NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

Bluetooth Voice Transmission

Graduation Project
COM-400

Student: Fadi Azzam Al-Aghbar (20020919)

Supervisor: Dr. Jamal Fathi Abu-Hasnah

Nicosia - 2006

**Dedicated to my Father, Mother,
Brother, and my Sister**

ACKNOWLEDGEMENTS

This project is done under the supervision of Dr. Jamal, I am very grateful to him who gave his technical and emotional support for the creation of this graduation project.

And my Thanks go to whom my love will never end, my father and my mother, to my brother and a sister, that help me a lot and their encouragement in my studies, so that I could be successful in my life.

I will also like to thanks my all friends in Cyprus who gave their ever devotion and helped me for their all valuable information to complete this project.

ABSTRACT

The concept behind Bluetooth is to provide a universal short-range wireless capability. Using the 2.4 GHz band, available globally for unlicensed low-power uses, two Bluetooth devices within 10 m of each other can share up to 720 Kbps of capacity. Bluetooth is intended to support an open-ended list of applications, including data (such as schedules and telephone numbers), audio, graphics, and even video. For example, audio devices can include headsets, cordless and standard phones, home stereos, and digital MP3 players.

In indoor pico-cellular wireless systems, such as Bluetooth, a pico-cell has a master-slave configuration. Bluetooth is a centralized master driven system that supports time division duplex medium access control. A pico-cell has a limit on the maximum number of active slaves. In Bluetooth, a pico-cell can have a maximum of seven slaves in active state (capable of transmitting and receiving data). The remaining slaves in a pico-cell remain in an inactive state. Having more than seven slaves connected to the master can be advantageous in many situations. Having a large number of slaves in one pico-cell as compared to forming new pico-cells can lead to lower power consumption and relatively simple network architecture. We investigate different methods of increasing the capacity of Bluetooth pico-cells. We propose new policies using the park mode to increase the number slaves virtually connected to a master. These policies can have a significant impact on system parameters such as the throughput, packet delays and dropping probability of packets.

CONTENTS

1. INTRODUCTION

1.1 Overview

Bluetooth has been the subject of much hype and media attention over the last couple of years. As various manufacturers prepare to launch products using Bluetooth technology, an unsuspecting public is about to be catapulted into the next stage of the information technology revolution.

Bluetooth is a low cost, low power short-range radio technology originally developed as a cable replacement to connect devices such as mobile phone handsets, headsets, and portable computers. This in itself sounds relatively innocuous; however, by enabling standardized wireless communications between any electrical devices, Bluetooth has created the notion of a Personal Area Network (PAN), a kind of close range wireless network that looks set to revolutionize the way people interact with the information technology landscape around them. No longer do people need to connect, plug into, install, enable or configure anything to anything else. Through a ubiquitous standardized communications subsystem, devices will communicate seamlessly. One does not need to know where one's cellular phone is, or even if it is switched on. As soon as the Web browser appears on the mobile computer screen, a link is established with the phone, the Internet Service Provider is connected to, and the user is surfing the Web.

The Bluetooth specification is an open, global specification defining the complete system from the radio right up to the application level. The protocol stack is usually implemented partly in hardware and partly as software running on a microprocessor.

1.2 What Is Bluetooth

Bluetooth is a wireless communication protocol mainly used for short distance and in devices with low power consumption. Because Bluetooth is capable of communicating in an omni-directional manner of up to 30 feet at 1 Mb/s it is far superior to infrared. Where infrared requires a distance of a few feet or less and requires a direct line of site for transmissions. Okay what about WiFi, which typical can transmit up to 300 feet at 11 Mb/s. Well the fact is these are really two different beasts; Bluetooth was developed for small data transfers and/or voice communications. Which makes it an excellent candidate for peripherals devices such as wireless microphones, headsets, mice, keyboards and of course mobile handsets. WiFi in general was developed to transmit large amounts of data and to serve as an extension of an existing network such as LAN. Not only does Bluetooth does away with wired cabled connections such as serial, parallel, USB and Fire; but also, it presents to us an unified standard that truly makes connecting to devices to each other ubiquitous. There are hundreds if not thousands ways Bluetooth and be used to enhance our daily lives. Aside from entertainment value of playing games head to head in multiplayer mode there are many business solutions for us to explore. Here are a couple of ideas:

1. Efficient and easy way to update your PIM from home to office, where ever you go .
2. Easy to exchange information with others like mobile business cards.
3. Concurrent exchange of data, this comes in handy when a group of people are in meetings or at conferences.
4. Accessing devices such as printers and fax machines, this would definitely come in handy when visiting other offices of your company or client site
5. Monitoring systems, for example if you were a maintenance man doing routine system checks in a factory, it allows you to easily interface at each check point.
6. Going beyond the peer-to-peer use of Bluetooth there is what is called BlipNet used in enterprise scenarios.
7. Profile Holder - This may be best explained with an example, say you are using your buddies gaming console that is Bluetooth enabled you can upload your saved games and download your current game. Another example, you visit your local drug store and beam your prescription and once it is filled out you get notified on your phone this allows you to continue shopping without the hassle of waiting inline or trying to decipher what is being said over the PA system.
8. Provide entertainment during waiting periods, for example waiting in line to buy a ticker form ovieyou could play Bluetooth movie trivia games.

Who invented Bluetooth? Bluetooth was originally researched and developed by the Ericsson organization and were the ones who named the technology after King Harald Blatand (Bluetooth) of Denmark. Ericsson formed the Bluetooth Special Interest Group. Definitely checkout all the products that are Bluetooth enabled, this definitely will if not already provide plenty of opportunity for us developers to make some innovative applications Bluetooth is an always-on, short-range radio hookup that resides on a microchip. It was initially developed by Swedish mobile phone maker Ericsson in 1994 as a way to let laptop computers make calls over a mobile phone. Since then, several thousand companies have signed on to make Bluetooth the low-power short-range wireless standard for a wide range of devices. Industry observers expect Bluetooth to be installed in billions of devices. The Bluetooth standards are published by an industry consortium known as the Bluetooth SIG (special interest group).

The concept behind Bluetooth is to provide a universal short-range wireless capability. Using the 2.4 GHz band, available globally for unlicensed low-power uses, two Bluetooth devices within 10 m of each other can share up to 720 Kbps of capacity. Bluetooth is intended to support an open-ended list of applications, including data (such as schedules and telephone numbers), audio, graphics, and even video. For example, audio devices can include headsets, cordless and standard phones, home stereos, and digital MP3 players. Following are some examples of the capabilities that Bluetooth can provide consumers:

1. Make calls from a wireless headset connected remotely to a cell phone.
2. Eliminate cables linking computers to printers, keyboards, and the mouse.
3. Hook up MP3 players wirelessly to other machines to download music.
4. Set up home networks so that a couch potato can remotely monitor air conditioning, the oven, and children's Internet surfing.
5. Call home from a remote location to turn appliances on and off, set the alarm, and monitor activity.

1.3 What is Bluetooth Technology?

Bluetooth technology is an industry wireless specification standard for use in various devices for short-range communications. As a radio-based technology it allows devices to share information over a maximum range of 10 meters. Bluetooth enables mobile computers, mobile phones, portable handhelds, and the Internet to “talk the talk” without cables. With Bluetooth, devices don't need to be 'looking' at each unlike other wireless technologies (i.e. infrared). As long as two Bluetooth devices are close enough to each other, it’s possible to make a connection. With Bluetooth technology getting connected takes on a whole new meaning.

Bluetooth technology allows a variety of devices, from cell phones to PDAs to desktop computers, to communicate with each other without connecting them via cables. Bluetooth has more applications in the mobile and embedded devices area where, according to industry observers, 80% of mobile phones will support Java by 2006. The reason for this is two-fold: the number of Java developers (and their technology demands) are increasingly on the rise and the standard Application Programming Interface (API) for Bluetooth technology was just defined for the Java programming language in February 2002. This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to create an implementation of a device. With Bluetooth™ technology, all connections are instant and automatic. The tiny Bluetooth™ microchip, incorporating a radio transceiver, is built into the devices and ensures fast and secure transmissions of both voice and data. The radio operates in a globally available frequency band, ensuring compatibility worldwide.

The Bluetooth technology is designed to be fully functional even in a very noisy radio environment, and its voice transmissions are audible under severe conditions.The technology also provides a very high transmission rate, and all data are protected by advanced error-correction methods, as well as encryption and authentication routines for the user’s privacy.

1.4 Bluetooth Tutorial - Profiles

The profiles have been developed in order to describe how implementations of user models are to be accomplished. The user models describe a number of user scenarios where Bluetooth performs the radio transmission. A profile can be described as a vertical slice through the protocol stack. It defines options in each protocol that are mandatory for the profile. It also defines parameter ranges for each protocol. The profile concept is used to decrease the risk of interoperability problems between different manufacturers' products.

Bluetooth specifies a telephony control protocol. TCS BIN (telephony control specification-binary) is a bit-oriented protocol that defines the call control signaling for the establishment of speech and data calls between Bluetooth devices. In addition, it defines mobility-management procedures for handling groups of Bluetooth TCS devices. The adopted protocols are defined in specifications issued by other standards-making organizations and incorporated into the overall Bluetooth architecture. The Bluetooth strategy is to invent only necessary protocols and use existing standards whenever possible.

1.5 There are the adopted protocols

1.5.1 The point-to-point protocol (PPP)

is an Internet standard protocol for transporting IP data-grams over a point-to-point link.

1.5.2 TCP/UDP/IP

These are the foundation protocols of the TCP/IP protocol suite.

1.5.3 OBEX

The object exchange protocol is a session-level protocol developed by the Infrared Data Association (IrDA) for the exchange of objects. OBEX provides functionality similar to that of HTTP, but in a simpler fashion. It also provides a model for representing objects and operations. Examples of content formats transferred by OBEX are vCard and vCalendar, which provide the format of an electronic business card and personal calendar entries and scheduling information, respectively.

1.5.4 WAE/WAP

Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.

1.6 Bluetooth Profiles

Bluetooth Profiles - defined functionality for Bluetooth such as Fax Profile that enables a Bluetooth device to send a fax via Bluetooth fax machine. These profiles may seem similar to the J2ME profiles but they aren't. It isn't an add-on to J2ME but rather an add-on to Bluetooth. Bluetooth profiles can be implemented in other languages like C/C++.

The network between Bluetooth enabled devices is called a PAN, which stands for Personal Area Networks. A PAN can be a Pico net or scatter net, where a Pico net is when there is one master and several slaves. A scatter net consists of 2 or more masters and several slaves, in other words one of the Bluetooth devices is both a master and a slave.

1.7 Current aspects

Bluetooth technology enables a lot of functions to make life easier. It allows you to send files from one mobile computer to another as easily as over a LAN, or to surf the Internet regardless of your location.

By installing a Bluetooth network at your office, you will no longer be bound to certain locations for connection and you don't need to draw new cables for new installations.

1.8 Future aspects

Because Bluetooth wireless technology can be used for a variety of purposes, it will also potentially replace multiple cable connections via a single radio link. This creates the possibility of using mobile data in a different way for different applications, such as "surfing on the sofa", "three in one phone", and many others.

1.9 Summary

Bluetooth wireless technology is finally here. Originally conceived as a low-power short range radio technology designed to replace cables for interconnecting devices such as printers, keyboards, and mice, its perceived potential has evolved into far more sophisticated usage models. The requirement to do this in a totally automated, seamless, and user-friendly fashion, without adding appreciable cost, weight, or power drain to the associated host is an enormous engineering challenge. Bluetooth devices can form piconets of up to seven slaves and one master, enabling discovery of services and subsequent implementation of many varied usage models including wireless headsets, Internet bridges, and wireless operations such as file exchange, data synchronization, and printing. Despite talk of Bluetooth competing with wireless LANs, Bluetooth products work over shorter distances and are designed to solve different problems. The Bluetooth SIG publishes the Bluetooth specification. The IEEE has formed the working group to define standards for wireless PANs.

2. WIRELESS

2.1 Wireless Overview

WLAN technology and the WLAN industry date back to the mid-1980s when the Federal Communications Commission (FCC) first made the RF spectrum available to industry. During the 1980s and early 1990s, growth was relatively slow. Today, however, WLAN technology is experiencing tremendous growth. The key reason for this growth is the increased bandwidth made possible by the IEEE 802.11 standard. As an introduction to the 802.11 and WLAN technology.

2.2 Wireless Technology

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. A brief overview of wireless networks, devices, standards, and security issues is presented in this section.

2.3 Wireless Networks

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and IR. All of these technologies are "tetherless" they receive and transmit information using electromagnetic (EM) waves. Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to and above the IR band. The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum. for a list of common wireless frequencies.) This document focuses on WLAN and WPAN technologies.

2.4 Brief History

Motorola developed one of the first commercial WLAN systems with its Altair product. However, early WLAN technologies had several problems that prohibited its pervasive use. These LANs were expensive, provided low data rates, were prone to radio interference, and were designed mostly to proprietary RF technologies. The IEEE initiated the 802.11 project in 1990 with a scope "to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area." In 1997, IEEE first approved the 802.11 international interoperability standard. Then, in 1999, the IEEE ratified the 802.11a and the 802.11b wireless networking communication standards. The goal was to create a standards-based technology that could span multiple physical encoding types, frequencies, and applications. The 802.11a standard uses orthogonal frequency division multiplexing (OFDM) to reduce interference. This technology uses the 5 GHz frequency spectrum and can process data at up to 54 Mbps. Although this section of the document focuses on the IEEE 802.11 WLAN standard, it is important to note that several other WLAN technologies and standards are available from which consumers may choose, including HiperLAN and HomeRF. For information on the European Telecommunications Standards Institute (ETSI) developed

HiperLAN, For more information on HomeRF, This document does not address those technologies.

2.5 Frequency and Data Rates

IEEE developed the 802.11 standards to provide wireless networking technology like the wired Ethernet that has been available for many years. The IEEE 802.11a standard is the most widely adopted member of the 802.11 WLAN family. It operates in the licensed 5 GHz band using OFDM technology. The popular 802.11b standard operates in the unlicensed 2.4 GHz–2.5 GHz Industrial, Scientific, and Medical (ISM) frequency band using a direct sequence spread-spectrum technology. The ISM band has become popular for wireless communications because it is available worldwide. The 802.11b WLAN technology permits transmission speeds of up to 11 Mbits per second. This makes it considerably faster than the original IEEE standard (that sends data at up to 2 Mbps) and slightly faster than standard Ethernet.

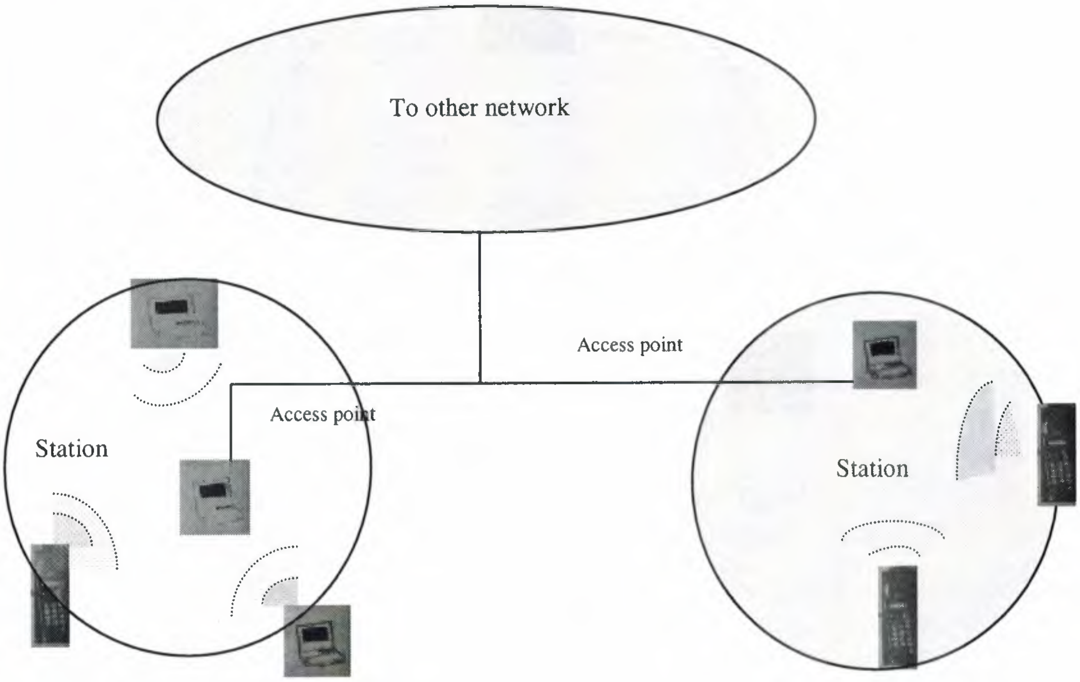


Figure 2.1 Fundamental 802.11 Wireless LAN Topology

Although most WLANs operate in the "infrastructure" mode and architecture described above, another topology is also possible. This second topology, the ad hoc network, is meant to easily interconnect mobile devices that are in the same area (e.g., in the same room). In this architecture, client stations are grouped into a single geographic area and can be Internet-worked without access to the wired LAN (infrastructure network). The interconnected devices in the ad hoc mode are referred to as an independent basic service set (IBSS). The ad hoc topology is depicted in Figure 2.2 below.

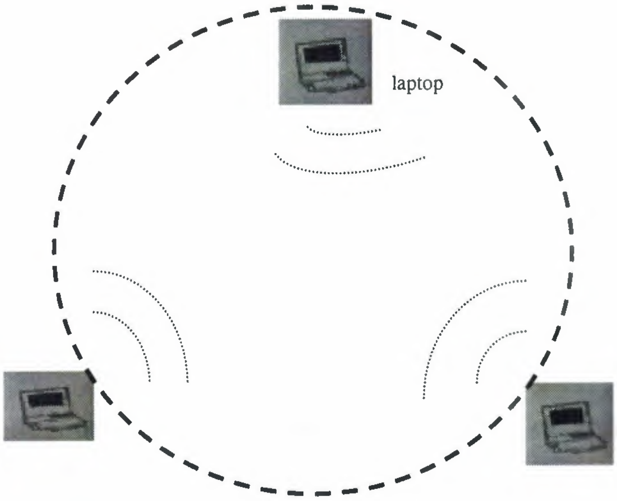


Figure 2.2 802.11 Wireless LAN Ad Hoc Topology

The ad hoc configuration is similar to a peer-to-peer office network in which no node is required to function as a server. As an ad hoc WLAN, laptops, desktops and other 802.11 devices can share files without the use of an AP.

2.6 Wireless LAN Components

A WLAN comprises two types of equipment: a wireless station and an access point. A station, or client, is typically a laptop or notebook personal computer (PC) with a wireless NIC. A WLAN client may also be a desktop or handheld device or equipment within a kiosk on a manufacturing floor or other publicly accessed area. Wireless laptops and notebooks "wireless enabled" are identical to laptops and notebooks except that they use wireless NICs to connect to access points in the network. The wireless NIC is commonly inserted in the client's Personal Computer Memory Card International Association (PCMCIA) slot or Universal Serial Bus (USB) port. The NICs use radio signals to establish connections to the WLAN. The AP, which acts as a bridge between the wireless and wired networks, typically comprises a radio, a wired network interface such as 802.3, and bridging software. The AP functions as a base station for the wireless network, aggregating multiple wireless stations onto the wired network.

2.6.1 Wireless LANs

WLANs allow greater flexibility and portability than do traditional wired local area networks (LAN). Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point device. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users to even "roam" within a building or between buildings.

2.6.2 Ad Hoc Networks

Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops, and PDAs. These networks are termed "ad hoc" because of their shifting network topologies. Whereas WLANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a master-slave system connected by wireless links to enable devices to communicate. In a Bluetooth network, the master of the piconet controls the changing network topologies of these networks. It also controls the flow of data between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing that protocol Bluetooth employs allows the master to establish and maintain these shifting networks. Figure 2.3 illustrates an example of a Bluetooth-enabled mobile phone connecting to a mobile phone Network.

