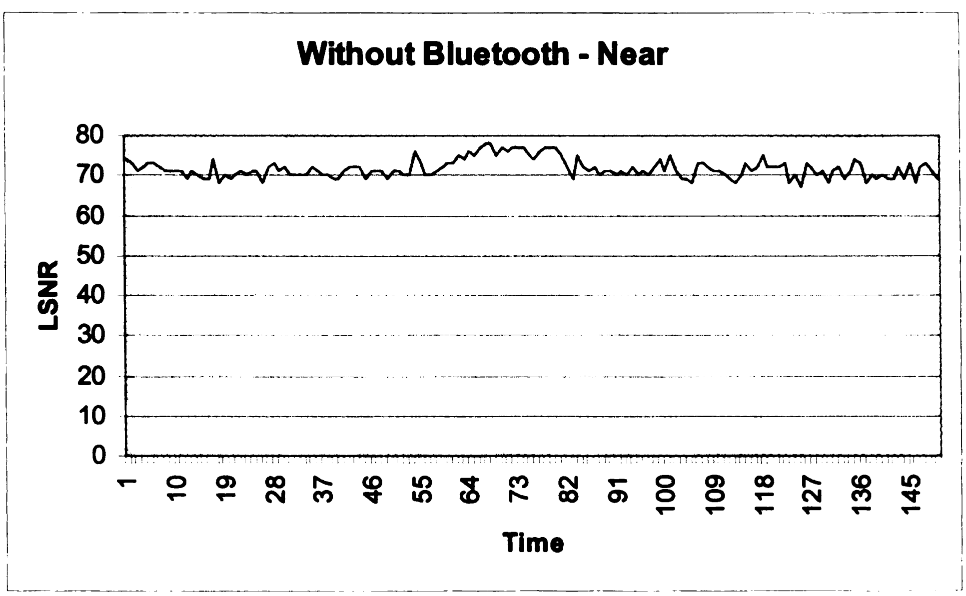


Figure 5.14: Local SNR without the presence of any interference from any Bluetooth device.

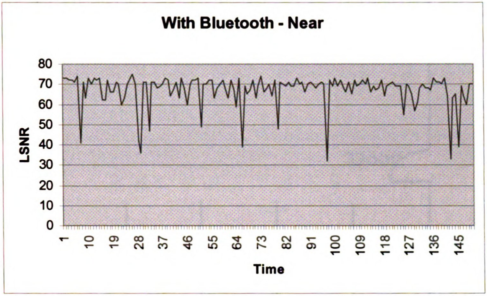


Figure 5.15: Local SNR when an active Bluetooth file transfer is being done in the vicinity.

Observation:

Sharp negative spikes are observed when Bluetooth is present in the environment clearly indicating that there is interference between the two technologies.

5.2.1.2 Far

The figure below shows the case when Bluetooth and 802.11b devices were placed far from each other. In this case, the laptop was placed in the last cubicle.

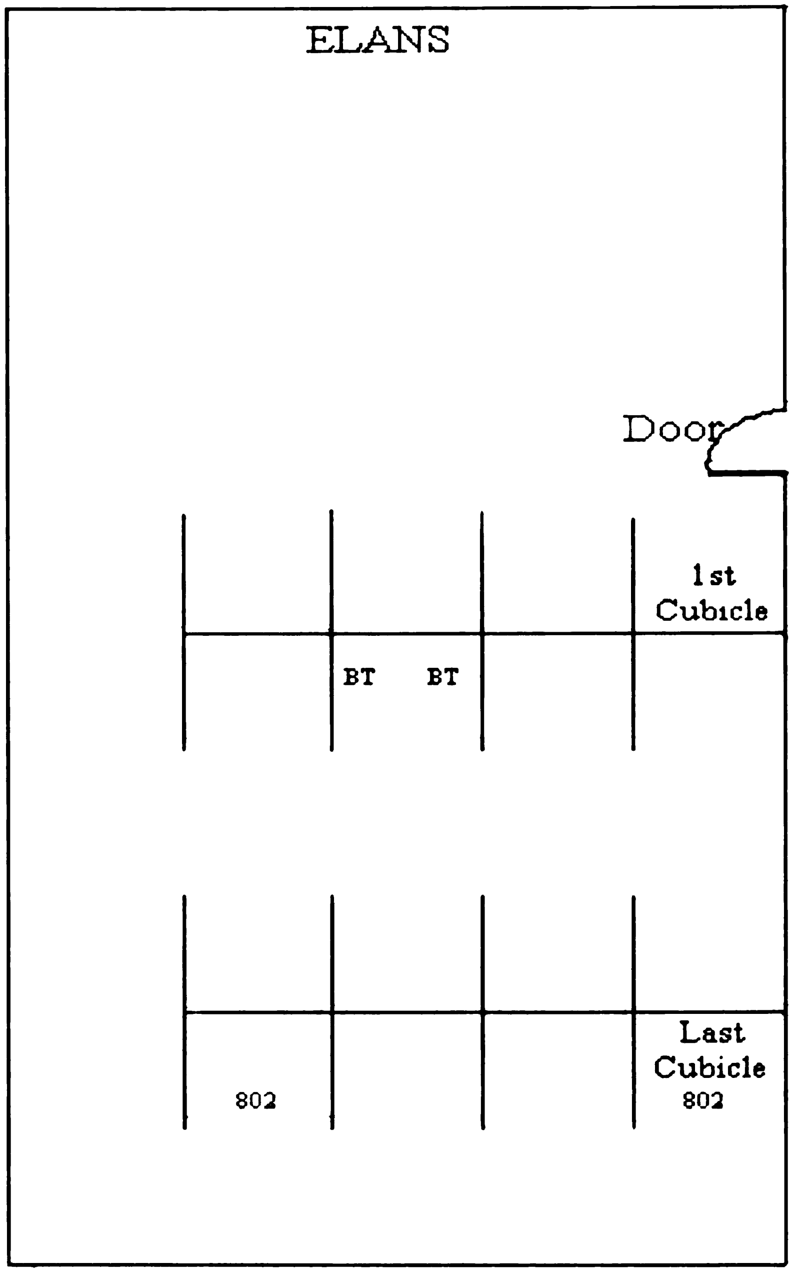


Figure 5.16: Laptop placed in the last cubicle

The Orinoco client manager logged the data on the laptop. The figures below show the result of the interference with and without the presence of Bluetooth.