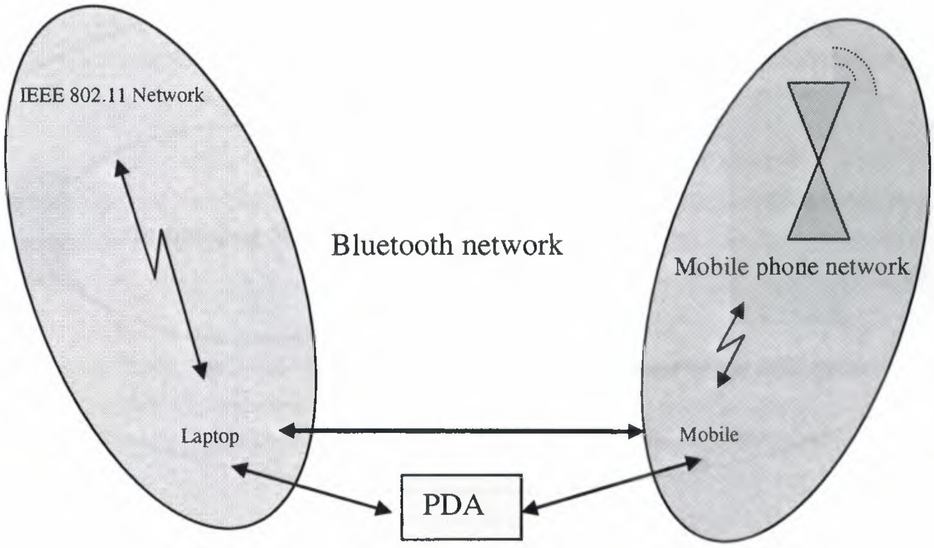


Figure 2.3 National Ad Hoc Network

2.7 Range

The reliable coverage range for 802.11 WLANs depends on several factors, including data rate required and capacity, sources of RF interference, physical area and characteristics, power, connectivity, and antenna usage. Theoretical ranges are from 29 meters (for 11 Mbps) in a closed office area to 485 meters (for 1 Mbps) in an open area. However, through empirical analysis, the typical range for connectivity of 802.11 equipment is approximately 50 meters indoors. A range of 400 meters, nearly ¼ mile, makes WLAN the ideal technology for many campus applications. It is important to recognize that special high-gain antennas can increase the range to several miles.

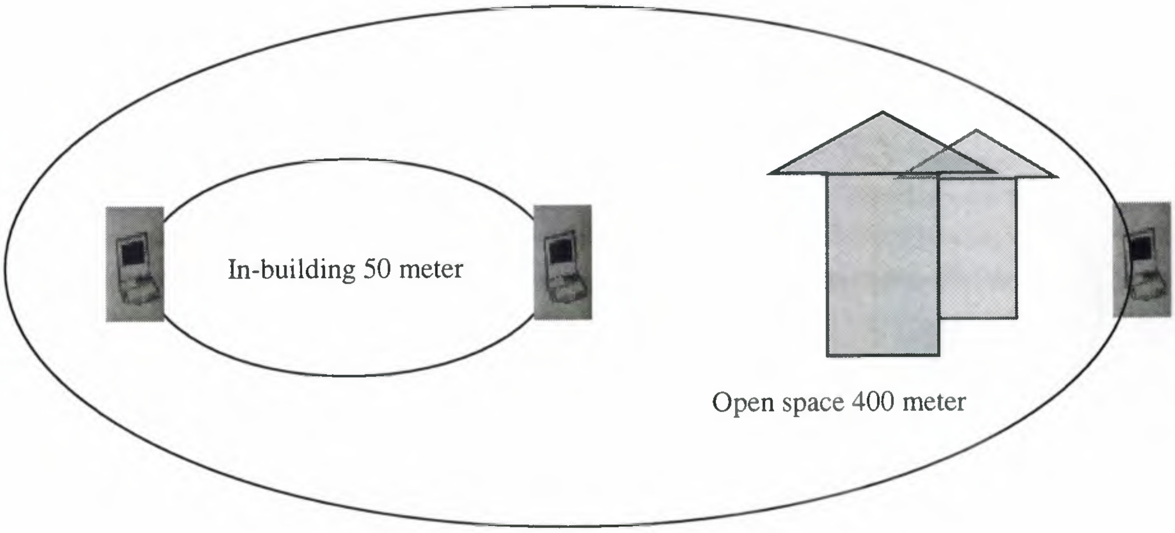


Figure 2.4 Typical Range of 802.11

APs may also provide a “bridging” function. Bridging connects two or more networks Bridging involves either a point-to-point or a multipoint configuration. In a point-to-point architecture, two LANs are connected to each other via. LANs’ respective APs. In multipoint bridging, one subnet on a LAN is connected to several other subnets on another LAN via each subnet AP. For example, if a computer on Subnet A needed to connect to computers on Subnets B, C, and D, Subnet A’s AP would connect to B’s, C’s, and D’s respective APs. Enterprises may use bridging to connect LANs between different buildings on corporate campuses. Bridging AP devices are typically placed on top of buildings to achieve greater antenna reception. The typical distance over which one AP can be connected wirelessly to another by means of bridging is approximately 2 miles. This distance may vary depending on several factors including the specific receiver or transceiver being used. Figure 2.5 illustrates point-to-point bridging between two LANs. In the example, wireless data is being transmitted from Laptop A to Laptop B, from one building to the next, using each building’s appropriately positioned AP. Laptop A connects to the closest AP within the building A. The receiving AP in building A then transmits the data to AP bridge located on the building’s roof. That AP bridge then transmits the data to the bridge on nearby building B. The building AP bridge then sends the data over its wired LAN to Laptop B.

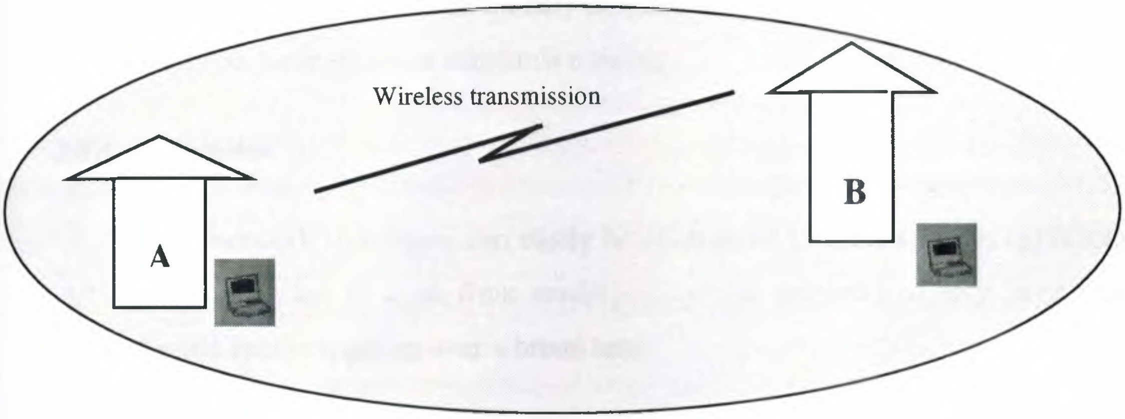


Figure 2.5 Access Point Briding

2.8 Benefits

WLANs offer four primary benefits:

2.8.1 User Mobility

Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN.

2.8.2 Rapid Installation

The time required for installation is reduced because network connections can be made without moving or adding wires, or pulling them through walls or ceilings, or making modifications to the infrastructure cable plant. For example, WLANs are often cited as making LAN installations possible in buildings that are subject to historic preservation rules.

2.8.3 Flexibility

Enterprises can also enjoy the flexibility of installing and taking down WLANs in locations as necessary. Users can quickly install a small WLAN for temporary needs such as a conference, trade show, or standards meeting.

2.8.4 Scalability

WLAN network topologies can easily be configured to meet specific application and installation needs and to scale from small peer-to-peer networks to very large enterprise networks that enable roaming over a broad area.

2.9 Wireless Devices

A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. This document discusses the most commonly used wireless handheld devices such as textmessaging devices, PDAs, and smart phones.

2.9.1 Personal Digital Assistants

PDAs are data organizers that are small enough to fit into a shirt pocket or a purse. PDAs offer applications such as office productivity, database applications, address books, schedulers, and to-do lists, and they allow users to synchronize data between two PDAs and between a PDA and a personal computer. Newer versions allow users to download their e-mail and to connect to the Internet. Security administrators may also encounter one-way and two-way text-messaging devices. These devices operate on a proprietary networking standard that disseminates e-mail to remote devices by accessing the corporate network. Text-messaging technology is designed to monitor a user's inbox for new e-mail and relay the mail to the user's wireless handheld device via the Internet and wireless network.

2.9.2 Smart Phones

Mobile wireless telephones, or cell phones, are telephones that have shortwave analog or digital transmission capabilities that allow users to establish wireless connections to nearby transmitters. As with WLANs, the transmitter's span of coverage is called a “cell.” As the cell phone user moves from one cell to the next, the telephone connection is effectively passed from one local cell transmitter to the next. Today’s cell phone is rapidly evolving to integration with PDAs, thus providing users with increased wireless e-mail and Internet access. Mobile phones with information-processing and data networking capabilities are called “smart phones.” This document addresses the risks introduced by the information-processing and networking capabilities of smart phones.

2.10 Wireless Standards

Wireless technologies conform to a variety of standards and offer varying levels of security features. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to interoperate. For this document, the discussion of wireless standards is limited to the IEEE 802.11 and the Bluetooth standard. WLANs follow the IEEE 802.11 standards. Ad hoc networks follow proprietary techniques or are based on the Bluetooth standard, which was developed by a consortium of commercial companies making up the Bluetooth Special Interest Group (SIG). These standards are described below.

2.10.1 IEEE 802.11

WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1997. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations. 802.11 is the original WLAN standard, designed for 1 Mbps to 2 Mbps wireless transmissions. It was followed in 1999 by 802.11a, which established a high-speed WLAN standard for the 5 GHz band and supported 54 Mbps. Also completed in 1999 was the 802.11b standard, which operates in the 2.4 - 2.48 GHz band and supports 11 Mbps. The 802.11b standard is currently the dominant standard for WLANs, providing sufficient speeds for most of today's applications. Because the 802.11b standard has been so widely adopted, the security weaknesses in the standard have been exposed. These weaknesses will be discussed in Section 3.3.2. Another standard, 802.11g, still in draft, operates in the 2.4 GHz waveband, where current WLAN products based on the 802.11b standard operate. Two other important and related standards for WLANs are 802.1X and 802.11i. The 802.1X, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard, also still in draft, was created for wireless-specific security functions that operate with IEEE 802.1X.

2.11 Wireless Security Threats and Risk Mitigation

The NIST handbook An Introduction to Computer Security generically classifies security threats in nine categories ranging from errors and omissions to threats to personal privacy. *6* All of these represent potential threats in wireless networks as well. However, the more immediate concerns for wireless communications are device theft, denial of service, malicious hackers, malicious code, theft of service, and industrial and foreign espionage. Theft is likely to occur with wireless devices because of their portability. Authorized and unauthorized users of the system may commit fraud and theft; however, authorized users are more likely to carry out such acts. Since users of a system may know what resources a system has and the system's security flaws, it is easier for them to commit fraud and theft. Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Malicious hackers are generally individuals from outside of an agency or organization (although users within an agency or organization can be a threat as well). Such hackers may gain access to the wireless network access point by eavesdropping on wireless device communications. Malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or bring down a system. Theft of service occurs when an unauthorized user gains access to the network and consumes network resources. Industrial and foreign espionage involves gathering proprietary data from corporations or intelligence information from governments through eavesdropping. In wireless networks, the espionage threat stems from the relative ease with which eavesdropping can occur on radio transmissions. Attacks resulting from these threats, if successful, place an agency's systems and, more importantly, its data at risk. Ensuring confidentiality, integrity, authenticity, and availability are the prime objectives of all government security policies and practices. Security Self-Assessment Guide for Information Technology System*s*, states that information must be protected from unauthorized, unanticipated, or unintentional modification. Security requirements include the following:

2.11.1 Authenticity

A third party must be able to verify that the content of a message has not been changed in transit.

2.11.2 Nonrepudiation

The origin or the receipt of a specific message must be verifiable by a third party.

2.11.3 Accountability

The actions of an entity must be traceable uniquely to that entity.

2.12 Privacy

The 802.11 standard supports privacy (confidentiality) through the use of cryptographic techniques for the wireless interface. The WEP cryptographic technique for confidentiality also uses the RC4 symmetric key, stream cipher algorithm to generate a pseudo-random data sequence. This "key stream" is simply added modulo 2 (exclusive-OR-ed) to the data to be transmitted. Through the WEP technique, data can be protected from disclosure during transmission over the wireless link. WEP is applied to all data above the 802.11 WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hyper Text Transfer Protocol (HTTP). As defined in the 802.11 standard, WEP supports only a 40-bit cryptographic keys size for the shared key. However, numerous vendors offer nonstandard extensions of WEP that support key lengths from 40 bits to 104 bits. At least one vendor supports a keysize of 128 bits. The 104-bit WEP key, for instance, with a 24-bit Initialization Vector (IV) becomes a 128-bit RC4 key. In general, all other things being equal, increasing the key size increases the security of a cryptographic technique. However, it is always possible for flawed implementations or flawed designs to prevent long keys from increasing security. Research has shown that key sizes of greater than 80-bits, for robust designs and implementations, make brute-force cryptanalysis (code breaking) an impossible task. For 80-bit keys, the number of possible keys a keyspace of more than 1026 exceeds contemporary computing power. In practice, most WLAN deployments rely on 40-bit keys. Moreover, recent attacks have shown that the WEP approach for privacy is, unfortunately, vulnerable to certain attacks regardless of keysize. However, the cryptographic, standards, and vendor WLAN communities have developed enhanced WEP, which is available as a prestandard vendor-specific implementations. The attacks mentioned above are described later in the following sections. The WEP privacy is illustrated conceptually in Figure 2.6.

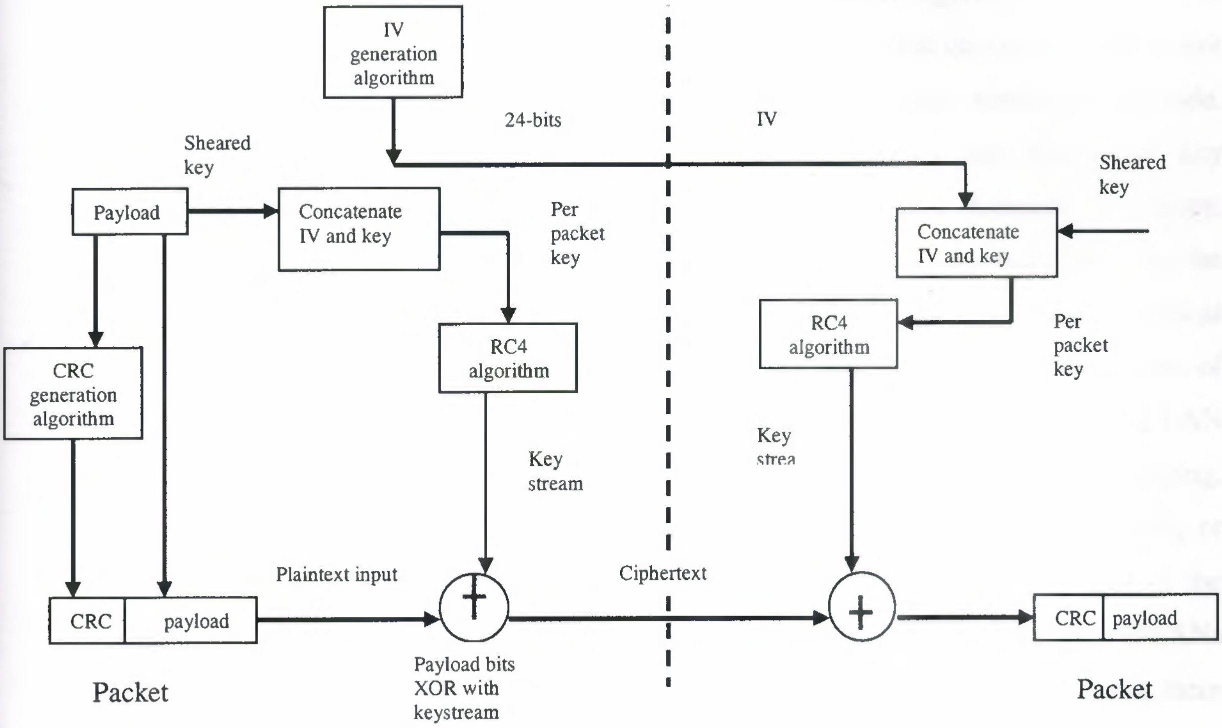


Figure 2.6 WEP Privacy Using RC4 Algorithm

2.13 Integrity

The IEEE 802.11 specification also outlines a means to provide data integrity for messages transmitted between wireless clients and access points. This security service was designed to reject any messages that had been changed by an active adversary “in the middle.” This technique uses a simple encrypted Cyclic Redundancy Check (CRC) approach. As depicted in the diagram above, a CRC-32, or frame check sequence, is computed on each payload prior to transmission. The integrity-sealed packet is then encrypted using the RC4 key stream to provide the cipher-text message. On the receiving end, decryption is performed and the CRC is recomputed on the message that is received. The CRC computed at the receiving end is compared with the one computed with the original message. If the CRCs do not equal, that is, “received in error,” this would indicate an integrity violation and the packet would be discarded. As with the privacy service, unfortunately, the 802.11 integrity is vulnerable to certain attacks regardless of key size. In summary, the fundamental flaw in the WEP integrity scheme is that the simple CRC is not a “cryptographically secure” mechanism such as a hash or message authentication code. The IEEE 802.11 specification does not, unfortunately, identify any means for key management (life cycle handling of cryptographic keys and related material). Therefore, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material is left to those deploying WLANs. Key management (probably the most critical aspect of a cryptographic system) for 802.11 is left largely as an exercise for the users of the 802.11 network. As a result, many vulnerabilities could be introduced into the WLAN environment. These vulnerabilities include WEP keys that are non-unique, never changing, factory-defaults, or weak keys (all zeros, all ones, based on easily guessed passwords, or other similar trivial patterns). Additionally, because key management was not part of the original 802.11 specification, with the key distribution unresolved, WEP-secured WLANs do not scale well. If a enterprise recognizes the need to change keys often and to make them random, the task is formidable in a large WLAN environment. For example, a large campus may have as many as 15,000 APs. Generating, distributing, loading, and managing keys for an environment of this size is a significant challenge. It is has been suggested that the only practical way to distribute keys in a large dynamic environment is to publish it. However, a fundamental tenet of cryptography is that cryptographic keys remain secret. Hence we have a major dichotomy. This dichotomy exists for any technology that neglects to elegantly address the key distribution problem.

3.14 Security Requirements and Threats

As discussed above, the 802.11 WLAN or WiFi industry is burgeoning and currently has significant momentum. All indications suggest that in the coming years numerous organizations will deploy 802.11 WLAN technology. Many organizations including retail stores, hospitals, airports, and business enterprises plan to capitalize on the benefits of "going wireless." However, although there has been tremendous growth and success, everything relative to 802.11 WLANs has not been positive. There have been numerous published reports and papers describing attacks on 802.11 wireless networks that expose organizations to security risks. This subsection will briefly cover the risks to security-i.e.,

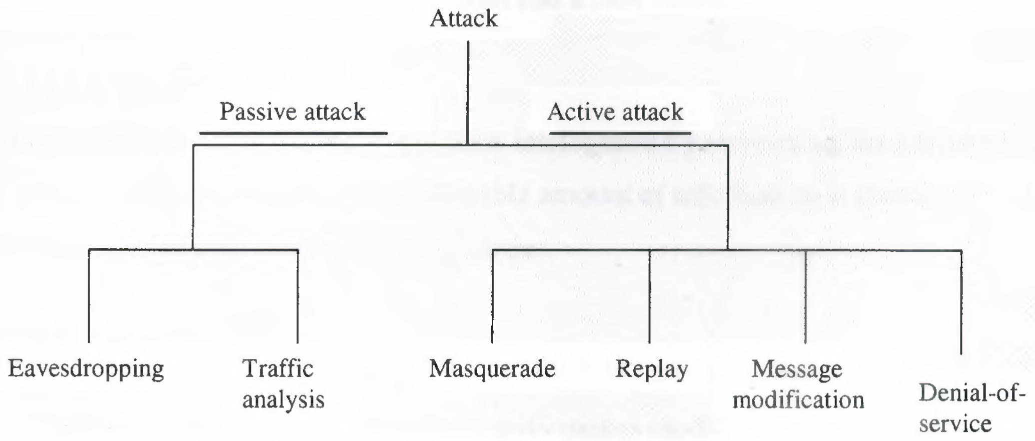


Figure 2.7 Taxonomy of Security Attacks

attacks on confidentiality, integrity, and network availability. Figure 2.7 provides a general taxonomy of security attacks to help organizations and users understand some of the attacks against WLANs.

Network security attacks are typically divided into passive and active attacks. These two broad classes are then subdivided into other types of attacks. All are defined below.

2.14.1 Passive Attack

An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.

2.14.1.1 Eavesdropping

The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

2.14.1.2 Traffic analysis

The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

2.14.2 Active Attack

An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below.