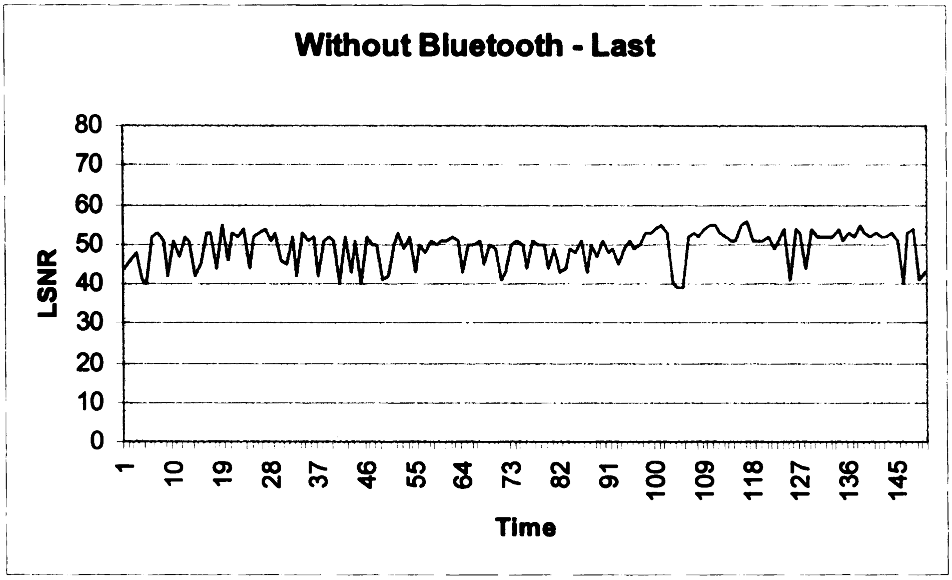


Figure 5.17: SNR values on the laptop when there is no Bluetooth activity and the laptop is in the last cubicle.

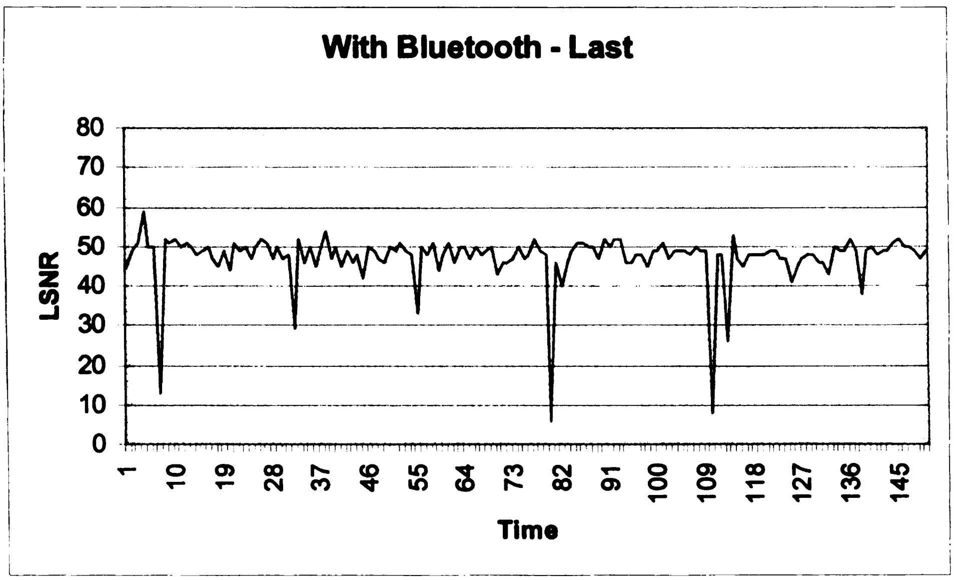


Figure 5.18: SNR values on the laptop when an active Bluetooth file transfer is in progress and the laptop is away (last cubicle) from the Bluetooth device.

Observation:

Again, like the earlier case, sharp spikes are observed in presence of Bluetooth. However, the frequency of the spikes is less.

5.2.2 Case 2: Interference between a pair of 802.11b & two pairs of Bluetooth devices.

In this set of experiment, all the devices were placed in the same cubicle. As always, the laptop had the Orinoco Client manager running which logged the SNR for the instance when Bluetooth was and was not present. Also, the readings were logged for 180sec but only 150secs were considered. The figures below show the result:

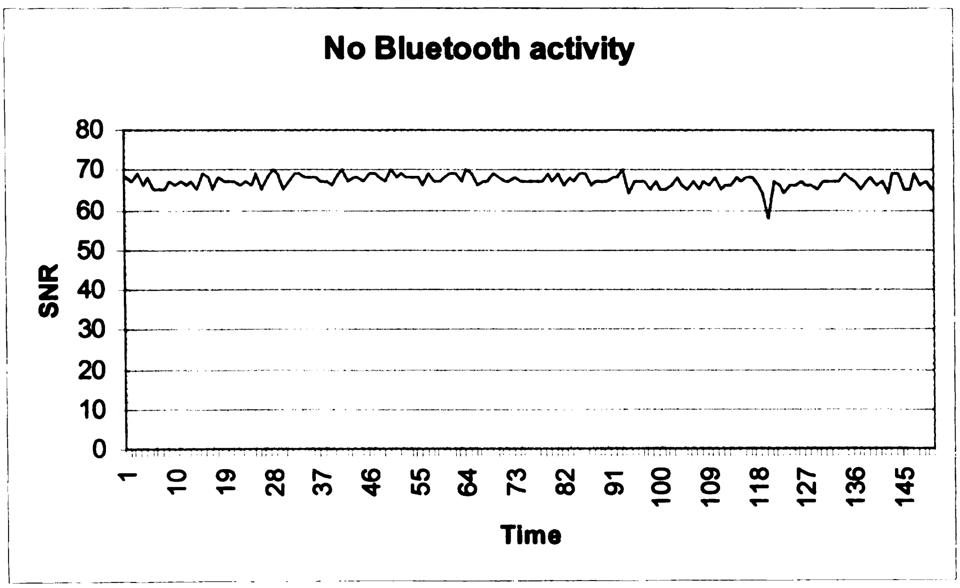


Figure 5.19: SNR value at the laptop when there are two pairs of Bluetooth devices in the vicinity but no Bluetooth activity going on.

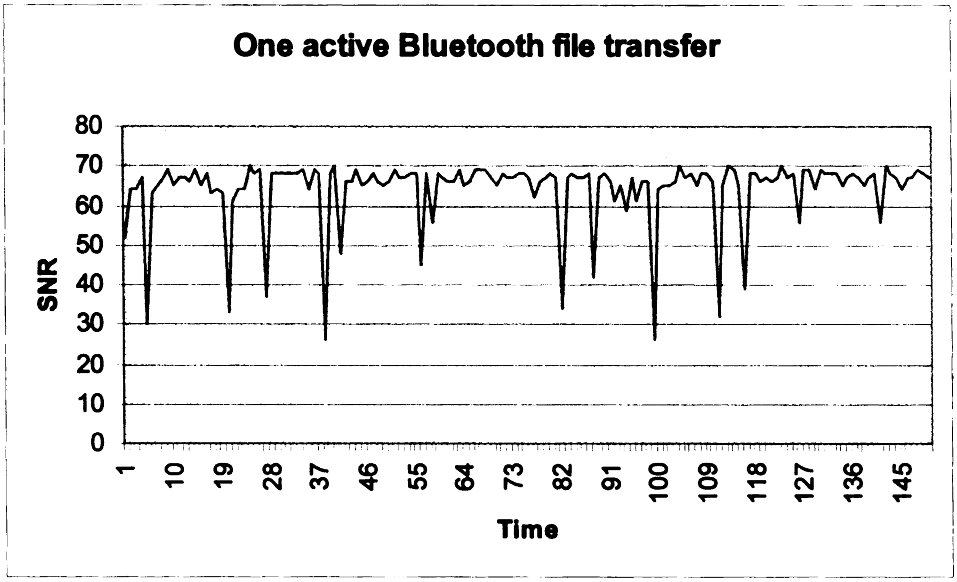


Figure 5.20: SNR value at the laptop when there are two pairs of Bluetooth devices in the vicinity and only one pair is doing a file transfer.

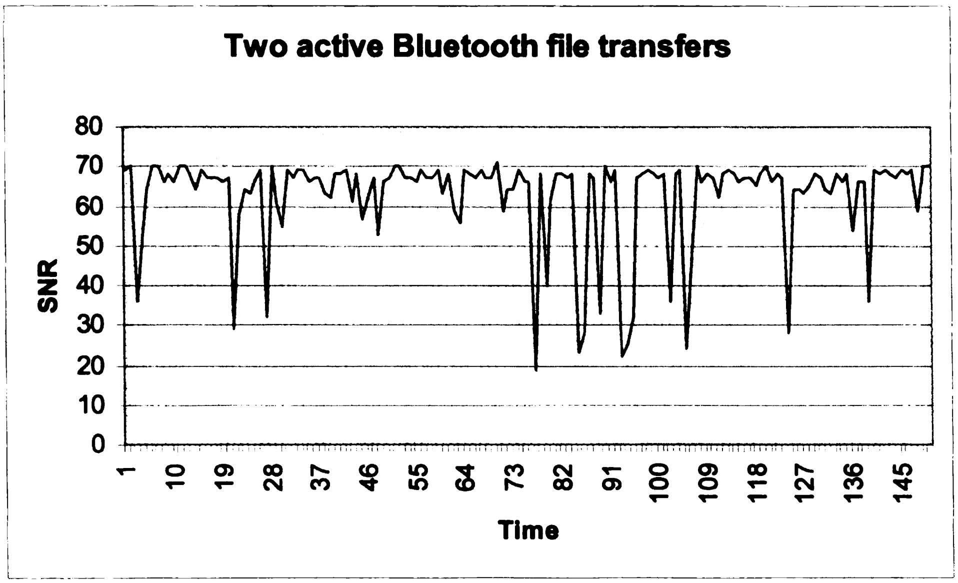


Figure 5.21: SNR value at the laptop when there are two pairs of Bluetooth devices in the vicinity and both the pairs are doing a file transfer.

Observation: In presence of more devices, the frequency of the negative spikes is higher. However, there is little increase in the magnitude of the spikes.

5.3 Effect of 802.11b on Bluetooth

The Bluetooth specification makes it optional for the manufacturers to give signal strength information for a particular link. The Bluetooth productions that were used in these experiments didn't give signal strength information and hence Bluetooth performance was measured in terms of file transfer time, which points to the effective bandwidth for a Bluetooth link.

Three experiments were carried out. In each case, a file of size 4437kb was transferred between two Bluetooth devices and also, the number of 802.11b pairs was increased. The table below shows the result:

Table A: Effect of 802.11b on Bluetooth

No. of 802.11b Pairs	File transfer time
1	6min 4sec
2	6min 5sec
3	6min 7sec

Observation:

It can be seen that there is a marginal decrease in the file transfer time as the number of 802.11b devices are increased. Implying that 802.11b had very little effect on the Bluetooth bandwidth. Since, Bluetooth API to do throughput measurements is currently unavailable, bandwidth performance measurement for Bluetooth in presence of interference is one of the items that we intend to take a look at in the future.

5.4 Explanation for interference between 802.11b and Bluetooth devices:

By their nature, when both Bluetooth and 802.11b devices occasionally hop to the same frequency, packets will be lost and throughput will be reduced. In the course of experiments, it was seen that in extreme conditions where a Bluetooth or 802.11 interfere is positioned right beside to a receiver of the opposite technology, throughput is significantly reduced. However, as the interferer is positioned further away, the interference reduced. If the distance between the two is more than 10m, then the throughput is only minimally reduced compared to normal.