2.14.2.1 Masquerading

The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

2.14.2.2 Replay

The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

2.14.2.3 Message modification

The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

2.14.2.4 Denial-of-service

The attacker prevents or prohibits the normal use or management of communications facilities.

2.15 Risk Mitigation

Government agencies can mitigate risks to their WLANs by applying countermeasures to address specific threats and vulnerabilities. Management countermeasures combined with operational and technical countermeasures can be effective in reducing the risks associated with WLANs. The following guidelines will not prevent all adversary penetrations, nor will these countermeasures necessarily guarantee a secure wireless networking environment. This section describes risk-mitigating steps for an agency, recognizing that it is impossible to remove all risks. Additionally, it should be clear that there is no "one size fits all solution" when it comes to security. Some agencies may be able or willing to tolerate more risk than others. Also, security comes at a cost: either in money spent on security equipment, in inconvenience and maintenance, or in operating expenses. Some agencies may be willing to accept risk because applying various countermeasures may exceed financial or other constraints.

2.16 Summary

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot. The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

3. BLUETOOTH

3.1 Bluetooth Overview

Ad hoc networks today are based primarily on Bluetooth technology. Bluetooth is an open standard for short-range digital radio. It is touted as a low-cost, low-power, and low-profile technology that provide a mechanism for creating small wireless networks on an ad hoc basis. Bluetooth is considered a wireless PAN technology that offers fast and reliable transmission for both voice and data. Undeterred Bluetooth devices will eliminate the need for cables and provide a bridge to existing networks.

3.2 Bluetooth

Bluetooth is a wireless communications and networking technology designed to eliminate cables between computers and cell phones, printers, scanners, digital cameras and other such peripherals. Bluetooth technology supports both voice and data. In the words of the official Bluetooth web site, this technology enables "users to connect a wide range of computing and telecommunications devices easily and simply, without the need to buy, carry, or connect cables". Because Bluetooth wireless technology can be used for a variety of purposes, it should eventually replace multiple cable connections with a single radio link. In summary, as noted at the Ericsson Bluetooth site "Bluetooth wireless technology is a low-cost, low-power, short-range radio link for mobile devices and for WAN/LAN access points". It offers "fast and reliable digital transmissions of both voice and data over the globally available 2.4 GHz ISM (Industrial, Scientific and Medical) band." From the idea of simply replacing cables, Bluetooth technology soon evolved to become more diversified, to become "a universal bridge to existing data networks, a peripheral interface, and a mechanism to form small private ad hoc groupings of connected devices away from fixed network infrastructures.

3.3 Bluetooth works

3.3.1 Network Topology

Any Bluetooth device can be a master or a slave, depending on the application scenario. Bluetooth employs frequency hopping spread spectrum (FHSS) to communicate. So in order for multiple Bluetooth devices to communicate, they must all synchronize to the same hopping sequence. The master sets the hopping sequence, and the slaves synchronize to the Master.

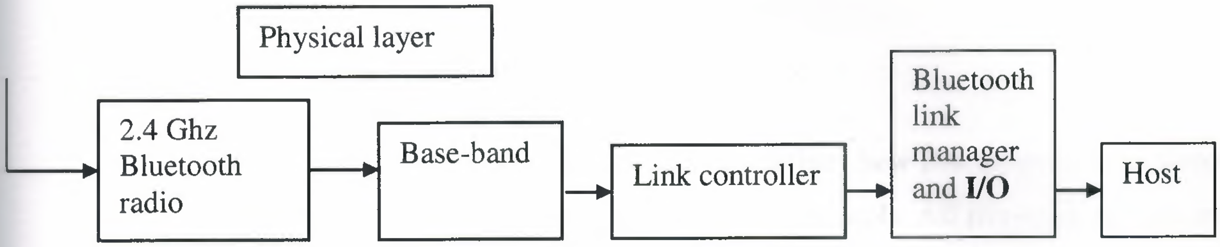


Figure 3.1 Functional Block of Bluetooth System

A scatter net can be formed by linking two or more piconets. When a device is present in more than one piconet, it must time-share and synchronize to the master of the piconet with which it is currently communicating. While the topology and hierarchical structure of WLAN networks are relatively simple, Bluetooth networks are far more diverse and dynamic. They are constantly being formed, modified, and dissolved, as Bluetooth devices move in and out of range of one another. And because different Bluetooth devices can represent many different usage profiles, there are many different ways in which Bluetooth devices can interact.

3.3.2 Service Discovery

The concept of service discovery is utilized to determine what kind of Bluetooth devices are present and what services they desire or offer. When a Bluetooth device requires a service, it begins a discovery process by sending out a query for other Bluetooth devices and the information needed to establish a connection with them. Once other Bluetooth devices are found and communication is established, the Service Discovery Protocol (SDP) is utilized to determine what services are supported and what kinds of connections should be made. In order for the above to happen, devices willing to connect must be located. Some devices may be set up so that they are invisible. In this case, they can scan for other Bluetooth devices, but will not respond if they are likewise queried. Applications determine whether a device is connectable or discoverable, and thus applications determine the topologies of networks and their internal hierarchies.

3.4 Bluetooth profiles

3.4.1 General Access Profile (GAP)

This profile is required by all usage models and defines how Bluetooth devices discover and connect to one another, as well as defines security protocols. All Bluetooth devices must conform to at least the GAP to ensure basic interoperability between devices.

3.4.2 Service Discovery Application Profile (SDAP)

The SDAP uses parts of the GAP to define the discovery of services for Bluetooth devices.

3.4.3 Serial Port Profile

This profile defines how to set up and connect virtual serial ports between two devices. This serial cable emulation can then be used for tasks such as data transfer and printing.

3.4.4 Generic Object Exchange Profile (GOEP)

GOEP is dependent on the Serial Port Profile and is used by applications to handle object exchanges. This capability is then used, in turn, by other profiles to perform such functions as Object Push, File Transfer, and Synchronization .

3.4.5 Object Push

This profile is used for the exchange of small objects, such as electronic calling cards.

3.4.6 File Transfer

This profile is used to transfer files between two Bluetooth devices.

3.4.7 Synchronization

This profile is used to synchronize calendars and address information between devices.

3.4.8 Power Levels and Range

Most Bluetooth devices, dependent on batteries for power, are designated as class 3 devices and are designed to operate at a power level of 0 dBm (1 mW), which provides a range of up to 10 m. Class 2 devices can utilize as much as 4 dBm (2.5 mW) output power, and class 1 devices can utilize up to 20 dBm (100 mW) of output power. Class 1 devices can have a range up to 100 m. Bluetooth class 2 and 3 devices can optionally implement adaptive power control. Required for class 1 devices, this mechanism allows a Bluetooth radio to reduce power to the minimum level required to maintain its link, thus saving power and reducing the potential for interfering with other nearby networks.

3.5 Protocol Architecture

Bluetooth is defined as a layered protocol architecture consisting of core protocols, cable replacement and telephony control protocols, and adopted protocols. The core protocols are as following:

3.5.1 Radio

Specifies details of the air interface, including frequency, the use of frequency hopping, modulation scheme, and transmit power.

3.5.2 Base-band

Concerned with connection establishment within a Pico net, addressing, packet format, timing, and power control.

3.5.3 Link manager protocol (LMP)

Responsible for link setup between Bluetooth devices and ongoing link management. This includes security aspects such as authentication and encryption, plus the control and negotiation of base-band packet sizes.

3.5.4 Logical link control and adaptation protocol (L2CAP)

Adapts upper-layer protocols to the base-band layer. L2CAP provides both connectionless and connection-oriented services.

3.5.5 Service discovery protocol (SDP)

Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices. RFCOMM is the cable replacement protocol included in the Bluetooth specification. RFCOMM presents a virtual serial port that is designed to make replacement of cable technologies as transparent as possible. Serial ports are one of the most common types of communications interfaces used with computing and communications devices. Hence, RFCOMM enables the replacement of serial port cables with the minimum of modification of existing devices. RFCOMM provides for binary data transport and emulates EIA-232 control signals over the Bluetooth base-band layer. EIA-232 (formerly known as RS-232) is a widely used serial port interface standard.

3.6 The Evolving Bluetooth Standard

3.6.1 The Bluetooth SIG

Since the original Bluetooth specification was published in 1999, more than 2000 additional companies have signed on as associate members, able to participate in development of future standards and extensions by contributing efforts to various working groups.

3.6.2 The Current Specification

The current specification, Ver. 1.1$_2$, defines a radio which operates in the unregulated Industrial, Scientific, and Medical (ISM) band as 2.4 GHz, FHSS w/1600 hops/s over 79 channels: 1 Mbps

The fundamental elements of a Bluetooth product are defined in the two lowest protocol layers, the *radio layer* and the base-band layer. Included in these layers are hardware tasks such as frequency hopping control and clock synchronization, as well as packet assembly with associated FEC (Forward Error Correction) and ARQ (Automatic Repeat Request). The *link manager layer* is responsible for searching for other Bluetooth devices, creating and tearing down piconets, as well as authentication and encryption. Higher layer definitions include the Bluetooth profiles.

3.7 Bluetooth Communication

3.7.1 Connectivity

Bluetooth allows users to connect to a wide range of devices at one time without cables, and potentially without actively initiating the connection. For example, your PDA could automatically update a copy of your schedule stored on a desktop PC the minute you walked into your office. This connectivity is enabled by a tiny microchip incorporating a radio transceiver that is built into Bluetooth devices. This radio transceiver provides the advantage of being effective through obstacles. Thus, you could ostensibly use a Bluetooth connection to send data from a computer in one room to a printer in the next--right through the wall.

One concern when using such a system is privacy. As Bluetooth operates in the globally available 2.4 GHz frequency, it is conceivable that an unintended recipient could intercept a signal. To combat this, all Bluetooth devices are keyed for their own networks. The transmissions use a sophisticated encoding specification that not only guards against interference, it also ensures that only devices specifically programmed to receive a broadcast will be able to decode it.

Bluetooth uses a flexible, multiple piconet structure for communication. It supports both point-to-point and multipoint connections for full-duplex networks. Currently up to seven slave devices can be configured to use a master radio in one device. Several of the piconets can be established and linked in scatternets to allow flexibility among configurations. Devices in the same piconet have priority synchronizations, but other devices can enter the network at any time. In a full-duplex network, a multiple piconet structure with 10 fully loaded, independent piconets, can maintain aggregate data transfer speeds of up to 6 Mbps.

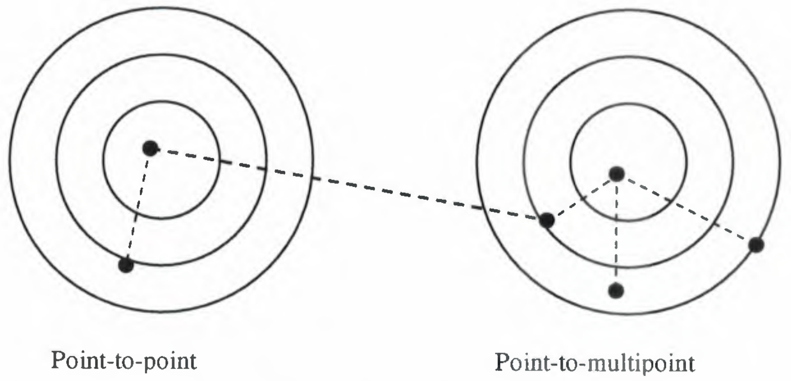


Figure 3.2 Bluetooth piconet communication structure

3.7.2 Class 1 and Class 2 Bluetooth

The major difference between the 2 classes of Bluetooth h adapter is communication range and power requirements. As a rule, you will typically trade power consumption for distance (though all Bluetooth devices typically have low power requirements relative to other types of computer add-in devices.) Class 2 Bluetooth devices have a communication range of 10 meters (30 feet), and Class 1 adapters provide a communication range of 100 meters (300 feet).

3.7.3 High and Low Power

The Bluetooth specification implements two power levels: a low power level designed for short distance communication such as within an office (Class 2), and a high power level that can accommodate a medium range, such as an entire building (Class 1). Additionally, Bluetooth limits power output to exactly what the device requires at any given time. For instance, when two devices connect and determine that they are close together, the transmitter immediately modifies its signal to the strength needed to accommodate that range. When traffic volume across a connection slows down, or stops completely, a receiving device will shift to a low power sleep mode that is intermittently interrupted for very short periods in order to maintain the network connection. With these power saving features, Bluetooth devices consume very small amounts of power, making them ideal for portable applications.

3.7.4 Bluetooth for Data Communication

Bluetooth technology makes data communication fast, easy, and convenient. As speeds and distances are currently limited, it should be viewed as a short-range solution for low to medium speed applications. It does provide remarkable flexibility, by communicating through walls and other obstacles, that makes it an ideal choice for home or office networks--for example sharing a printer among multiple PCs located in different rooms on the same floor. It also expands the functionality of a mobile phone, allowing it to serve as a modem for Internet connections, or allowing it to communicate with other devices--such as the prospect of using mobile phones to purchase drinks from vending machines.

3.8 Bluetooth Transmission Technologies

The dream for true, seamless, mobile data and voice communications that enables constant connectivity anywhere is quickly becoming a reality. Wireless and computer industries are clearly leading the way with revolutionary components that will shape our lives in the next century. In 1994, Ericsson Mobile Communications initiated a study to investigate the feasibility of a low power, low cost radio interface between mobile phones and their accessories. The aim of this study was to eliminate cables between mobile phones and PC Cards used to connect the phones to a computer for dial up networks (DUN). In 1998 Intel, IBM, Toshiba, Ericsson and Nokia began developing a technology that would allow users to easily connect to mobile devices without cables. This technological vision became a reality through the synergy of market leaders in laptop computing, telecommunications, and core digital signal processing. May 20th, 1998 marked the formation of the Bluetooth Special Interest Group (SIG) with the goal to design a royalty free, open specification, de facto, short range, low power wireless communication standard, as well as a specification for small-form factor, low-cost, short range radio links between mobile PCs, mobile phones and other portable devices codenamed Bluetooth. The result was an open specification for a technology to enable short-range wireless voice and data communications anywhere in the world. A simple 8 way to connect and communicate without wires or cables between electronic devices including computers, PDA's, cell-phones, network access and peripherals. Bluetooth is named after Herald Blatant, “Bluetooth”, a Viking 10th century king. Herald had a penchant for surrounding himself with the right group of people, which enabled him to strategically secure new lands for Viking settlements. Herald conquered all of Denmark and Norway and made the Danes Christian. Thus Herald's conquest inspired the name of a global wireless specification achieved through the cooperation of many leading companies within the computer and telecommunications industries. The technology operates in a globally available frequency band ensuring communication compatibility worldwide. One of the primary advantages of the Bluetooth system is ease of computer

vendor product integration. Other key benefits of this technology are low power, long battery life, low cost, low complexity, and wireless connectivity for personal space, peer-to-peer, cable replacement, and seamless and ubiquitous connectivity. To achieve the Bluetooth goal, tiny, inexpensive, short-range transceivers are integrated into devices either directly or through an adapter device such as a PC Card. Add on devices such as a USB or Parallel port connections are also available for legacy systems. By establishing links in a more convenient manner this technology will add tremendous benefits to the ease of sharing data between devices.

3.9 Bluetooth application

Bluetooth is designed to operate in an environment of many users. Up to eight devices can communicate in a small network called a piconet. Ten of these piconets can coexist in the same coverage range of the Bluetooth radio. To provide security, each link is encoded and protected against eavesdropping and interference. Bluetooth provides support for three general application areas using short-range wireless connectivity:

3.9.1 Data and voice access point

Bluetooth facilitates real-time voice and data transmissions by providing effortless wireless connection of portable and stationary communications devices.

3.9.2 Cable replacement

Bluetooth eliminates the need for numerous, often proprietary cable attachments for connection of practically any kind of communications device. Connections are instant and are maintained even when devices are not within line of sight. The range of each radio is approximately 10 m, but can be extended to 100 m with an optional amplifier.

3.9.3 Ad hoc networking

A device equipped with a Bluetooth radio can establish instant connection to another Bluetooth radio as soon as it comes into range.

3.10 Bluetooth Security

Bluetooth security, when compared with WLAN security, is both more complex and simpler. It is more complex in the sense that there are many different options for security based on different application scenarios. It is simpler in the sense that, for the most part, they are transparent to the user. With WLANs it is up to the network administrator to add security at higher levels. With Bluetooth, since the Bluetooth spec includes all levels, higher-level security features are already built into the devices when appropriate. Bluetooth security includes both authentication and confidentiality, and is based around the SAFER+ encryption algorithm. SAFER+ is a block cipher, but in this application is implemented as a stream cipher. SAFER+ was thoroughly analyzed and tested during the NIST's search for a national encryption standard. Although some versions were found to have very minor weaknesses, the 128-bit version as used in Bluetooth is considered very strong.

3.10.1 Link layer security – keys and more keys

The Bluetooth Base-band (link layer) specification defines methods for both authentications and encryption that are subsequently utilized by higher layers. These methods utilize a number of keys generated by a process that begins with three basic device entities: a public 48-bit device address, a random number generator, and a secret PIN which is either built into the unit by the manufacturer or programmed by the user. A typical PIN may consist of just four decimal digits. However, for applications requiring more security a PIN code up to 128-bits long can be entered.

The first of many keys is created the first time the Bluetooth device is installed on the host and is typically never changed. This is referred to as the unit key.

3.10.2 Authentication

When a Bluetooth session (defined as the time interval for which the device is part of a piconet) is initiated, a series of additional keys is generated. One of these keys, referred to as the link key or authentication key, is a one-time 128-bit secret key that is used only

during that session. The process of authentication employs the encryption of a random number by each device to verify that each is sharing the same secret link key.

3.10.3 Encryption

If encryption is required by the application, an encryption key is further derived from the link key, a ciphering offset number, and a random number. While the authentication key is always 128-bits, the encryption key may be shorter to accommodate government restrictions on encryption, which vary from country to country. A new encryption key is generated each time the device enters encryption mode. The authentication key, however, is used during the entire session.

3.10.4 Application layer security

The Bluetooth General Access Profile defines three security modes: Mode 1 is non-secure. Authentication is optional. Mode 2 gives service-level enforced security. The service provided by the application decides whether or not authentication or encryption is required. The Bluetooth SIG has published the Bluetooth Security Architecture white papers that defines a suitable architecture for implementing service-level enforced security on Bluetooth devices.

The white paper splits devices into different categories and trust levels, as well as suggesting three security levels for services. The utilization of a database is suggested for enabling the user to authorize devices to utilize only particular services. Because the implementation of security at this level does not affect interoperability, this white paper is advisory only, and is not part of the Bluetooth specification. Mode 3 is link-level enforced security. Both devices must implement security procedures in order for a connection to be established. In addition to the above modes, a device can be configured to not respond to paging, so that other devices cannot connect to it. Or it can be configured so that only devices that already know its address can connect to it. Such numerous and complex levels of security are necessary to accommodate the large variety of different usage scenarios. It falls on the designers of Bluetooth products to ensure that the complexity of Bluetooth is hidden from the user, while still providing the user with necessary security options.

3.11 Summary

Bluetooth wireless technology is conceived as a low-power short range radio technology designed to replace cables for interconnecting devices such as printers, keyboards, and mice, its perceived potential has evolved into far more sophisticated usage models. The requirement to do this in a totally automated, seamless, and user-friendly fashion, without adding appreciable cost, weight, or power drain to the associated host is an enormous engineering challenge. Bluetooth devices can form piconets of up to seven slaves and one master, enabling discovery of services and subsequent implementation of many varied usage models including wireless headsets, Internet bridges, and wireless operations such as file exchange, data synchronization, and printing. Despite talk of Bluetooth competing with wireless LANs, Bluetooth products work over shorter distances and are designed to solve different problems.

4. CELLULAR COMMUNICATIONS

4.1 Overview

A cellular mobile communications system uses a large number of low-power wireless transmitters to create cells, the basic geographic service area of a wireless communications system. Variable power levels allow cells to be sized according to the subscriber density and demand within a particular region. As mobile users travel from cell to cell, their conversations are handed off between cells to maintain seamless service. Channels (frequencies) used in one cell can be reused in another cell some distance away. Cells can be added to accommodate growth, creating new cells in un-served areas or overlaying cells in existing areas.

This chapter discusses the basics of radio telephony systems, including both analog and digital systems. Upon completion of this chapter, you should be able to describe the basic components of a cellular system and identify digital wireless technologies.

4.2 Mobile Communications Principles

Each mobile uses a separate, temporary radio channel to talk to the cell site. The cell site talks to many mobiles at once, using one channel per mobile. Channels use a pair of frequencies for communication—one frequency (the forward link) for transmitting from the cell site and one frequency (the reverse link) for the cell site to receive calls from the users. Radio energy dissipates over distance, so mobiles must stay near the base station to maintain communications. The basic structure of mobile networks includes telephone systems and radio services. Where mobile radio service operates in a closed network and has no access to the telephone system, mobile telephone service allows interconnection to the telephone network.

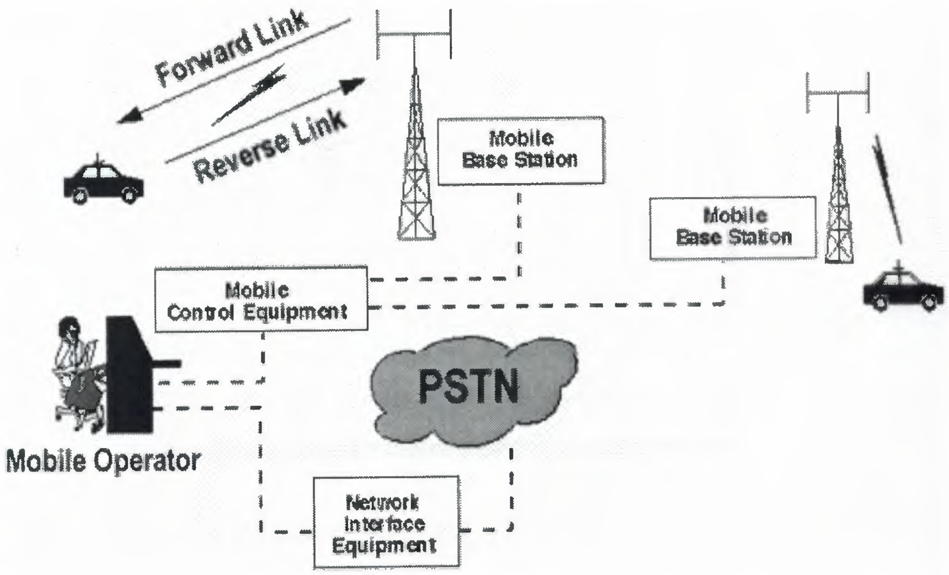


Figure 4.1 Basic Mobile Telephone Service Network

4.2.1 Early Mobile Telephone System Architecture

Traditional mobile service was structured in a fashion similar to television broadcasting: One very powerful transmitter located at the highest spot in an area would broadcast in a radius of up to 50 kilometers. The cellular concept structured the mobile telephone network in a different way. Instead of using one powerful transmitter, many low-power transmitters were placed throughout a coverage area. For example, by dividing a metropolitan region into one hundred different areas (cells) with low-power transmitters using 12 conversations (channels) each, the system capacity theoretically could be increased from 12 conversations or voice channels using one powerful transmitter to 1,200 conversations (channels) using one hundred low-power transmitters. Shows a metropolitan area configured as a traditional mobile telephone network with one high-power transmitter.

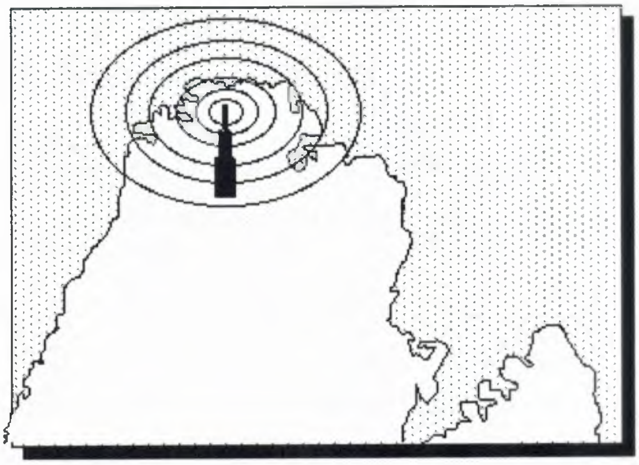


Figure 4.2. Early Mobile Telephone System Architecture

4.3 Mobile Telephone System Using the Cellular Concept

Interference problems caused by mobile units using the same channel in adjacent areas proved that all channels could not be reused in every cell. Areas had to be skipped before the same channel could be reused. Even though this affected the efficiency of the original concept, frequency reuse was still a viable solution to the problems of mobile telephony systems.

Engineers discovered that the interference effects were not due to the distance between areas, but to the ratio of the distance between areas to the transmitter power (radius) of the areas. By reducing the radius of an area by 50 percent, service providers could increase the number of potential customers in an area fourfold. Systems based on areas with a one-kilometer radius would have one hundred times more channels than systems with areas 10 kilometers in radius. Speculation led to the conclusion that by reducing the radius of areas to a few hundred meters, millions of calls could be served.

The cellular concept employs variable low-power levels, which allow cells to be sized according to the subscriber density and demand of a given area. As the population grows, cells can be added to accommodate that growth.

Frequencies used in one cell cluster can be reused in other cells. Conversations can be handed off from cell to cell to maintain constant phone service as the user moves between cells.

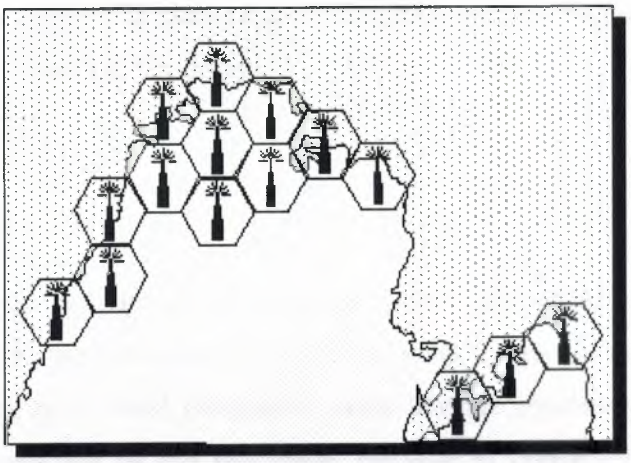


Figure 4.4. Mobile Telephone System Using a Cellular Architecture

The cellular radio equipment (base station) can communicate with mobiles as long as they are within range. Radio energy dissipates over distance, so the mobiles must be within the operating range of the base station. Like the early mobile radio system, the base station communicates with mobiles via a channel. The channel is made of two frequencies, one for transmitting to the base station and one to receive information from the base station.

4.4 Cellular System Architecture

Increases in demand and the poor quality of existing service led mobile service providers to research ways to improve the quality of service and to support more users in their systems. Because the amount of frequency spectrum available for mobile cellular use was limited, efficient use of the required frequencies was needed for mobile cellular coverage.

In modern cellular telephony, rural and urban regions are divided into areas according to specific provisioning guidelines. Deployment parameters, such as amount of cell-splitting and cell sizes, are determined by engineers experienced in cellular system architecture. Provisioning for each region is planned according to an engineering plan that includes cells, clusters, frequency reuse, and handovers.

4.4.1 Cells

A cell is the basic geographic unit of a cellular system. The term *cellular* comes from the honeycomb shape of the areas into which a coverage region is divided. Cells are base stations transmitting over small geographic areas that are represented as hexagons. Each cell size varies depending on the landscape. Because of constraints imposed by natural terrain and man-made structures, the true shape of cells is not a perfect hexagon.

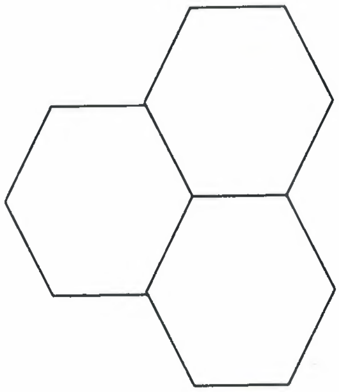


Figure 4.4. Cells

4.4.2 Clusters

A cluster is a group of cells. No channels are reused within a cluster. Figure 4.5 illustrates a seven-cell cluster.

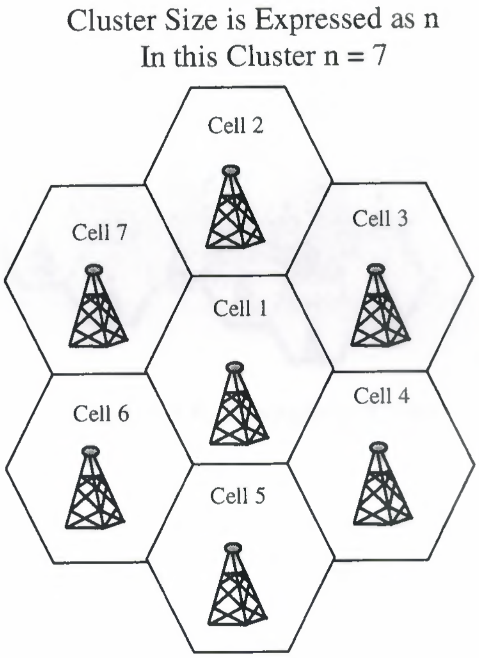


Figure 4.5. A Seven-Cell Cluster

4.4.3 Frequency Reuse

Because only a small number of radio channel frequencies were available for mobile systems, engineers had to find a way to reuse radio channels to carry more than one conversation at a time. The solution the industry adopted was called frequency planning or frequency reuse. Frequency reuse was implemented by restructuring the mobile telephone system architecture into the cellular concept.

The concept of frequency reuse is based on assigning to each cell a group of radio channels used within a small geographic area. Cells are assigned a group of channels that is completely different from neighboring cells. The coverage area of cells is called the footprint. This footprint is limited by a boundary so that the same group of channels can be used in different cells that are far enough away from each other so that their frequencies do not interfere.

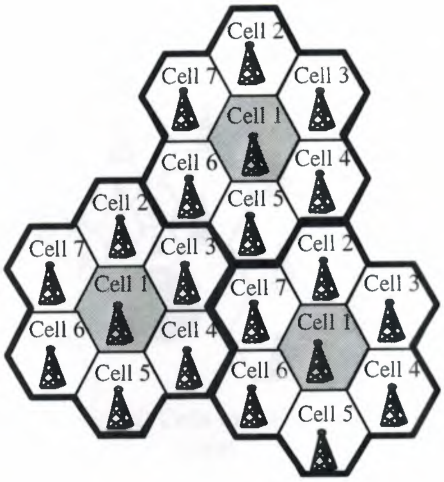


Figure 4.6. Frequency Reuse

Cells with the same number have the same set of frequencies. Here, because the number of available frequencies is 7, the frequency reuse factor is 1/7. That is, each cell is using 1/7 of available cellular channels.

4.4.4 Cell Splitting

Unfortunately, economic considerations made the concept of creating full systems with many small areas impractical. To overcome this difficulty, system operators developed the idea of cell splitting. As a service area becomes full of users, this approach is used to split a single area into smaller ones. In this way, urban centers can be split into as many areas as necessary to provide acceptable service levels in heavy-traffic regions, while larger, less expensive cells can be used to cover remote rural regions.

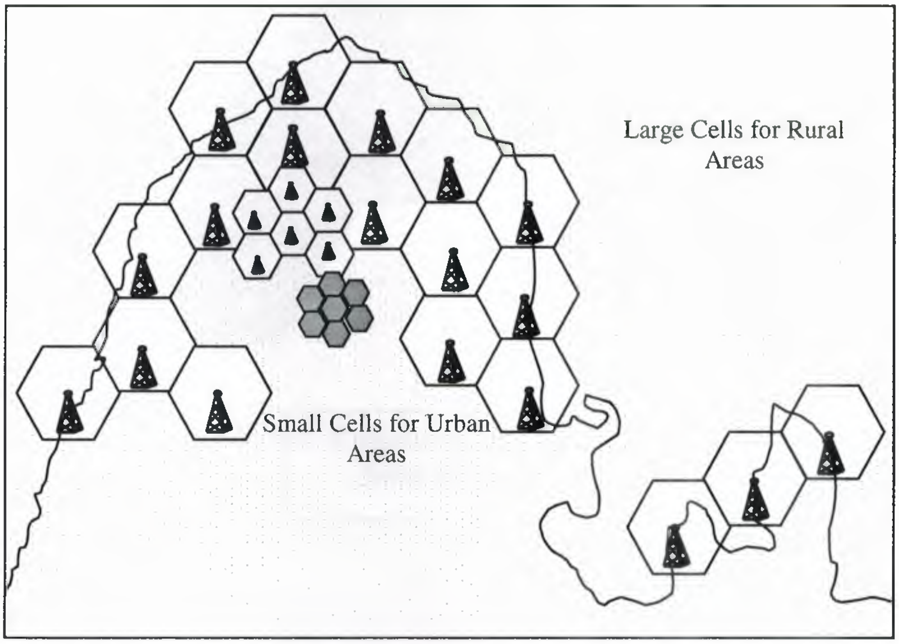


Figure 4.6. Cell Splitting

4.4.5 Handoff

The final obstacle in the development of the cellular network involved the problem created when a mobile subscriber traveled from one cell to another during a call. As adjacent areas do not use the same radio channels, a call must either be dropped or transferred from one radio channel to another when a user crosses the line between adjacent cells. Because dropping the call is unacceptable, the process of handoff was created. Handoff occurs when the mobile telephone network automatically transfers a call from radio channel to radio channel as mobile crosses adjacent cells.

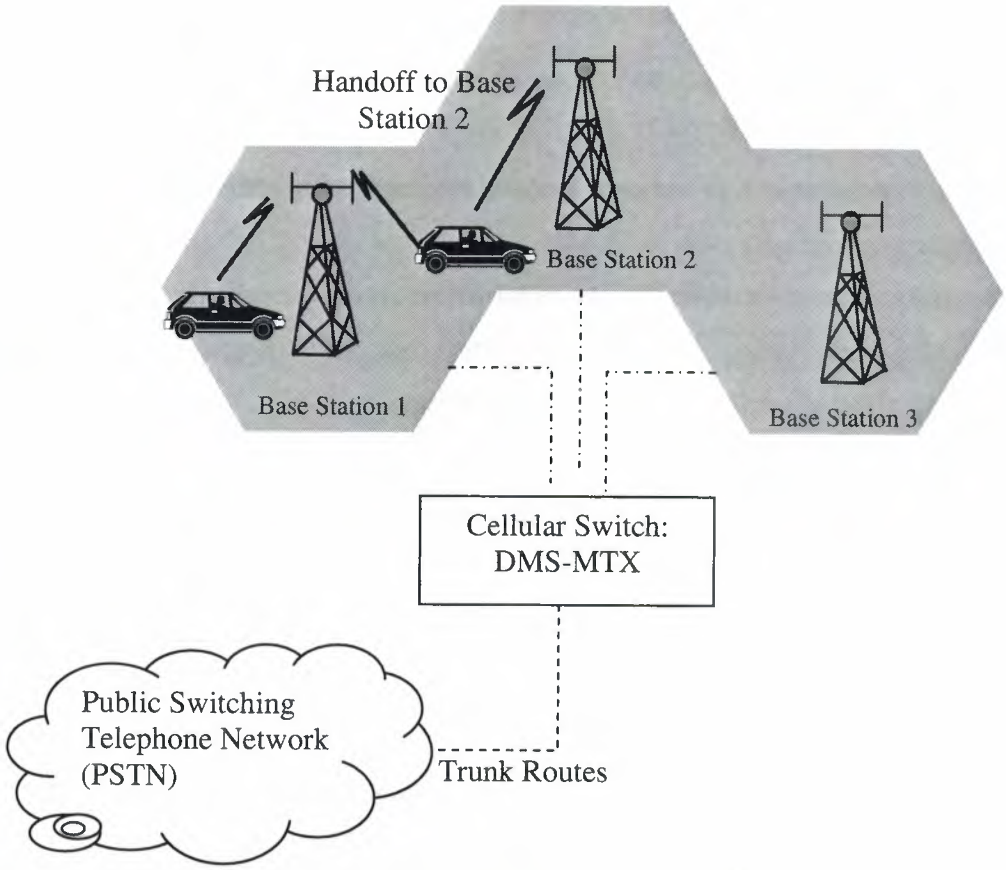


Figure 4.7. Handoff between Adjacent Cells

During a call, two parties are on one voice channel. When the mobile unit moves out of the coverage area of a given cell site, the reception becomes weak. At this point, the cell site in use requests a handoff. The system switches the call to a stronger-frequency channel in a new site without interrupting the call or alerting the user. The call continues as long as the user is talking, and the user does not notice the handoff at all.

4.5 North American Analog Cellular Systems

Originally devised in the late 1970s to early 1980s, analog systems have been revised somewhat since that time and operate in the 800-MHz range. A group of government, Telco, and equipment manufacturers worked together as a committee to develop a set of rules (protocols) that govern how cellular subscriber units (mobiles) communicate with the cellular system. System development takes into consideration many different, and often opposing, requirements for the system, and often a compromise between conflicting requirements results. Cellular development involves the following basic topics:

- frequency and channel assignments
- type of radio modulation
- maximum power levels
- modulation parameters
- messaging protocols
- call-processing sequences

4.5.1 The Advanced Mobile Phone Service (AMPS)

AMPS was released in 1983 using the 800-MHz to 900-MHz frequency band and the 30-kHz bandwidth for each channel as a fully automated mobile telephone service. It was the first standardized cellular service in the world and is currently the most widely used standard for cellular communications. Designed for use in cities, AMPS later expanded to rural areas. It maximized the cellular concept of frequency reuse by reducing radio power output. The AMPS telephones (or handsets) have the familiar telephone-style user interface and are compatible with any AMPS base station. This makes mobility between service providers (roaming) simpler for subscribers. Limitations associated with AMPS include the following:

- low calling capacity
- limited spectrum
- no room for spectrum growth
- poor data communications
- minimal privacy
- inadequate fraud protection

AMPS is used throughout the world and is particularly popular in the United States, South America, China, and Australia. AMPS uses Frequency Modulation (FM) for radio transmission. In the United States, transmissions from mobile to cell site use separate frequencies from the base station to the mobile subscriber.

4.5.2 Narrowband Analog Mobile Phone Service (NAMPS)

Since analog cellular was developed, systems have been implemented extensively throughout the world as first-generation cellular technology. In the second generation of analog cellular systems, NAMPS was designed to solve the problem of low calling capacity. NAMPS is now operational in 35 U.S. and overseas markets, and NAMPS was introduced as an interim solution to capacity problems. NAMPS is a U.S. cellular radio system that combines existing voice processing with digital signaling, tripling the capacity of today's AMPS systems. The NAMPS concept uses frequency division to get 3 channels in the AMPS 30-kHz single channel bandwidth. NAMPS provides 3 users in an AMPS channel by dividing the 30-kHz AMPS bandwidth into 3-10 kHz channels. This increases the possibility of interference because channel bandwidth is reduced.

4.6 Cellular System Components

The cellular system offers mobile and portable telephone stations the same service provided fixed stations over conventional wired loops. It has the capacity to serve tens of thousands of subscribers in a major metropolitan area. The cellular communications system consists of the following four major components that work together to provide mobile service to subscribers.

- public switched telephone network (PSTN)
- mobile telephone switching office (MTSO)
- cell site with antenna system
- mobile subscriber unit (MSU)

4.6.1 PSTN

The PSTN is made up of local networks, the exchange area networks, and the long-haul network that interconnect telephones and other communication devices on a worldwide basis.

4.6.2 Mobile Telephone Switching Office (MTSO)

The MTSO is the central office for mobile switching. It houses the mobile switching center (MSC), field monitoring, and relay stations for switching calls from cell sites to wire line central offices (PSTN). In analog cellular networks, the MSC controls the system operation. The MSC controls calls, tracks billing information, and locates cellular subscribers.

4.6.3 The Cell Site

The term *cell site* is used to refer to the physical location of radio equipment that provides coverage within a cell. A list of hardware located at a cell site includes power sources, interface equipment, radio frequency transmitters and receivers, and antenna systems.

4.6.4 Mobile Subscriber Units (MSUs)

The mobile subscriber unit consists of a control unit and a transceiver that transmits and receives radio transmissions to and from a cell site. The following three types of MSUs are available:

- the mobile telephone (typical transmit power is 4.0 watts)
- the portable (typical transmit power is 0.6 watts)
- the transportable (typical transmit power is 1.6 watts)

The mobile telephone is installed in the trunk of a car, and the handset is installed in a convenient location to the driver. Portable and transportable telephones are hand-held and can be used anywhere. The use of portable and transportable telephones is limited to the charge life of the internal battery.

4.7 Digital Systems

As demand for mobile telephone service has increased, service providers found that basic engineering assumptions borrowed from wire line (landline) networks did not hold true in mobile systems. While the average landline phone call lasts at least 10 minutes, mobile calls usually run 90 seconds. Engineers who expected to assign 50 or more mobile phones to the same radio channel found that by doing so they increased the probability that a user would not get dial tone—this is known as call-blocking probability. As a consequence, the early systems quickly became saturated, and the quality of service decreased rapidly. The critical problem was capacity. The general characteristics of time division multiple access (TDMA), Global System for Mobile Communications (GSM), personal communications service (PCS) 1900, and code division multiple access (CDMA) promise to significantly increase the efficiency of cellular telephone systems to allow a greater number of simultaneous conversations. Figure 4.8 shows the components of a typical digital cellular system.