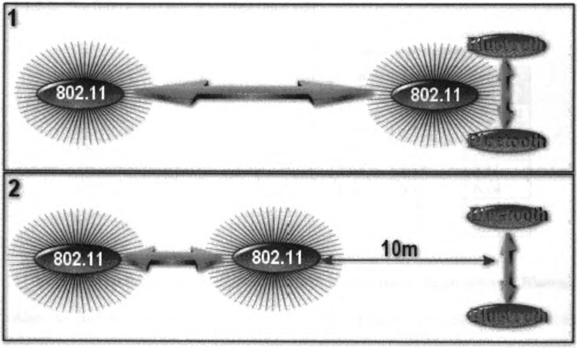


Figure 5.22: Effects of Bluetooth on 802.11b. If Bluetooth is within 10m of 802.11b, the performance of 802.11b is greatly affected[19].

One thing to note, as shown in case studies, is that Bluetooth will cause more interference with 802.11, than the other way around due to Bluetooth's much faster hop particular frequency, a Bluetooth device might hop to this frequency several times before 802.11 device hops to the next frequency. Bluetooth hops 600 times faster than 802.11b.

5.4.1 Effect on Throughput

Although both technologies drop packets, 802.11's packets are bigger so more information has to be re-transmitted. Thus, the effect of interference is more on 802.11b.

To study the effect of Bluetooth on the throughput of 802.11b, we carried out performance measurement using Netperf [20], similar to the ones described in Section 5.1.3.2. The following table describes the result:

Table B: Performance of 802.11b in presence of Bluetooth.

Condition	**Receiver Throughput (10^6 bits/sec)**		
	Lowest	Average[1]	Highest
No Bluetooth device present	6.11	6.12	6.15
One Bluetooth Pair in close vicinity	4.37	5.33	5.91
One Bluetooth pair in middle cubicle[2]	5.64	5.88	6.11
One Bluetooth pair in last cubicle[3]	6.10	6.12	6.14
Two Bluetooth pairs in close vicinity	3.60	3.94	5.08
Two Bluetooth pairs in middle cubicle	6.07	6.09	6.11

It can be seen that the throughput of 802.11b is affected by the presence of Bluetooth. Also, as the distance increases, the interference effect is reduced. Throughput also depends on the number of devices present in the environment.

[1] Interference from Bluetooth is not constant but in the form of spikes. Hence, values in this column are average of 10 trials.
[2] Middle Cubicle is about 7m from the test pair with one cubicle partition in between.
[3] Last Cubicle was about 10m from the test pair with two cubicle partitions in between.

5.5 Experiment to study the interference between Bluetooth devices.

The currently Bluetooth products available in the market do not support signal strength measurement. Therefore, the average time required for a file transfer was used as a measure to study the effects of Bluetooth on other Bluetooth devices.

The table below shows the result for a file size of 4437kb:

Table C: Effect of Bluetooth on Bluetooth

No. of Bluetooth Pairs	Effective Bandwidth
1	6min 7sec
2	6min 9sec
3	6min 11sec
4	6min 12sec

Observation:

It can be seen that there wasn't much difference between the average time it took to complete the file transfer in each case.

5.5.1 Explanation

Since Bluetooth hops at 1600hops per sec, the chances of collision are low. Besides a Bluetooth packet is small and hence, retransmissions are smaller. Thus the effective bandwidth is not affected to a great extent.

Since, Bluetooth API to do throughput measurements is currently unavailable, bandwidth performance measurement for Bluetooth in presence of interference is one of the items that we intend to take a look at in the future.

5.6 Experiment to study the signal variation in an indoor environment.

Although, the experiment described in this section does not go with the title of this chapter, it is described here since its results apply to all wireless devices used in indoor environment like offices, hospitals etc. Besides, the results of this experiment give rise to a very important concept – the concept of using reference tags. The aim of this experiment was to prove that signal strength is not a good measure of distance.

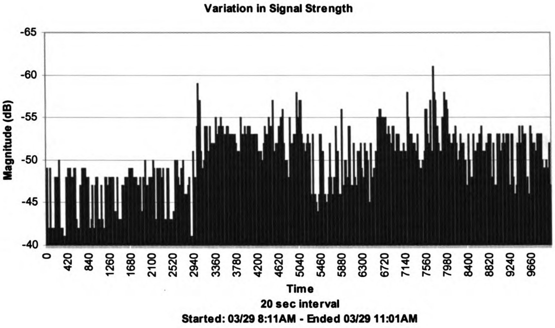


Figure 5.23: Signal variations over time, as different activities are a carried out in a room.

Description:

A laptop was placed in the cubicle next to the door in the ELANS lab. The Orinoco software on the laptop was monitoring and logging the link status with the wireless access point in the room. As can be seen from the figure, the experiment was started at approx 8.10AM and logged the data for about 3hrs with every sample at 20sec interval.

Some facts about 03/29/02:

- 8AM – 9AM ELANS lab empty.
- SWIM team meeting started at 9AM and got over at about 10AM.
- 10AM – 10:30AM presentation in CSE conference room.
- 11AM onwards, lab almost full with all its occupants present in their respective cubicle.

Observation:

From Figure 5.23 it can be seen that the signal strength was strong during 8-9AM when the lab was empty. There is a strong degradation in the signal strength during the time the SWIM team meeting and the time when everyone was present in the lab. There is an improvement in the signal strength when some of the lab members attended the seminar in the CSE conference room.

Explanation:

There are many factors involved in signal propagation in an indoor environment. Signal propagation is greatly affected by placement of furniture, movement of people, walls, etc. Thus, signal strength alone cannot be used for estimating distance. Later, the concept of reference tags is explained to overcome this problem.

6 Location-Sensing with Bluetooth

From the experiments described in the previous chapter, we can conclude:

- As the number of 802.11b devices operating over the same channel increases, the interference between them increases.
- There is significant interference between Bluetooth and 802.11b devices. The interference is higher when the devices are close to each other. Beyond the range of Bluetooth, it drops down significantly. Also, the effect of Bluetooth is more on 802.11b than the reverse case.
- There is very little interference between two Bluetooth devices place in close vicinity.

6.1 General Configuration:

In a location-sensing environment, we would need to have several devices of the same type operating on the same network. Hence, it would be important that these devices have very little interference between them. With the above results, it can be seen that

Bluetooth can satisfy these requirements and hence, can be a good candidate for use in indoor location sensing.