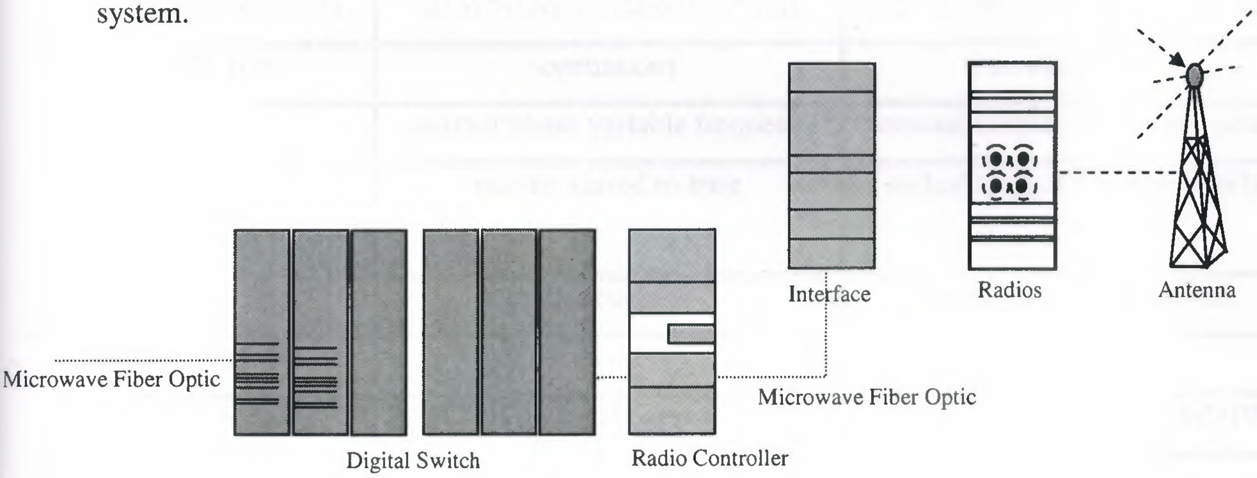


Figure 4.8. Digital Cellular System

The advantages of digital cellular technologies over analog cellular networks include increased capacity and security. Technology options such as TDMA and CDMA offer more channels in the same analog cellular bandwidth and encrypted voice and data. Because of the enormous amount of money that service providers have invested in AMPS hardware and software, providers look for a migration from AMPS to digital analog mobile phone service (DAMPS) by overlaying their existing networks with TDMA architectures.

Table 4.1. AMPS/DAMPS Comparison

	Analog	**Digital**
standard	EIA–553 (AMPS)	IS–54 (TDMA + AMPS)
spectrum	824 MHz to 891 MHz	824 MHz to 891 MHz
channel bandwidth	30 kHz	30 kHz
channels	21 CC/395 VC	21 CC / 395 VC
Conversations per channel	1	3 or 6
subscriber capacity	40 to 50 conversations per cell	125 to 300 conversations per cell
TX/RCV type	continuous	time shared bursts
carrier type	constant phase variable frequency	constant frequency variable phase
mobile/base relationship	mobile slaved to base	authority shared cooperatively
privacy	poor	better—easily scrambled
noise immunity	poor	high
fraud detection	ESN plus optional password (PIN)	ESN plus optional password (PIN)

4.7.1 Time Division Multiple Access (TDMA)

North American digital cellular (NADC) is called DAMPS and TDMA. Because AMPS preceded digital cellular systems, DAMPS uses the same setup protocols as analog AMPS. TDMA has the following characteristics:

1. IS–54 standard specifies traffic on digital voice channels
2. initial implementation triples the calling capacity of AMPS systems
3. capacity improvements of 6 to 15 times that of AMPS are possible
4. many blocks of spectrum in 800 MHz and 1900 MHz are used
5. all transmissions are digital
6. TDMA/FDMA application 7. 3 callers per radio carrier (6 callers on half rate later), providing 3 times the AMPS capacity

TDMA is one of several technologies used in wireless communications. TDMA provides each call with time slots so that several calls can occupy one bandwidth. Each caller is assigned a specific time slot. In some cellular systems, digital packets of information are sent during each time slot and reassembled by the receiving equipment into the original voice components. TDMA uses the same frequency band and channel allocations as AMPS. Like NAMPS, TDMA provides three to six time channels in the same bandwidth as a single AMPS channel. Unlike NAMPS, digital systems have the means to compress the spectrum used to transmit voice information by compressing idle time and redundancy of normal speech. TDMA is the digital standard and has 30-kHz bandwidth. Using digital voice encoders, TDMA is able to use up to six channels in the same bandwidth where AMPS uses one channel.

4.7.2 Extended Time Division Multiple Access (E–TDMA)

The E–TDMA standard claims a capacity of fifteen times that of analog cellular systems. This capacity is achieved by compressing quiet time during conversations. E–TDMA divides the finite number of cellular frequencies into more time slots than TDMA. This allows the system to support more simultaneous cellular calls.

4.7.3 Fixed Wireless Access (FWA)

FWA is a radio-based local exchange service in which telephone service is provided by common carriers. It is primarily a rural application—that is, it reduces the cost of conventional wire line. FWA extends telephone service to rural areas by replacing a wire line local loop with radio communications. Other labels for wireless access include fixed loop, fixed radio access, wireless telephony, radio loop, fixed wireless, radio access, and Ionic. FWA systems employ TDMA or CDMA access technologies.

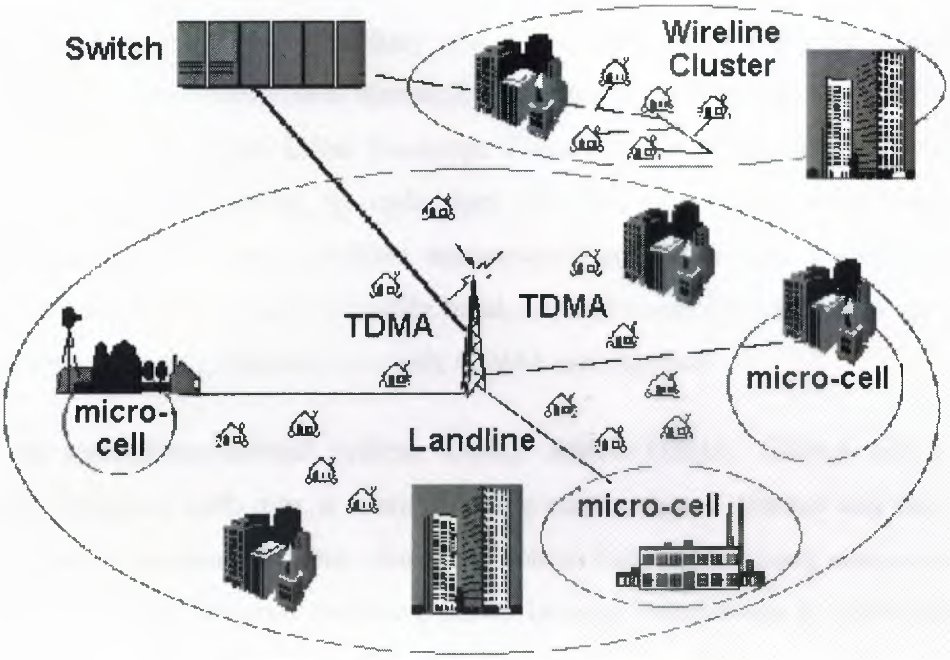


Figure 4.9 Fixed Wireless Access

4.7.4 Personal Communications Service (PCS)

The future of telecommunications includes PCS. PCS at 1900 MHz (PCS 1900) is the North American implementation of digital cellular system (DCS) 1800 (GSM). Trial networks were operational in the United States by 1993, and in 1994 the Federal Communications Commission (FCC) began spectrum auctions. As of 1995, the FCC auctioned commercial licenses. In the PCS frequency spectrum, the operator's authorized frequency block contains a definite number of channels. The frequency plan assigns specific channels to specific cells, following a reuse pattern that restarts with each *n*th cell. The uplink and downlink bands are paired mirror images. As with AMPS, a channel number implies one uplink and one downlink frequency (e.g., Channel 512 = 1850.2-MHz uplink paired with 1930.2-MHz downlink).

4.7.5 Code Division Multiple Access (CDMA)

CDMA is a digital air interface standard, claiming 8 to 15 times the capacity of analog. It employs a commercial adaptation of military, spread-spectrum, single-sideband technology. Based on spread spectrum theory, it is essentially the same as wire line service-the primary difference is that access to the Local Exchange Carrier (LEC) is provided via wireless phone. Because users are isolated by code, they can share the same carrier frequency, eliminating the frequency reuse problem encountered in AMPS and DAMPS. Every CDMA cell site can use the same 1.25-MHz band, so with respect to clusters, $n = 1$. This greatly simplifies frequency planning in a fully CDMA environment.

CDMA is an interference-limited system. Unlike AMPS/TDMA, CDMA has a soft capacity limit; however, each user is a noise source on the shared channel and the noise contributed by users accumulates. This creates a practical limit to how many users a system will sustain. Mobiles that transmit excessive power increase interference to other mobiles. For CDMA, precise power control of mobiles is critical in maximizing the system's capacity and increasing battery life of the mobiles. The goal is to keep each mobile at the absolute minimum power level that is necessary to ensure acceptable service quality. Ideally, the power received at the base station from each mobile should be the same (minimum signal to interference).

5. GENERAL HCI BRIDGING CONSIDERATION FOR BLUETOOTH

5.1 Overview

This chapter gives an overview of Bluetooth wireless technology and how Xilinx high-volume programmable devices can be used to integrate Bluetooth network interfaces at the system level. The Xilinx device families targeted at these high-volume applications include XC9500 CPLDs and Spartan FPGAs.

The flow of this document will be to start with an overview of Bluetooth. We will next examine the major functional blocks of a Bluetooth interface and give an overview of the Application Specific Standard Products (ASSPs) that are available to implement them. We will then illustrate the Host Controller Interface (HCI) that is standard for interfacing the Bluetooth subsystem to the host.

While this document focuses on the use of these devices in Bluetooth HCI interface applications, the examples discussed illustrate many of the issues found in other designs, specifically, how to cost effectively interface complex ASSPs with incompatible interfaces. The ASIC vendors have abandoned the traditional solution for this class of problems, the small ASIC, as they moved towards the system on chip market. Fortunately for system designers, new classes of low cost PLDs, such as the Spartan family, have filled this void with devices that replace low density ASICs and retain the time to market advantages of FPGAs.

5.2 Bluetooth Background

Bluetooth is a short-range radio link that is intended to replace cabling used to connect fixed or portable electronic devices. Bluetooth devices operate in the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) frequency band. The Bluetooth baseband protocol supports both circuit switched and packet-switched communications and uses Frequency Hopping Spread Spectrum (FHSS) technology for transmission. In North

America and most of Euro, Bluetooth operates in the frequency range from 2.402 to 2.480 GHz, with this band divided into 79, 1 MHz sub-channels.

Up to eight Bluetooth devices with overlapping coverage share channel bandwidth and form what is called a piconet. On each piconet one Bluetooth unit acts as the master while the other unit(s) acts as slave(s). In addition to the seven slaves that may be active on each piconet, more slaves can remain locked to the master in a parked state. The piconet master controls channel access for both active and parked slaves.

Multiple piconets with overlapping coverage areas form a scatternet. While each piconet can only have a single master, slaves can participate in different piconets on a time-division basis.

In addition, a master in one piconet can be a slave in another piconet. The Bluetooth protocol includes support for both packet and circuit switching. Each piconet can support an asynchronous data channel, up to three simultaneous synchronous voice channels, or a mix of links. Each voice channel is 64 kb/s synchronous, full duplex, and is referred to as a Synchronous Connection-Oriented (SCO) link. The asynchronous channels are called Asynchronous Connection-Less (ACL) links and can support an asymmetric link of maximally 723.2 kb/s in either direction while permitting 57.6 kb/s in the return direction, or a 433.9 kb/s symmetric link.

The Bluetooth specification breaks the functions required to implement a Bluetooth interface into three major functional blocks as shown in Figure 5.1. These functional blocks map directly to the partitioning of the Bluetooth specification.

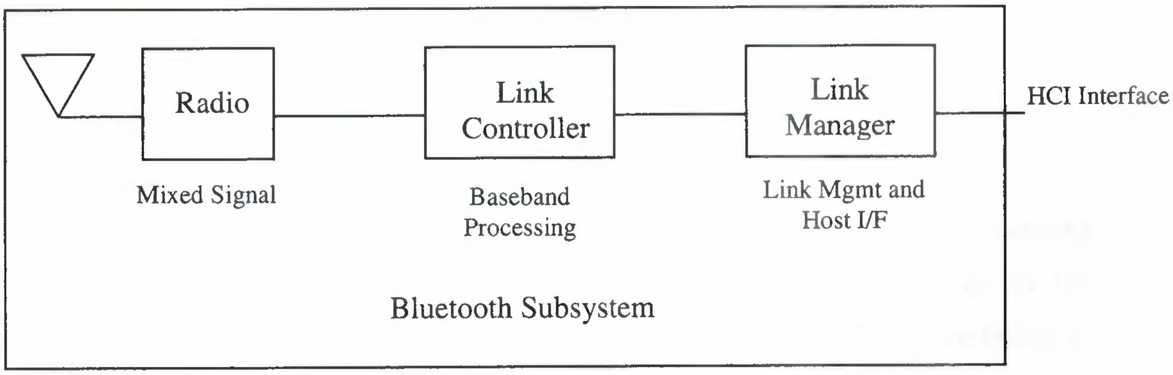


Figure 5.1 Bluetooth Functional Blocks

5.2.1 Bluetooth Radio

The Radio implements the broadband air interface for Bluetooth devices. The radio is typically implemented as a multi-chip module and includes an antenna switch, baluns, amplifiers, digital PLL based clock recovery, modulation, and demodulation circuitry.

5.2.2 Bluetooth Link Controller

The Link Controller Bluetooth baseband functions are described in Part B of the specification, and consist of low-level link layer functions. Baseband functions include:

- CVSD speech coding
- Header Error Check (HEC) generation and checking
- Forward Error Correction (FEC) generation and checking
- Cyclic Redundancy Check (CRC) generation and checking
- Data whitening (scrambling)
- Payload encryption and decryption
- Sequencing of frequency hopping

5.2.3 Bluetooth Link Manager

The Link Management block implements the Link Manager Protocol (LMP), which handles low level control plane functions such as:

- Link setup between devices
- Generating, exchanging, and checking encryption keys
- Negotiation of baseband packet sizes
- Power modes and duty cycles of the radio
- Connection states of the unit in a piconet

The complexity of these functions mandates a software implementation, typically running on an embedded RISC processor. This software approach leads to the use of the processor for other functions as well, including the firmware required for interfacing to the host system.

5.3 The Bluetooth Host Controller Interface

The Bluetooth specification defines the Host Controller Interface (HCI) as follows:
"The HCI provides a command interface to the baseband controller and link manager, and access to hardware status and control registers. This interface provides a uniform method of accessing the Bluetooth baseband capabilities."
The HCI consists of two parts — the software that implements the command interface and the physical hardware that is used to connect the Bluetooth subsystem to the host. The purpose of the HCI software is to make the hardware that comprise the interface transparent to higher level software in the system.

5.3.1 HCI Software

The Bluetooth software architecture consists of two types of components — Data Plane and Control Plane. Data Plane components are responsible for the transfer of data across the link.
Control Plane components are responsible for link control and management. For the purposes of this chapter we will be focused on the Data and Control Plane components that make up the HCI. Figure 5.2 illustrates the HCI software architecture and how it relates to the Bluetooth host interface hardware.

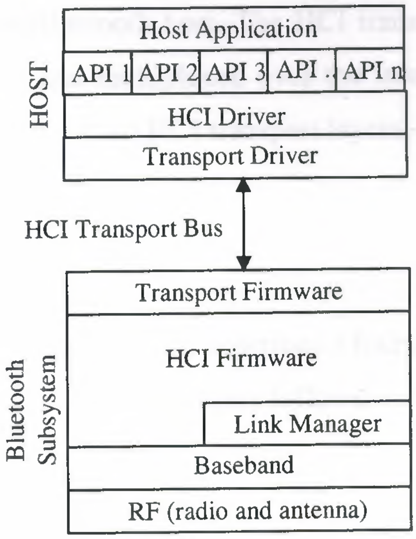


Figure 5.2 Bluetooth HCI Software Architecture

5.3.2 HCI Commands and Events

The host controls the Bluetooth network interface through a variety of commands that are provided by the HCI driver. In addition to these commands, the Bluetooth specification defines a set of events that are generated by the HCI firmware in the Bluetooth Network Interface to indicate state changes in the interface.

HCI commands and events are combined with data from ACL and SCO links over the interface hardware that is used for HCI transport. The scheme used to multiplex this data over the interface is specific to each interface. Figure 5.3 illustrates how this works.

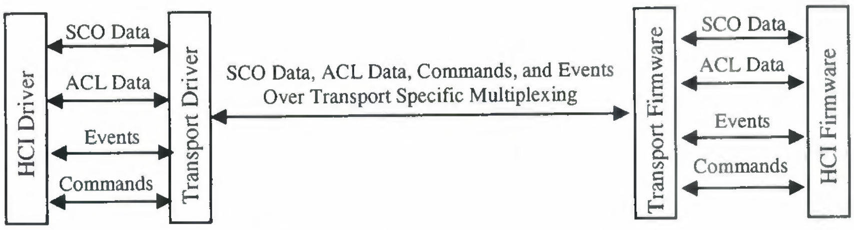


Figure 5.3 HCI Multiplexing

5.3.3 HCI Hardware/Transports

The HCI transports define how to transfer three classes of data between the Bluetooth network interface and the Bluetooth host. The HCI transports define how each of these data types is encapsulated and multiplexed over the interface hardware. The Bluetooth specification currently defines three HCI transport layers.

- UART Transport Layer
- RS232 Transport Layer
- USB Transport Layer

A white chapter from the Bluetooth SIG describes a fourth, the PC Card Transport Layer. An overview of each of these transport layers follows.

5.3.4 UART Transport Layer

Both the RS232 and the UART transport layers use serial communication via a UART to transfer data between the Bluetooth Network Interface and the Bluetooth Host. The difference between the two lies in the environmental assumptions that drive the design of the protocol.

The UART transport layer is designed for an environment where the Bluetooth Network Interface and the host are located on the same printed circuit board and, as a result, the link is relatively error free. The encapsulation of the HCI commands consists of an HCI Packet Indicator, which indicates whether the frame contains a command, an event, or a data packet followed by a length indicator. The length indicator is used to check whether frame synchronization has been lost and a simple recovery mechanism is used in the event that it is.

Since both ends of the link are collocated on the same board, the UART transport layer does not specify the electrical signaling and in most cases this will be done using TTL levels. Since both ends of the link are on the same board, there is no mechanism defined for baud rate negotiation.

5.3.5 RS232 Transport Layer

The RS232 transport layer was designed to support communication between a Bluetooth Network Interface and a host located in separate enclosures. As a result, RS232 electrical signaling is specified and a far more elaborate link protocol is defined. Both of these are needed in order to deal with a link that spans larger distances and must be able to handle a much higher line error rate. In addition to the four HCI Packet Indicators used by the UART transport layer, the RS232 layer adds two additional types. One is used to negotiate the baud rate, parity type, number of stop bits, and the protocol mode. The second is used to communicate line errors to the transmitter. The RS232 transport layer defines two encapsulation schemes. One uses HDLC like framing and a 16-bit CRC. The second scheme omits the CRC and uses the RTS/CTS signals for delineation. Both schemes include a sequence number in each frame so that receivers can easily detect lost frames.

5.3.6 USB Transport Layer

Unlike the UART and RS232 transports, the endpoint mechanisms defined in USB provide a simple means of multiplexing traffic over the link without additional overhead to identify the type of traffic. As a result, this specification primarily describes how the Bluetooth data types are mapped to USB endpoints. This includes how to map SCO data streams to the USB isochronous data services.

5.3.7 PC Card Transport Layer

This layer is not defined in the Bluetooth specification, but is described in a white chapter. The reason for this is that the Bluetooth specification decided not to restrict the implementation details other than the requirement that the card comply with the requirements of the PC Card and Cardbus standards. In order to support interoperability, the manufacturer must provide an interface hardware specific transport driver that can be used with the HCI driver on the host system.