Before we get into the details of implementing a Bluetooth based location sensing system, here is a overall layout shows a possible Bluetooth location-sensing environment:

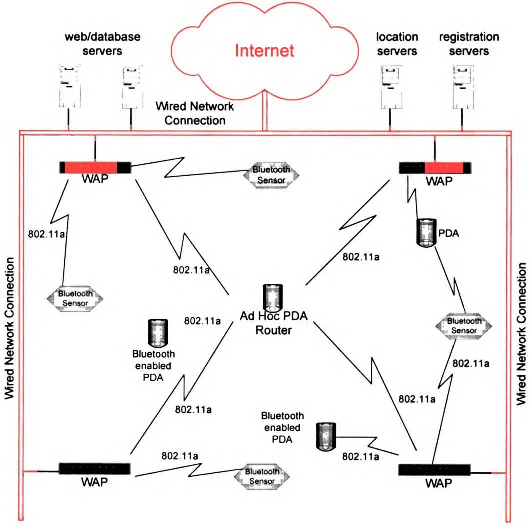


Figure 6.1: General system infrastructures with Bluetooth as a location sensing technology and 802.11a being the wireless backbone.

Since Bluetooth and 802.11b don't get along very well, this thesis proposes the use of 802.11a as an alternative. 802.11a, as we have earlier seen, uses the 5GHz band. Thus there won't be any chance of interference between Bluetooth and an 802.11a device. Besides, it is said that 802.11a due to its faster data rate would soon replace the existing 802.11b infrastructure. Since Bluetooth is becoming a standard feature in most hand-held devices, it would eliminate the need for the user to carry additional sensory devices, as needed by several location-sensing technologies of earlier times.

As explained earlier, a Bluetooth piconet can have 7 active slaves and up to 200 inactive devices in parked mode. For location sensing application, it is enough to 'see' another Bluetooth device. Also, it doesn't matter if the other device is a master or a slave. The device should be within the range to be detected. This implies that a Bluetooth sensor would be able to detect up to 200 other Bluetooth devices. The next sections talk about some possible architectures using Bluetooth for location sensing:

6.2 Bluetooth location sensing with reference tags

We have already seen in Section 5.6, Signal strength varies randomly with time. The signal strength variation affects the tracking and the reference tag in the same manner. Thus, by using the concept of reference tags, a real-time system can be designed. With the advent of Bluetooth ASIC chips, the price of Bluetooth devices is expected to drop down significantly in the near future and the size of a Bluetooth sensor would be very small. Thus using Bluetooth reference tags would very much be a feasible idea.

We consider two possibilities – location sensing when signal strength information is not made available and location sensing when that information is available. At present all of the Bluetooth devices available in the market don't make signal strength information available. Making it available is optional according to the Bluetooth specification.

6.2.1 Without signal strength information

Similar to RFIDs, every Bluetooth device has a 48bit address. These reference tags can be uniformly spread in the area of interest. The Bluetooth sensors can be placed at 5m each so that they overlap in their range.

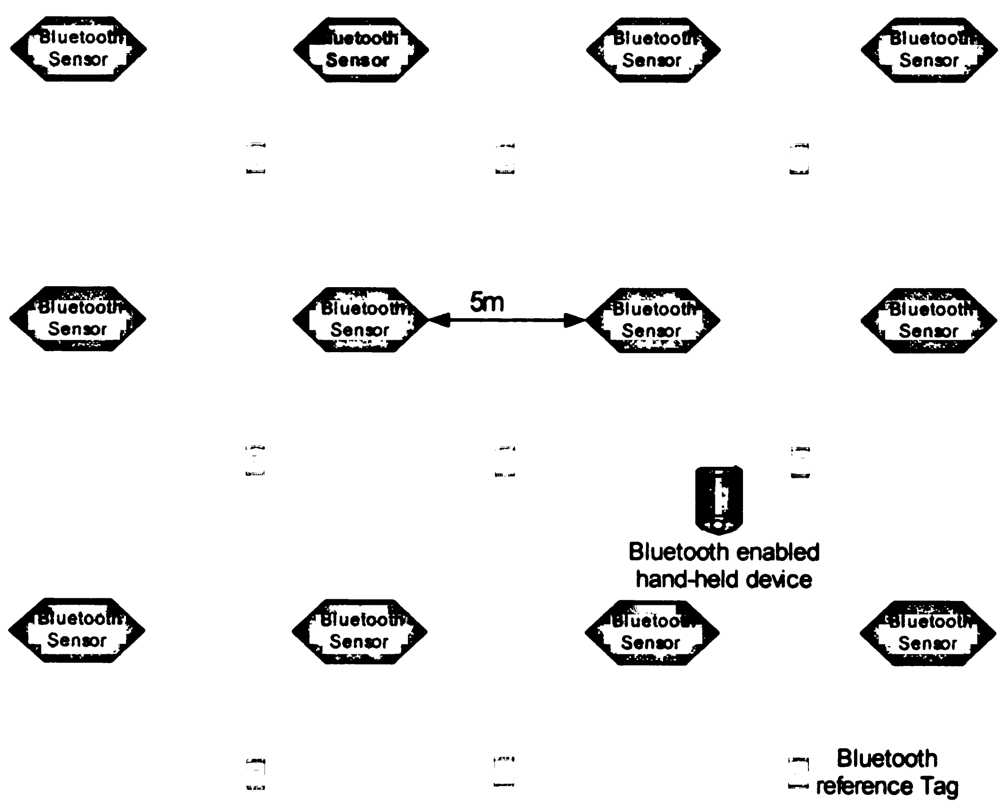


Figure 6.2: Bluetooth location sensing using the concept of reference tags.

Since the reference tags are positioned in-between the sensors and the sensor range overlap, each reference tag would be seen by more than one sensor. We define a table whose rows represent individual tags and the columns represent every reader. Now, for a device whose location is unknown, we can similarly have a row in the table. By compare this row with the ones that already exists, we can predict where the device might be present. For example:

Table D: Locating unknown tag using reference tag (in absence of signal strength information)

	Reader 1	Reader 2	Reader 3	Reader 4
Tag – 1	0	1	1	0
Tag – 2	1	1	1	0
Tag – 3	0	0	1	1
Unknown – 1	0	0	1	1
Unknown – 2	1	0	1	0

We can see from the table that the Unknown-1 device's row information matches with that of Tag 3 which means that they are very close to each other (if not at the same place). While for Unknown-2, the information closely matches with that for reference tag 2. Hence, Unknown-2 must be located somewhere in the vicinity of Ref Tag 2.

The accuracy of this approach depends on how tight the reference tags are placed, the geometric placement of readers and reference tags and the amount of overlap between neighboring readers.

6.2.2 If signal strength information available

If in the future Bluetooth products meant for location sensing could give signal strength information then, a real-time system can be implemented. Referring to Figure 6.2 again, we do the following analysis.

Assume there are n Bluetooth readers and m reference tags. We define the Range Vector of an unknown tag as:

$$u = (u_1, u_2, \ldots\ldots, u_n)$$

where R_i denotes the signal strength value of the unknown tag perceived on Bluetooth reader i, $i \in (1, n)$. For the reference tags, each one also has its range vector as:

$$r_i = (r_{i,1}, r_{i,2} \ldots\ldots r_{i,n}) \text{ where } i \in (1, m).$$

Due to the instability of the signals, we cannot obtain the physical distance between the reader and a tag (reference tag or unknown tag) directly from the signal strength. However, with the known coordinates of all the reference tags, we are able to physically locate an unknown tag based on the reference cell of the unknown tag.

The Figure 6.3 shows the signal strength information as perceived by the different readers for a particular reference tag (ref tag 5 in this case). Note that the figure doesn't show the values seen by all readers. In practice, each reader will receive some signal strength from every tag.

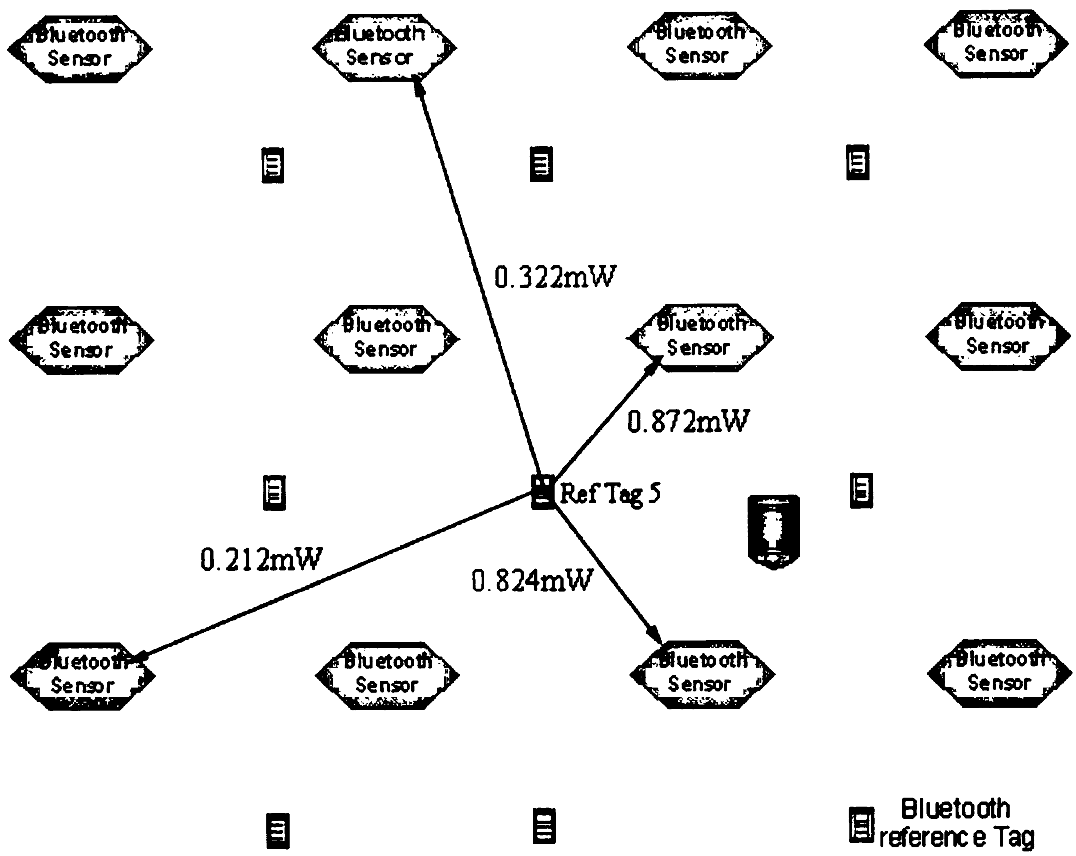


Figure 6.3: Signal strength of Ref Tag 5 as perceived by Bluetooth readers.

We can introduce the Euclidian distance in signal strength. For each individual unknown tag, we define:

$$E_i = \sqrt{\sum_{k=1}^{n}(r_{i,k} - u_k)^2}$$

as the Euclidian distance in signal strength between an unknown tag and a reference tag r_i. To simplify the description of our approach, let us assume there are 4 RF readers and 16 reference tags in the experimental environment. Our approach can be easily extended to an environment that has more than 4 RF readers and 16 reference tags. The signal strength vector of the reference tag and the unknown tag is $s = (s_1, s_2, s_3, s_4)$. When we consider one individual unknown tag only, its vector of E is given by:

$$E_1 = \sqrt{\sum_{k=1}^{4} (r_{1,k} - u_k)^2}$$

$$E_2 = \sqrt{\sum_{k=1}^{4} (r_{2,k} - u_k)^2}$$

......

......

$$E_{16} = \sqrt{\sum_{k=1}^{4} (r_{16k} - u_k)^2}$$

Let E denotes the location relationship between the reference tags and this unknown one.

There are three key issues that we examine through the process of locating the unknown tag. The first issue is the placement of the reference tags. Since the unknown tag is ultimately located in a reference tag cell, the layout of reference tags may significantly affect the location accuracy of an algorithm.