5.3.8 HCI Support in ASSPs

Unless you have the time and resources to implement a Bluetooth network interface from scratch, you will need to base your HCI implementation strategy on what is provided by existing ASSPs. Table 5.1 provides a survey of the available ASSPs that implement Bluetooth Link Controller and/or Link Manager functionality.

Table 5.1 Bluetooth ASSPs

Vendor	Part Number	Radio	Link Controller	Link Manager	Processor	HCI Transport Support
Qualcomm	MSM3300		√	√	ARM7TDMI	USB, UART
Ericsson	ROK 101 007		√	√	ARMT-Thumb	USB, UART
National Semiconductor	LMX5001		√		None	None
Silicon Wave	SiW1601		√		None	None
Texas Instruments	BSN6030		√	√	ARM7TDMI	UART
Infineon	BlueMoon 1	√	√	√	TBD	UART
Lucent	W7400		√	√	TBD	USB, UART
Alcatel	TBD	√	√	√	ARM7	UART
Cambridge Silicon Radio	BlueCore	√	√	√	Proprietary	USB, UART
Philsar Semiconductor	PH2410		√	√	ARM7TDMI	USB, UART

For the purposes of our further discussion, these ASSPs fall into two broad categories:1) those that implement only the Link Controller functions and 2) those that include both the Link Controller and the Link Manager. The key difference between these two classes of devices is that the first includes an embedded RISC processor used to implement Link Manager and HCI functions and the second does not.

The decision regarding which class device to use requires analyzing the tradeoffs for each alternative. In the next section we will review these tradeoffs and show how Spartan devices can provide solutions to HCI interface issues.

5.4 The Challenges of Creating Real World Solutions

The cost effective integration of Bluetooth technology into a system level design can present many challenges, including:

- Evolving standards. While the Bluetooth core protocols are stable, the mapping of higher level protocols and services such as IP traffic is still evolving.
- Buggy ASSPs. Most of the ASSPs that are being used are relatively new and will have deficiencies that must be dealt with by the system designer.
- Emerging product use models. In most cases Bluetooth technology is currently too expensive for it's original target market, cable replacement. This and the lure of other potential "killer apps" has driven many to push Bluetooth into application areas that are still being defined.

Clearly what is needed is a flexible technology that allows system designers to quickly develop Bluetooth solutions, but at the same time can respond to this fluid environment. Let's explore how Spartan devices can meet this need when used to interface the two classes of Bluetooth ASSPs that we have discussed.

5.4.1 Link Controller + Link Manager ASSPs

If you choose to use one of the ASSPs that implements both Link Controller and Link Manager functions you have the advantage of starting with a fairly complete solution. The manufacturers of these devices provide not only a RISC processor and one or more of the defined HCI transport interfaces, but also provide HCI and Link Manager firmware. With these devices, system level integration consists of connecting the HCI transport interface to the host. If the host system has an available USB or UART port, system level integration can be accomplished with no additional hardware. In many cases, these ports are integrated into the system's core logic chipset. Figure 5.4 illustrates a system that utilizes this type of zero-glue interface.

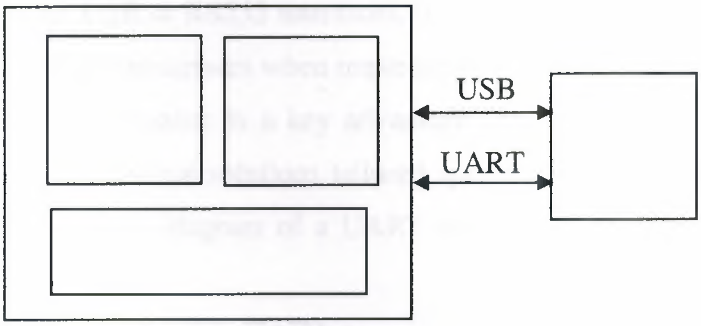


Figure 5.4 Zero-Glue Bluetooth Interface

In many cases this approach may not be workable for any of the following reasons:

- The host system may not have sufficient USB or UART ports for the application. This can occur when the host has a limited number of ports, or when that application requires a large number of ports.
- The host system may not have serial ports that can support the data rate required for full Bluetooth performance. In order to support maximum system level performance, Bluetooth ASSPs include UARTs that are capable of supporting transfer rates of up to 1.5 Mbps.
- Standard port interface ASSPs are not tailored for Bluetooth protocol handling, and as a result, they may consume significant processing resources when operating at Bluetooth

rates. As we will see, interrupt processing overhead can become a drain on host processing resources.

In any of these situations a Spartan device can be used to implement the required interface hardware. In deeply embedded applications this would typically be an interface between a USB or UART core and the local bus of the embedded processor used in the system. While Spartan devices can be used to implement either a USB or UART transport interface, the simpler transport protocol of the UART interface results in a more cost effective interface with better system level performance.

A UART interface is more cost effective since it requires fewer hardware resources to implement. Since the UART only operates in a single mode, eight bits of data, no parity, and one stop bit, the implementation can be very simple and operate at a very high speed. In addition, unlike the USB or RS232 interfaces, the UART transport layer does not need external level shifters or transceivers when implemented in an FPGA.

Better system level performance is a key advantages of Spartan FPGAs. They can be used to quickly create interface solutions tailored specifically for the target application. Figure 5.5 shows the block diagram of a UART enhanced with DMA and HCI frame transfer state machine logic.

This design is described in detail in XAPPxxx.

The use of Spartan FPGAs improve system level performance by reducing the overhead of servicing interrupts for transmission and reception. Unlike traditional UARTs where an interrupt is generated every time the small on-chip FIFOs are filled or emptied, this design generates an interrupt only when a complete HCI frame has been transmitted or received. This is accomplished by having application specific logic that decodes the frame size information in the HCI header and configures the DMA logic appropriately. This logic also checks to ensure that proper frame level synchronization is being maintained. The net result being that the burden of interrupt handling is considerably reduced for the host processor. As a result, more processor performance is available for other value added functions. In addition, with the wide range of standard interface and memory controller IP available, the Spartan device can be used to implement other core logic functions as well.

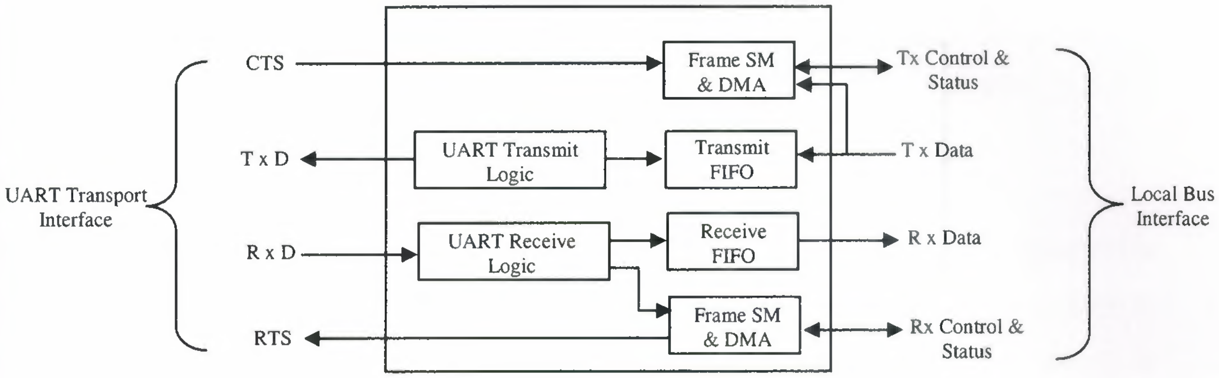


Figure 5.5 Bluetooth Application Tailored UART

5.4.2 Link Controller Only ASSPs

Link controller logic only ASSPs can result in additional design work in order to create a complete solution. They also present the opportunity for tighter integration and lower system cost for deeply embedded systems. This is due to the fact that if the Bluetooth Network Interface and the host are located on the same board, there is no need for an HCI transport layer. In this case, the interfaces used to control the Baseband Processing and Radio functions, as well as the interfaces used to transfer data frames, are simply interfaced directly to the host processor. Since these interfaces are usually specific to the ASSP involved, a Spartan device provides a low cost means of interfacing them to either the host processors bus or an I/O bus such as PCI (Figure 5.6). Note that here is another situation where the Spartan device can be used to integrate other core logic functions as well.

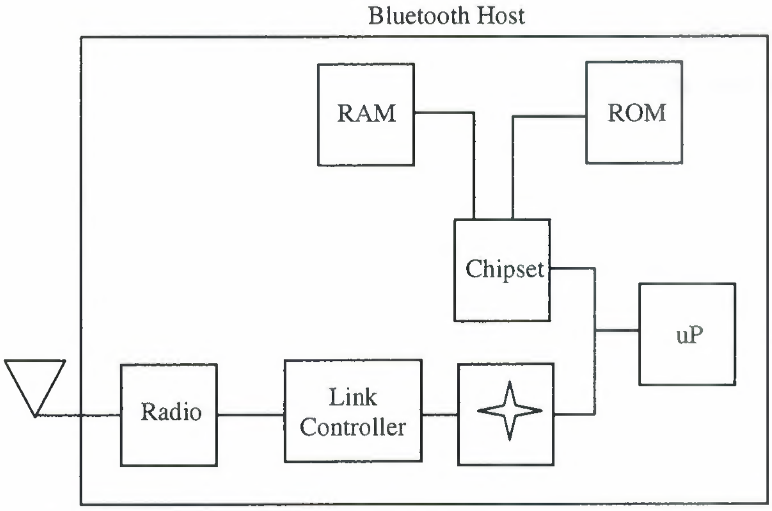


Figure 5. 6 Link Controller ASSP Interface

In this arrangement, the host CPU takes on all protocol processing functions. These results in further economies since the RISC processor that was dedicated to Link Management functions and its non-volatile memory requirements are eliminated from the system. In this architecture, the Bluetooth software stack collapses to the arrangement shown in Figure 5.7.

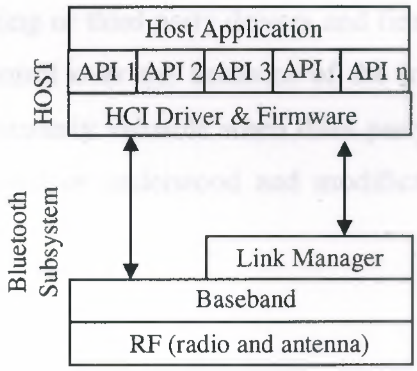


Figure 5.7 Collapsed Software Stack

As we have seen, programmable logic provides an excellent platform for integrating Bluetooth technology into embedded systems. Let's highlight the key benefits that they bring:

5.4.3 Time-to-Market

Xilinx programmable logic provides several advantages that reduces time-to-market. First, a broad range of IP support from Xilinx and a ever growing number of third party IP partners provide quick access to key design building blocks. Second, as benchtop programmable solutions, they allow the system designer to achieve a functional hardware platform more rapidly than any alternative. And third, programmable devices are standard parts that are easy to reproduce quickly in limited-to-high volumes to capture a position in strategic accounts before the competition.

5.4.4 Rapid Software Development

Software development is one of the biggest issues in integrating Bluetooth technology. And, obviously, since programmable logic can achieve functional hardware sooner it creates an advantage in this area. However, this advantage can be even greater when you consider the flexibility that programmability brings to the equation. For instance, it is often desirable to use existing or third party drivers and firmware. With a programmable solution, you have full control over the behavior of the interface ensuring a workable approach. This can be particularly valuable when third party code is involved because it may not be well documented or understood and modifications can raise support and maintenance concerns.

5.4.5 Time-in-Market

Product development by its nature is not an exact science. Bugs and incompatibilities are simply a reality that engineering must deal with. Here, especially Xilinx programmable devices can provide a valuable advantage, as our solutions are inherently **reprogrammable**. Thus, patches for known problems can be put into production as soon as they are validated on the existing hardware revision and can also be deployed to installed systems. This allows you to keep your existing design shipping and greatly reduces the risk of obsolete part inventories and expensive field replacement programs.

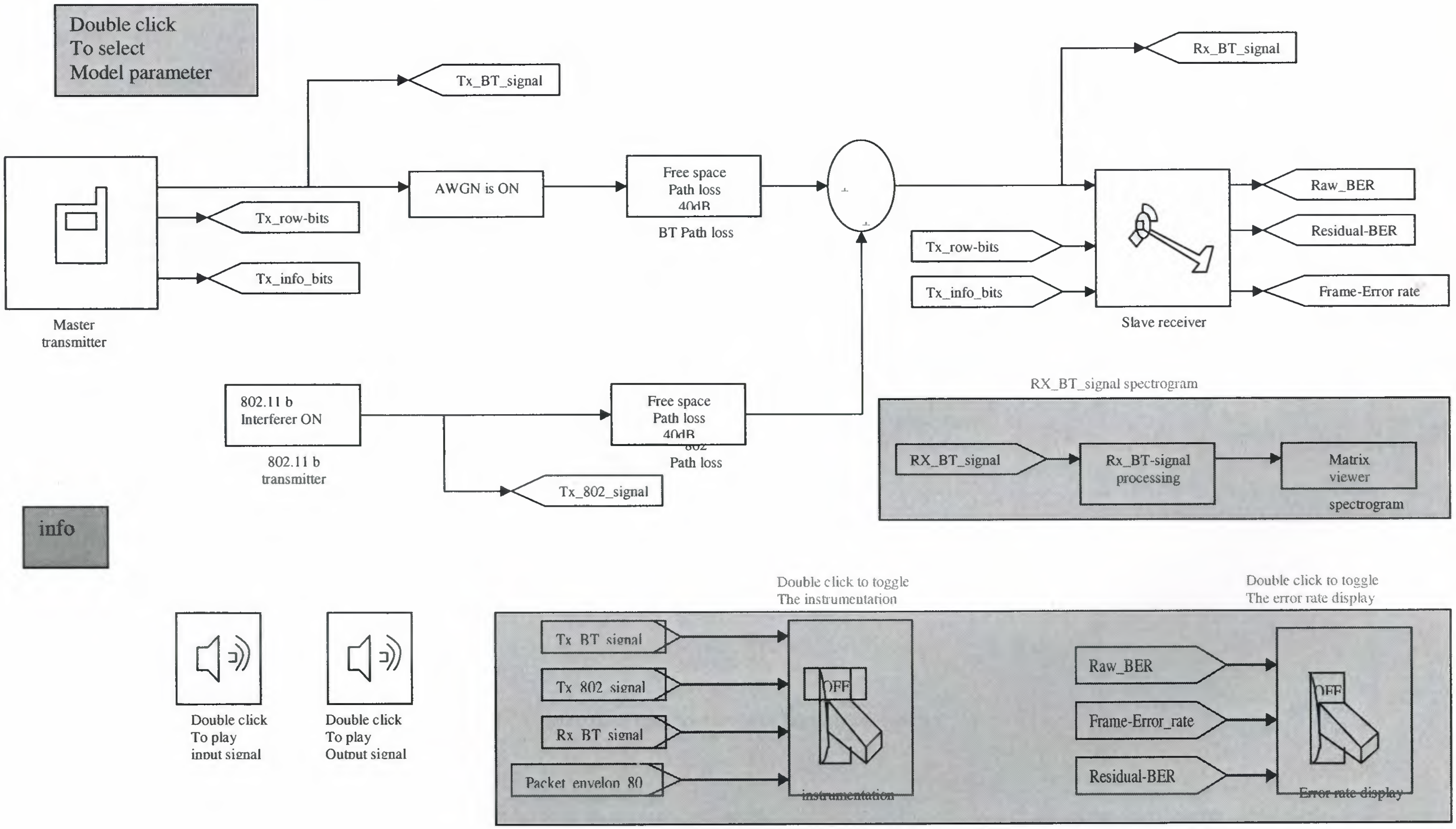
5.4.6 Rapid Design Derivation

A system design is a corporate asset and in today's world of hyper competition and compressed development cycles, these assets must be flexible. Standards evolve, customers request new features, and experience reveals new business opportunities that can be exploited. Thoughtful designs that incorporate programmable logic are inherently more scalable and are superior platforms for rapid and efficient product derivation. Thus, well exploited programmable logic can make your future product roadmap a strategic competitive advantage.

5.4.7 System Level Cost Reduction

In the past, the use of programmable logic was considered an expensive solution. However, times have changed because Moore's Law has worked to the advantage of programmable solutions. Today, $10 will buy 100,000 system gates in volume, off the shelf, and ready to go. And, as these devices usually replace other functions in your design as well, they can often enable real system level cost reductions. Programmable logic has replaced the small cost reduction ASICs of yesterday and brings many other advantages to your system too!

6 Bluetooth Voice Transmissions



6.1 Master transmission

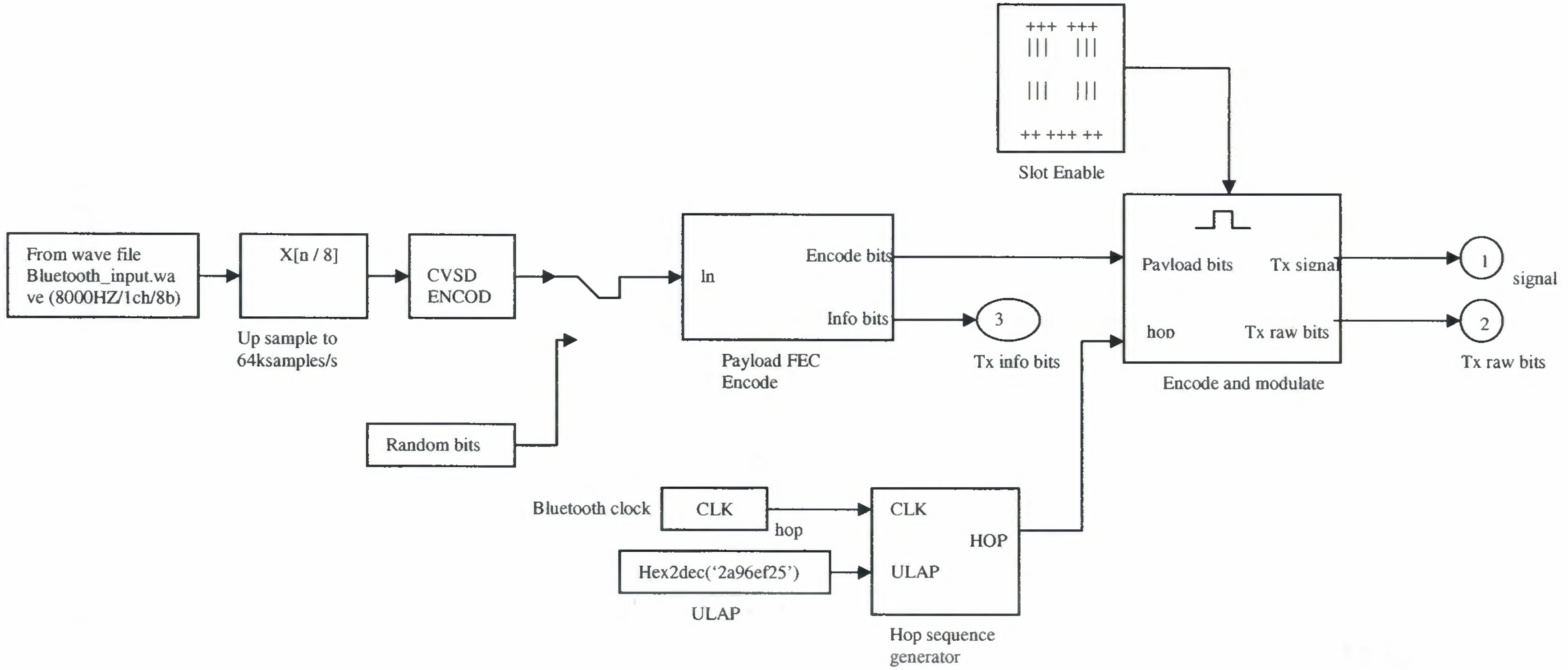


Figure 6.1: Bluetooth voice/master transmitter

.1 Payload FEC Encode

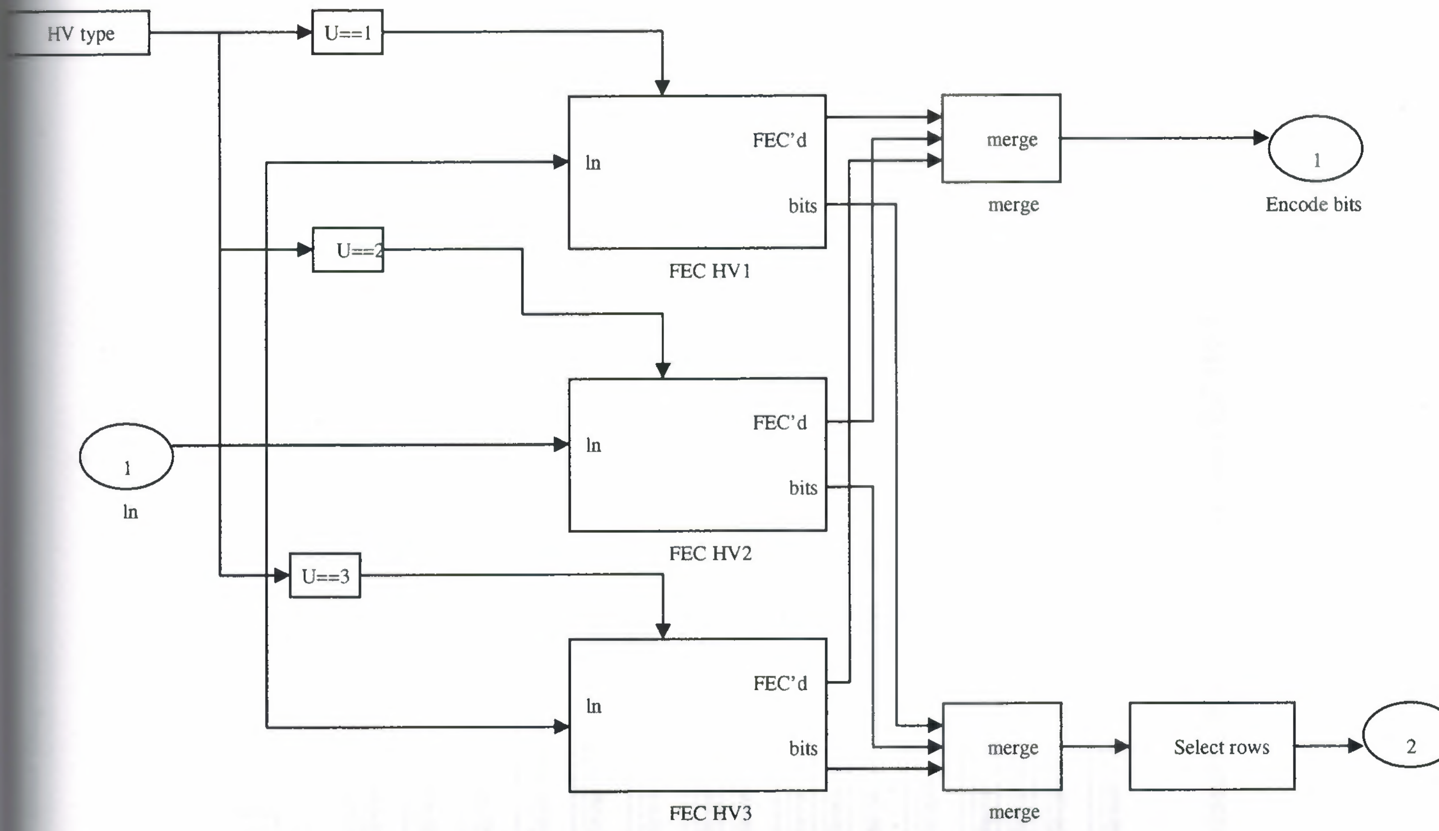


Figure 6.1.2: Master Transmitter/Payload FEC Encode

6.1.1.2 FEC HV2

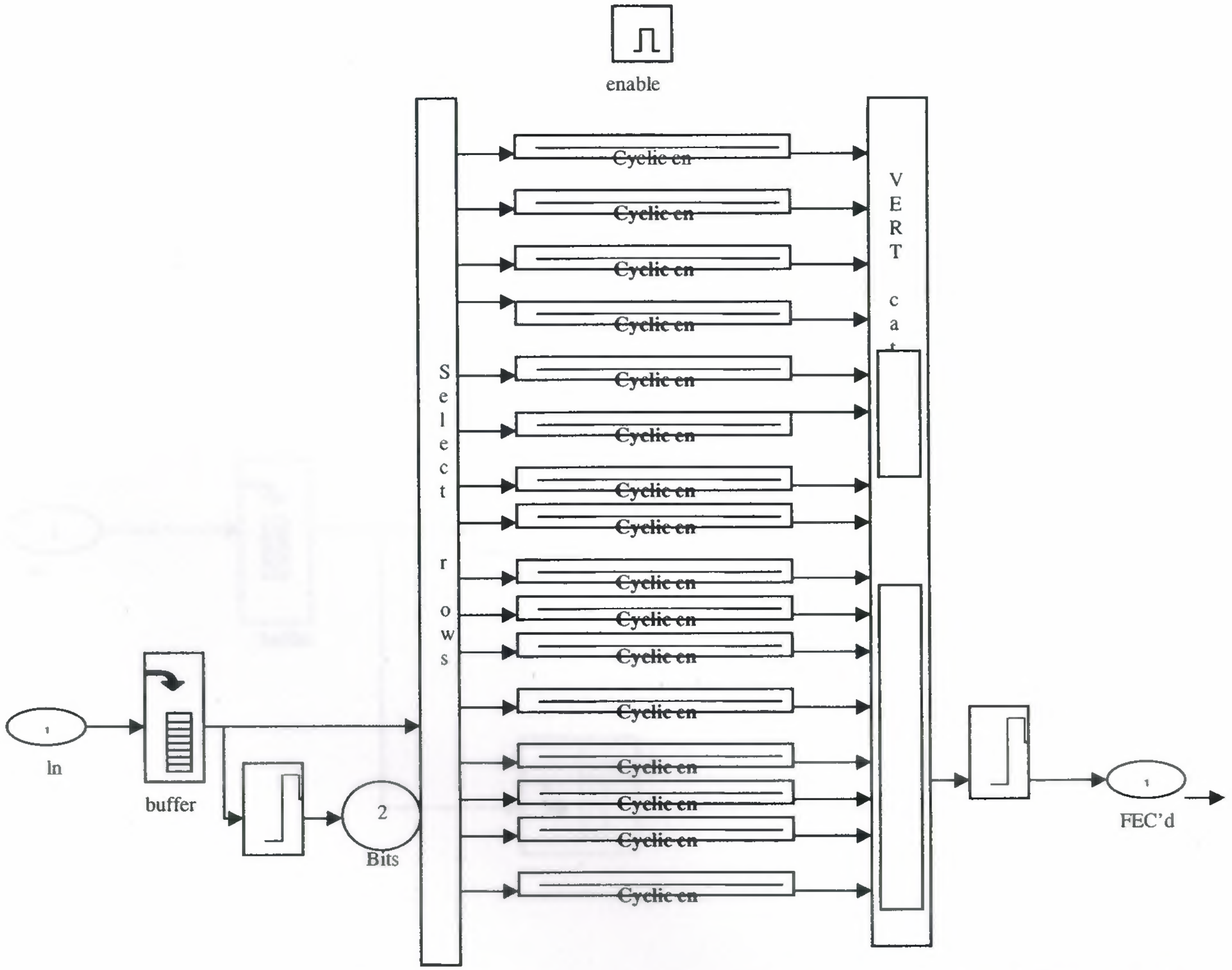


Figure6.1.1.2: Master Transmitter/Payload FEC Encode/FEC HV2

6.1.1 FEC HV1

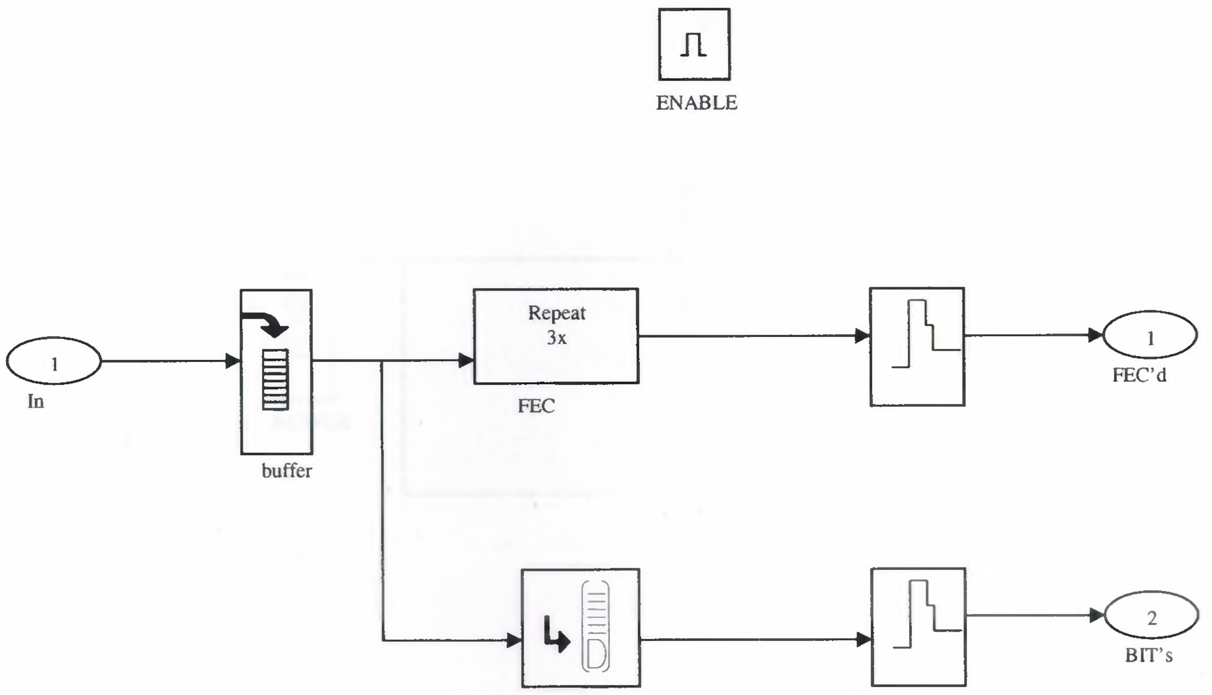


Figure6.1.1.1: Master Transmitter/Payload FEC Encode/FEC HV1

6.1.1.3 FEC HV3

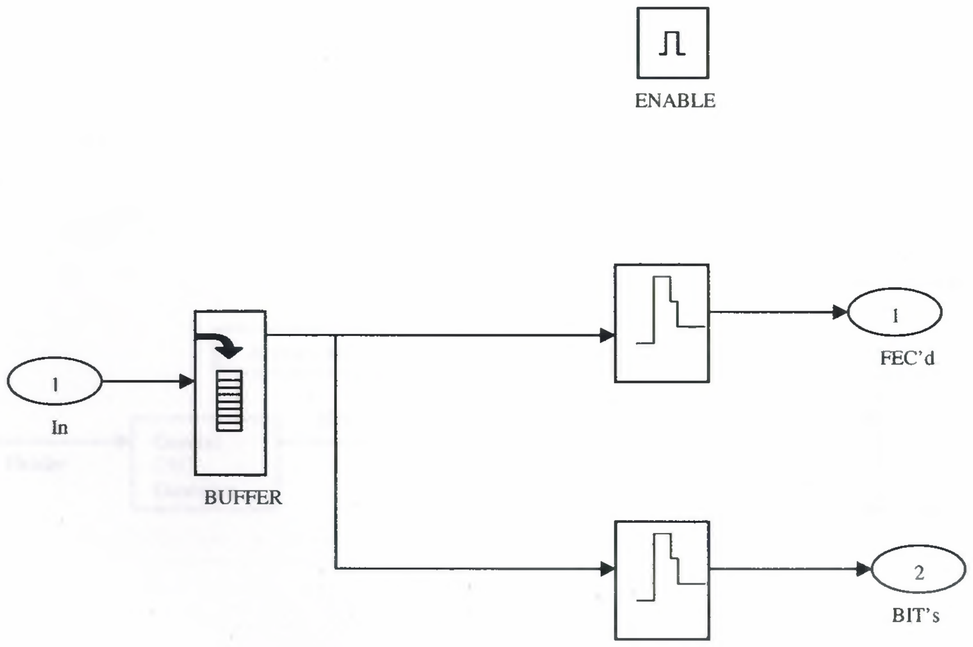


Figure6.1.1.3: Master Transmitter/Payload FEC Encode/FEC HV3

6.1.2 Encode and Modulate

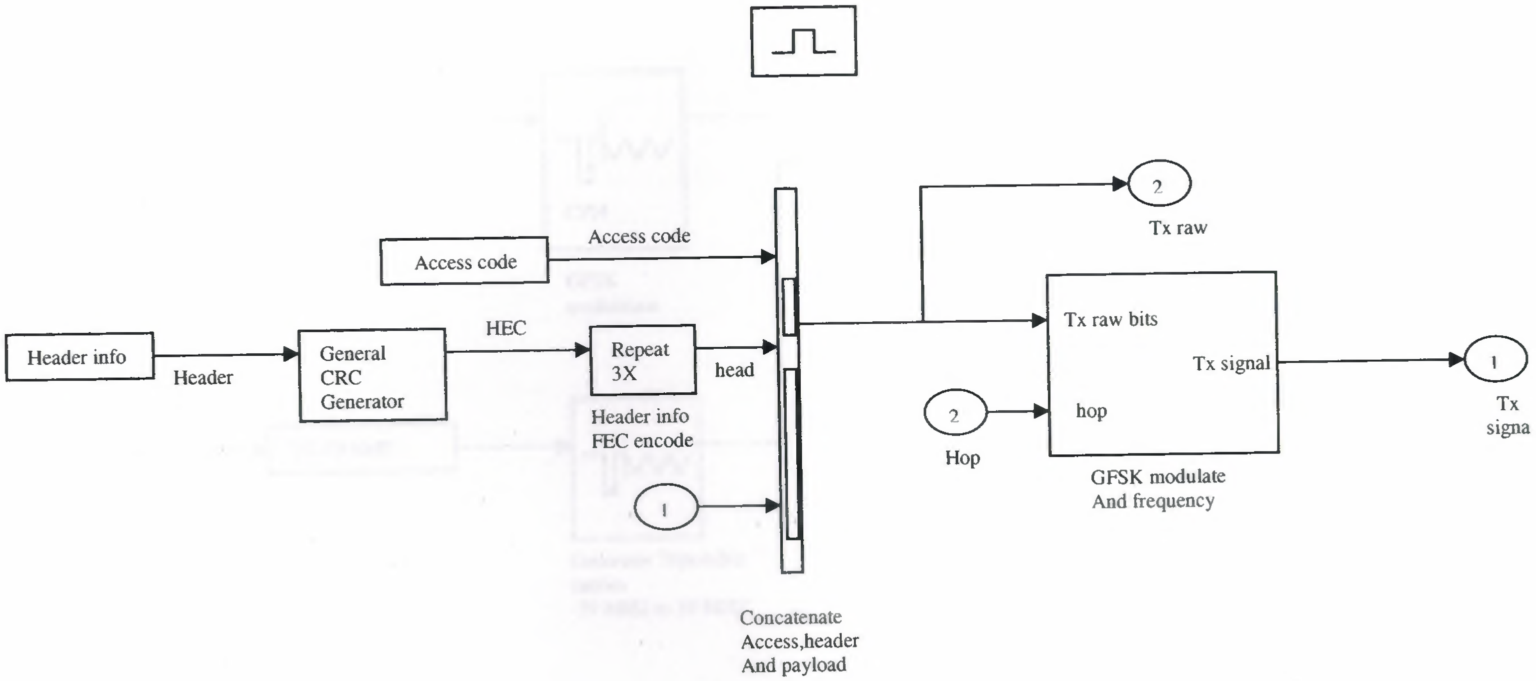


Figure 6.1.2: Master Transmitter/Encode and Modulate

6.1.2.1 GFSK modulate and frequency hop

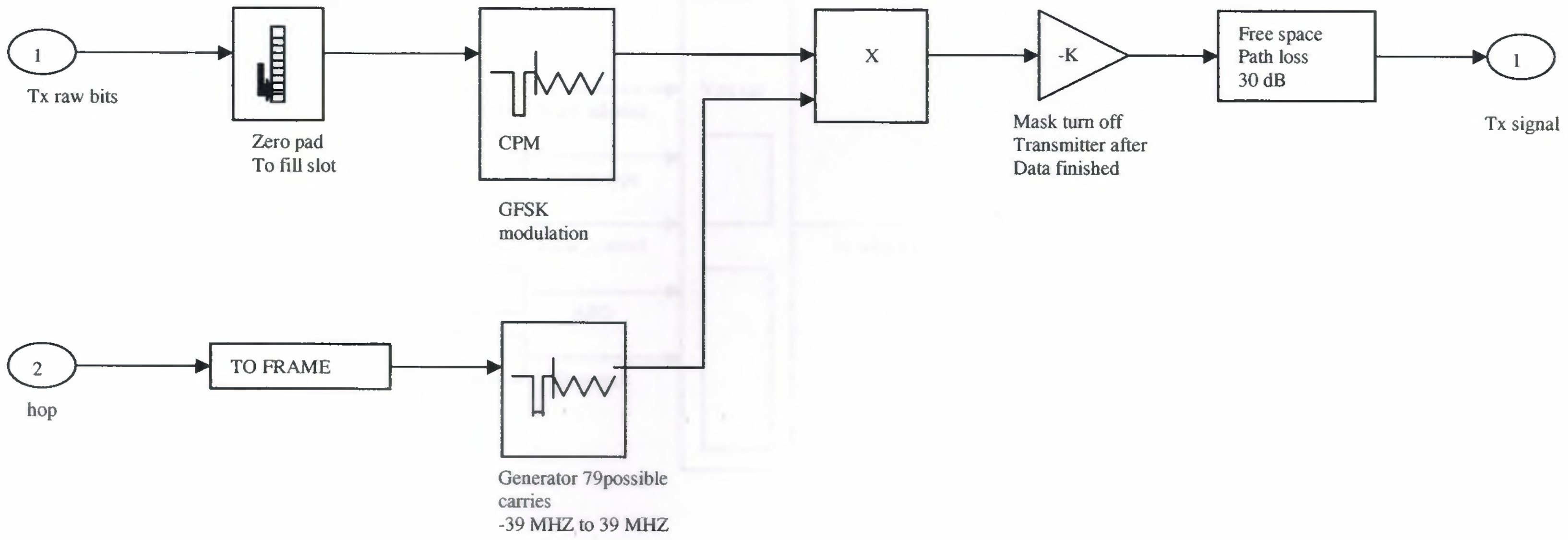


Figure6.1.2.1: Encode and Modulate/GFSK modulate and frequency hop

6.1.2.2 Header Info

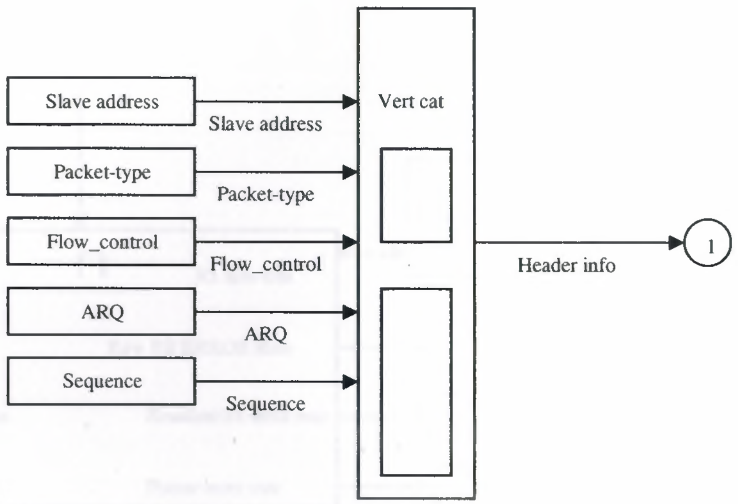


Figure 6.1.2.2: Encode and Modulate/header info

6.2 Slave Receiver

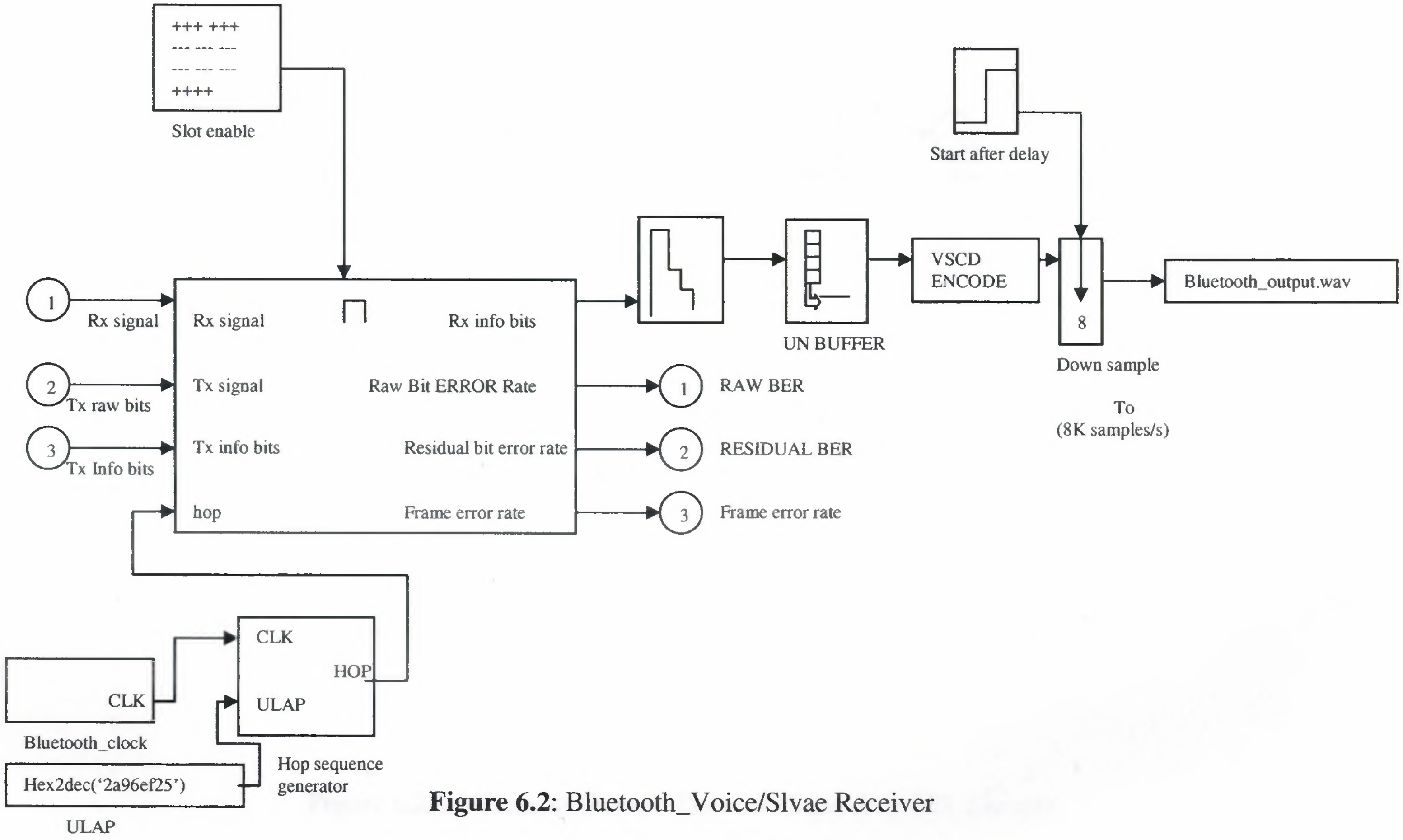