The second issue is to determine the number of reference tags in a reference cell that are used in obtaining the most approximate coordinate of the unknown tags. This may also be termed as selecting 'k' nearest neighbors. Now, for example we may use the coordinate of the reference tag with the smallest E value to the tracking tag as this unknown tag's coordinate (k=1), or we can choose 2 nearest tags (k=2) and the unknown tag's coordinates can be simply determined by the arithmetic means of the coordinates of those two nearest tags as:

$$x_{unknown} = \frac{1}{2}(x_{nearest1} + x_{neraest2})$$

$$y_{unknown} = \frac{1}{2}(y_{nearest1} + y_{neraest2})$$

When we are using k nearest reference tags' coordinate to locate one unknown tag, the following equation could be introduced:

$$(x, y) = \frac{1}{k}\sum_{i=1}^{k}(x_{ri}, y_{ri})$$

However, since the nearest neighbors are not at the same distance from the unknown tag, we need to assign weight so that the nearest tag gets more importance than the one far. This becomes the third issue in this approach. Thus, the unknown's coordinate can be obtained as:

$$(x, y) = \sum_{i=1}^{k} w_i (x_{ri}, y_{ri})$$

Intuitively, this must be done based on the E value of each reference tag in the cell.

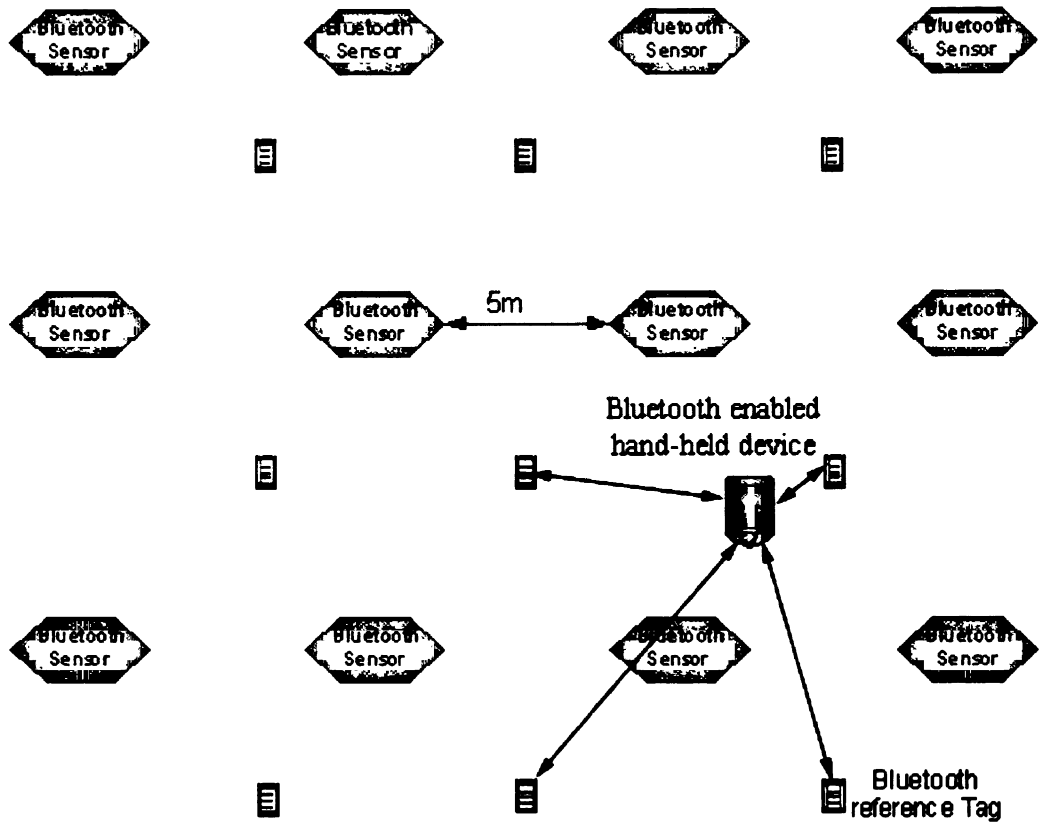


Figure 6.4: Case of 4-nearest Neighbors.

Instead of giving weight to all *k*-nearest neighbors the same weights in averaging, w_i is introduced and it is a function of the E of all *k*-nearest neighbors. Our approach of the weight is depending on the E as:

$$w_j = \frac{\frac{1}{E_i}}{\sum_{i=1}^{k} \frac{1}{E_i}}$$

In this approach, the reference tag with the smallest E value has the largest weight.

7 Future Work

From the performance measurements of chapter 5, we can see that Bluetooth can indeed be a good replacement for current indoor location-sensing technologies.

7.1 Bluetooth Wish-list

However, it must be noted that Bluetooth was not designed for location sensing and hence there are certain enhancements that it would have to undergo so that it is best suited for indoor location sensing. Some of these enhancements are stated below:

- An important improvement would be to reduce the time taken by a Bluetooth device to detect another Bluetooth device in its vicinity. The time taken in the present system is not short enough to track a moving object. In addition, many of the Bluetooth products available today have their refresh time fixed to a certain value. For example, in the 3COM USB adapter, the smallest refresh time is 5mins and it increases in multiples of 5. Future devices should have an option so that this time is much shorter and configurable. This would mean that other Bluetooth devices would be detected with very little delay and a system for tracking moving objects can be designed.

- Another feature mentioned in the Bluetooth specification but not implemented in any of the recent Bluetooth products is to give the signal strength information for a particular link. If this information is made available, it can greatly aid in accurate location sensing. The concepts developed in chapter 3 and chapter 7 can be applied.
- In the current Bluetooth spec, there is provision for 3 power levels. The minimum power level gives a range of 10m. If future implementations can give a shorter range, then location sensing can be made more accurate. Since Bluetooth devices are expected to be cheaper in the future, we can use more sensors covering very short area thus improving accuracy.

Currently, we haven't been able to test any of the configurations mentioned in chapter 7 since we didn't have many Bluetooth devices. Although, the price of Bluetooth devices is dropping, the current price is not encouraging enough to buy a whole lot of Bluetooth devices for implementing a prototype system in the lab. Once we get enough number of equipment, we plan to test the different configurations described in the earlier chapter and try to find which one amongst them gives greater accuracy.

We also plan to look at other commodity wireless technologies that can be used in conjunction with Bluetooth so that we can set up a system similar to Cricket[6].

Another item in the list for future works is the throughput measurement for Bluetooth in presence of interference. Currently, we didn't have any Bluetooth API to do bandwidth measurements and hence we could not do effective bandwidth calculation in presence of interference in presence of other Bluetooth devices or other wireless technologies operating in the same frequency range.

7.2 Some new configurations:

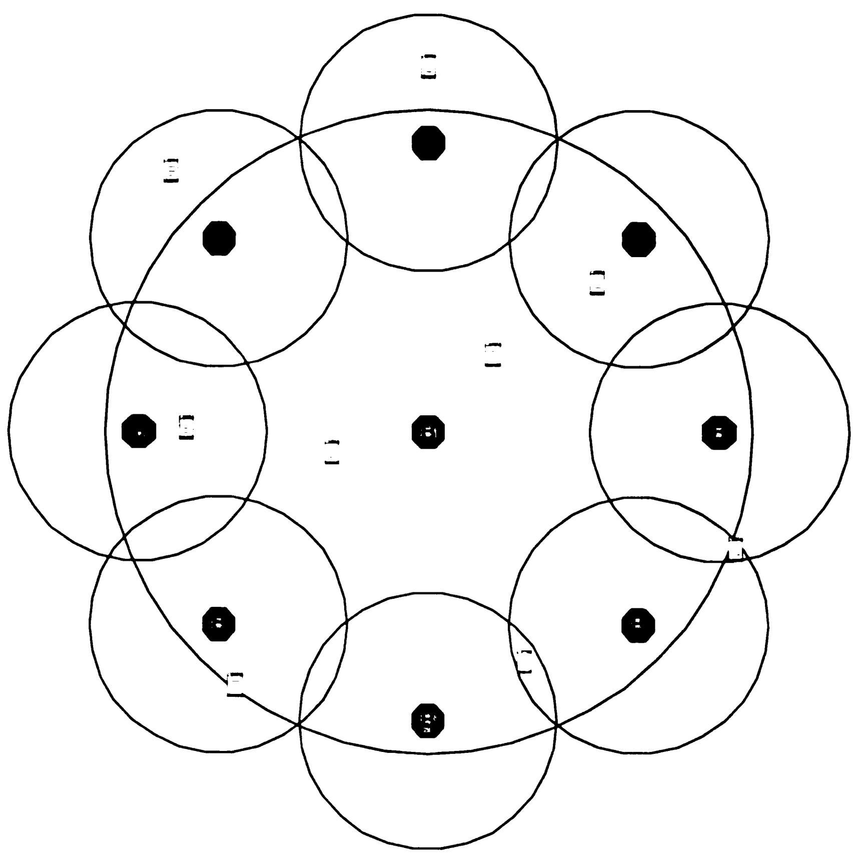


Figure 7.1: Bluetooth sensors placed to form a Ring of Circles.

Place of readers is an open issue; we can try different configurations to see which one gives the best accuracy. The central reader is operated at Class 1 or Class 2 signal strength thus allowing it to scan a large area. Several readers are placed along the circumference range of this reader.

The advantage of using this approach is that the region is divided into several smaller regions that can be uniquely identified. A tag that is sensed by one of the readers along the circumference and the central reader is in the intersection of the central reader and the outer circle. A tag that is read only by an outer circle is located outside the bigger circle but within the outer circle and so on. Besides, the system is more flexible and easier to deploy due to its modularity.

BIBLIOGRAPHY

[1] A. H. Roy Want, Veronica Falcão and Jonathan Gibbons, "The Active Badge Location System."

[2] P. B. a. V. N. Padmanabhan, "RADAR: An In-building RF-based User Location and Tracking System.", *Proceedings of IEEE INFOCOM 2000.*

[3] R. W. Jeffrey Hightower, and Gaetano Borriello, "SpotON: An Indoor 3D Location Sensing Technology Based on RF Signal Strength."

[4] J. Small, Smailagic, A.and Siewiorek, D., "Determining User Location For Context Aware Computing Through the Use of a Wireless LAN Infrastructure.", Dec 2000.

[5] M. A. Andy Ward, Paul Osborn, Joe Newman, Steve Hodges, "The Bat Ultrasonic Location System.", http://www.uk.research.att.com/bat/

[6] "The Cricket Indoor Location System.", http://nms.lcs.mit.edu/projects/cricket/

[7] University of Berkeley, California, "TinyOS project.", http://webs.cs.berkeley.edu/tos/

[8] "HP Cooltown project.", http://www.cooltown.hp.com/

[9] Y. C. Lau, "LANDMARC: Location Identification based on Dynamic Active RFID Calibration."

[10] "Radio Frequency Identification (RFID) home page.", http://www.aimglobal.org/technologies/rfid/what_is_rfid.htm

[11] "RF Code, Inc", http://www.rfcode.com/

[12] S. Kapp, "802.11: Leaving the Wire Behind.", *IEEE Internet Computing*, Jan-Feb 2002.

[13] C. Bisdikian, "An overview of the Bluetooth wireless technology.", *IEEE Communications Magazine*, Dec 2001.

[14] A. M. Godfrey Tan, John Guttag and Hari Balakrishnan, "Forming scatternet from bluetooth personal area networks.", MIT Laboratory for Computer Science.

[15] "PoceketPCPassion Review H3800.", http://www.pocketpcpassion.com/iPAQ/H3800/H3870_Screens.html

[16] "3Com Corporation Homepage."

[17] "D-Link Homepage."

[18] "Orinoco Homepage."

[19] "Palowireless.com - Wireless Resource Center."

[20] "Netperf Homepage.", http://www.netperf.org/netperf/NetperfPage.html

[21] Amar. K. Mehta, Kai-Yeung Sui and Ching Law, "Performance of a New Bluetooth Scatternet Formation Protocol.", MIT.

[22] Jeffrey Hightower and Gaetano Borriello, "A Survey and Taxonomy of Location Sensing Systems for Ubiquitous Computing.", Aug 2001.

[23] C. Johnson and K. Cheng, "The Glasgow Context Server: A wireless system fir location awareness in mobile computing."

[24] S. Waterson, S. Klemmer, K. Whitehouse, "Towards a Location-Based Context-Aware Sensor Infrastructure.", Dec 2000.

[25] Nathan J. Muller, "Bluetooth Demystified" McGraw-Hill Telecom.