Figure 6.2: Bluetooth_Voice/Slvae Receiver

6.2.1.2 Header Info FEC Decode

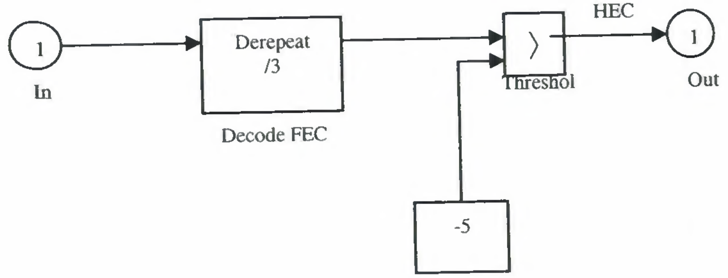


Figure 6.2.1.2: Demodulate and Decode/Header Info FEC Decode

.2.1 Demodulate and Decode

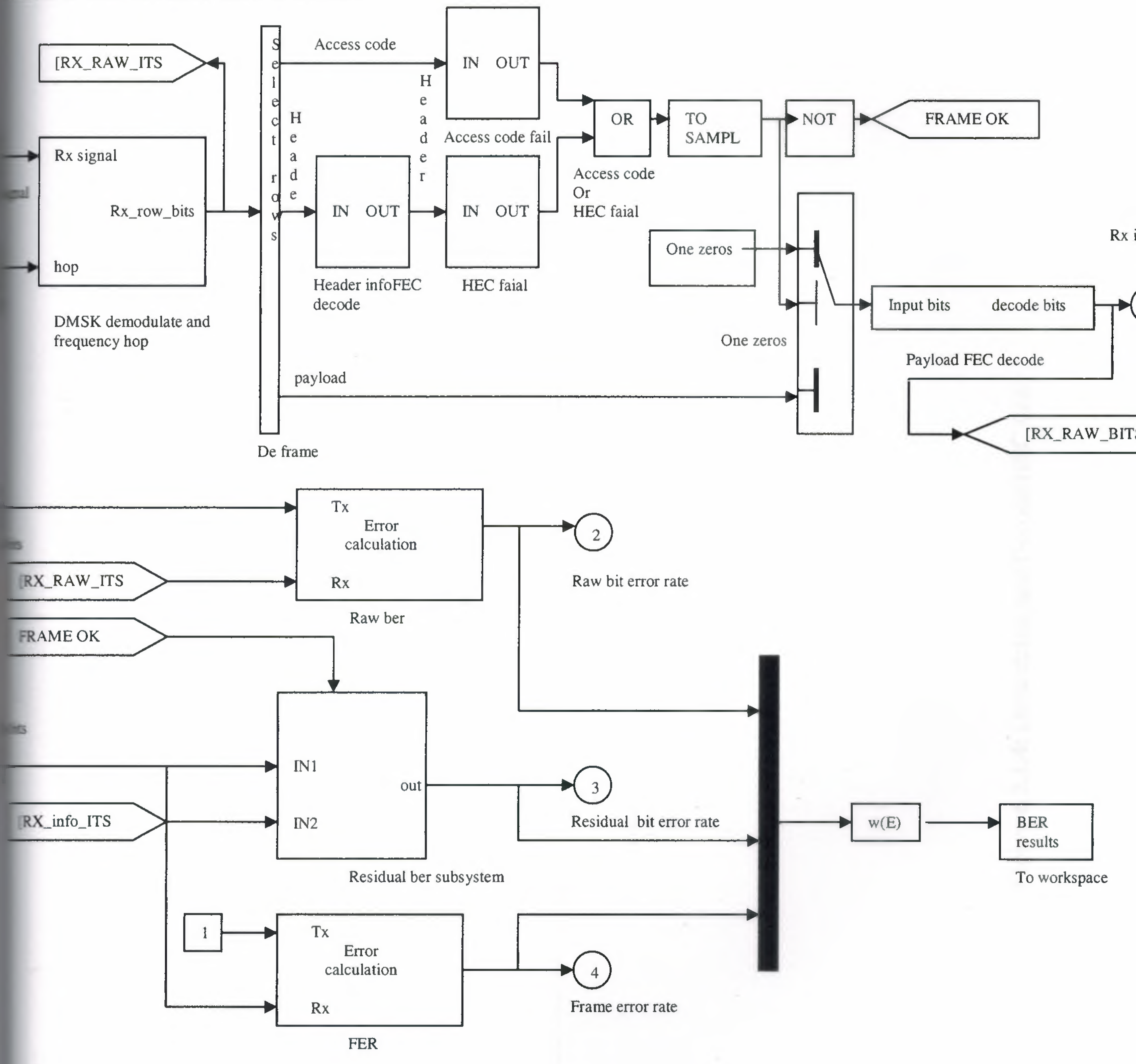


Figure 6.2.1: Slave_Reciever/Demodulate and Decode

6.2.1.4 HEC Fail

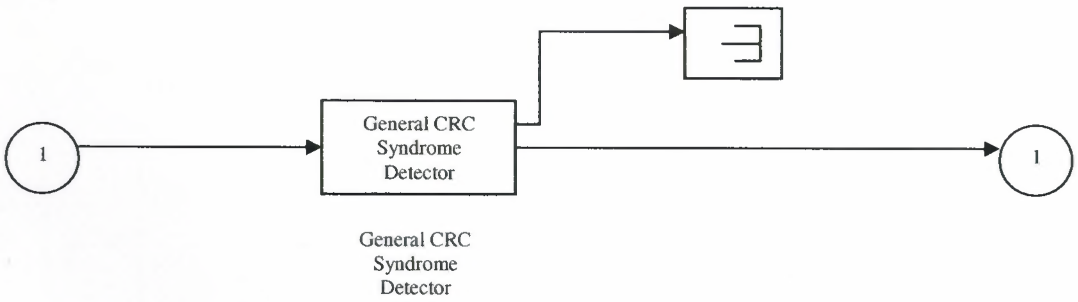


Figure 6.2.1.4: Demodulate and Decode/HEC Fail

6.2.1.3 Access Code Fail

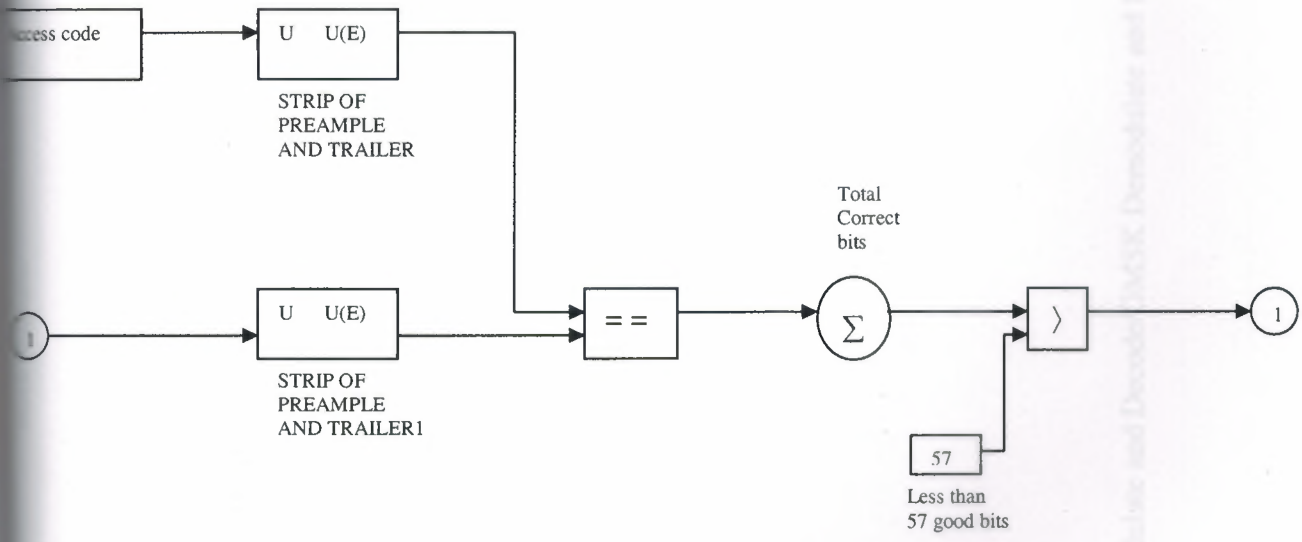


Figure 6.2.1.3: Demodulate and Decode/Access Code Fail

6.2.1.1 GMSK Demodulate and Frequency Hop

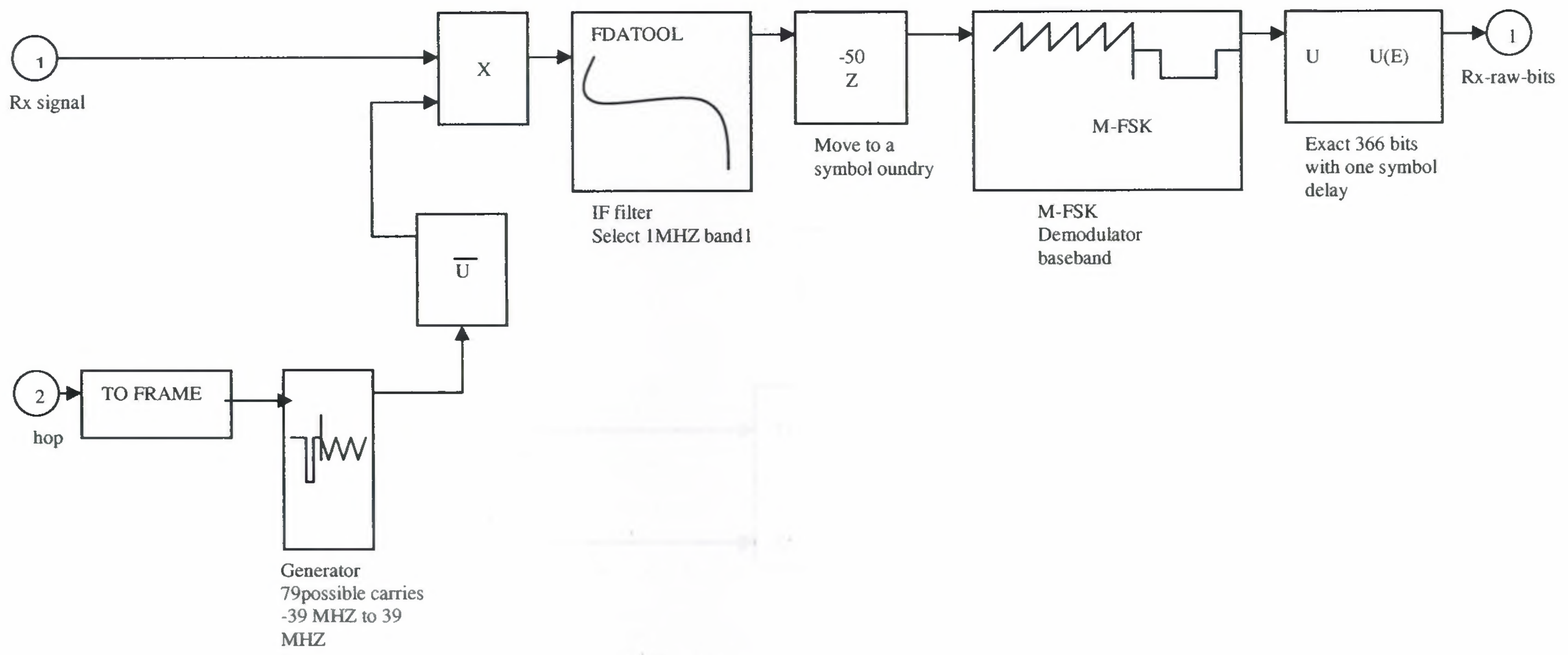


Figure 6.2.1.1: Demodulate and Decode/GMSK Demodulate and Frequency Hop

6.2.1.7 Residual BER Subsystem

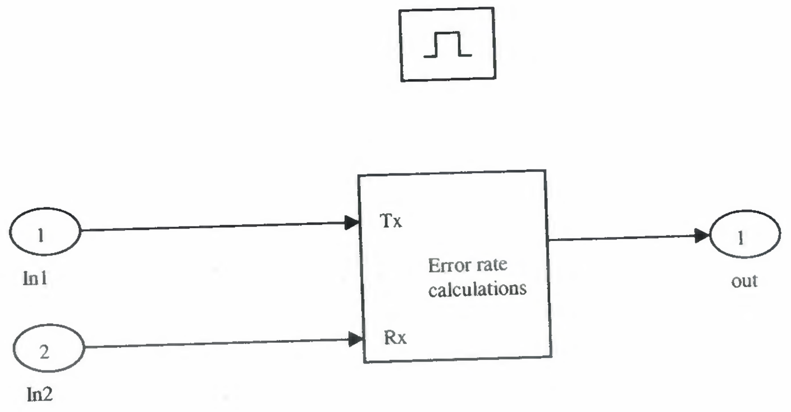


Figure 6.2.1.7: Demodulate and Decode/Residual BER Subsystem

6.2.1.5 One Zeros

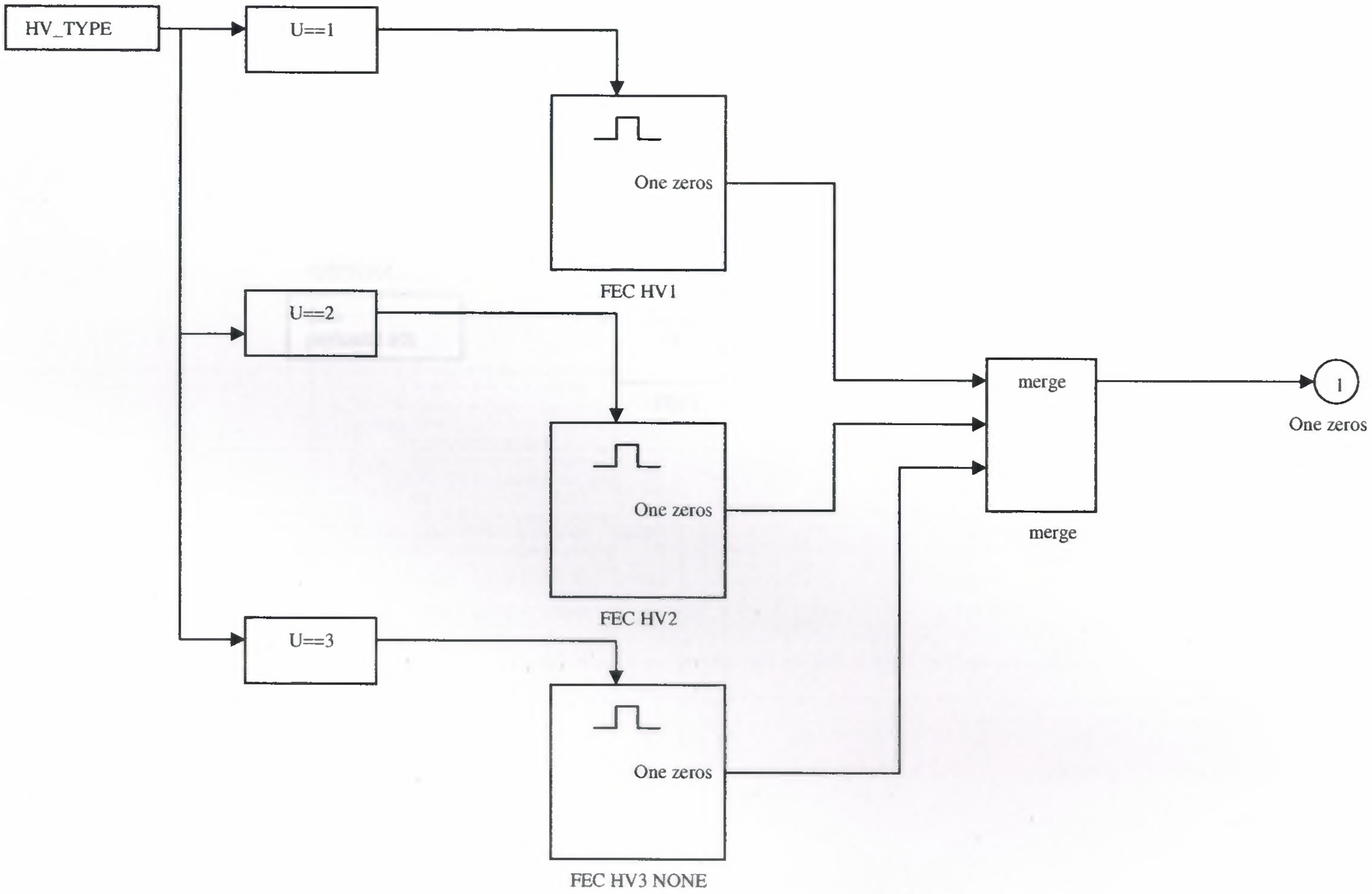


FIGURE 6.2.1.5: Demodulate and Decode/One Zeros

6.2.1.5.1 One Zeros/FEC HV1

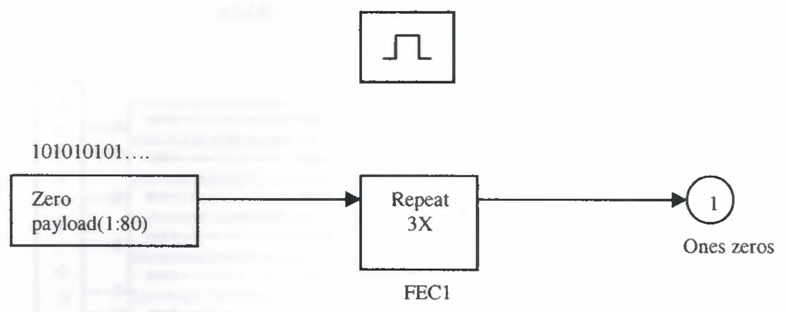


Figure 6.2.1.5.1: Demodulate and Decode/One Zeros/FEC HV1

6.2.5.1.2`One Zeros/FEC HV2

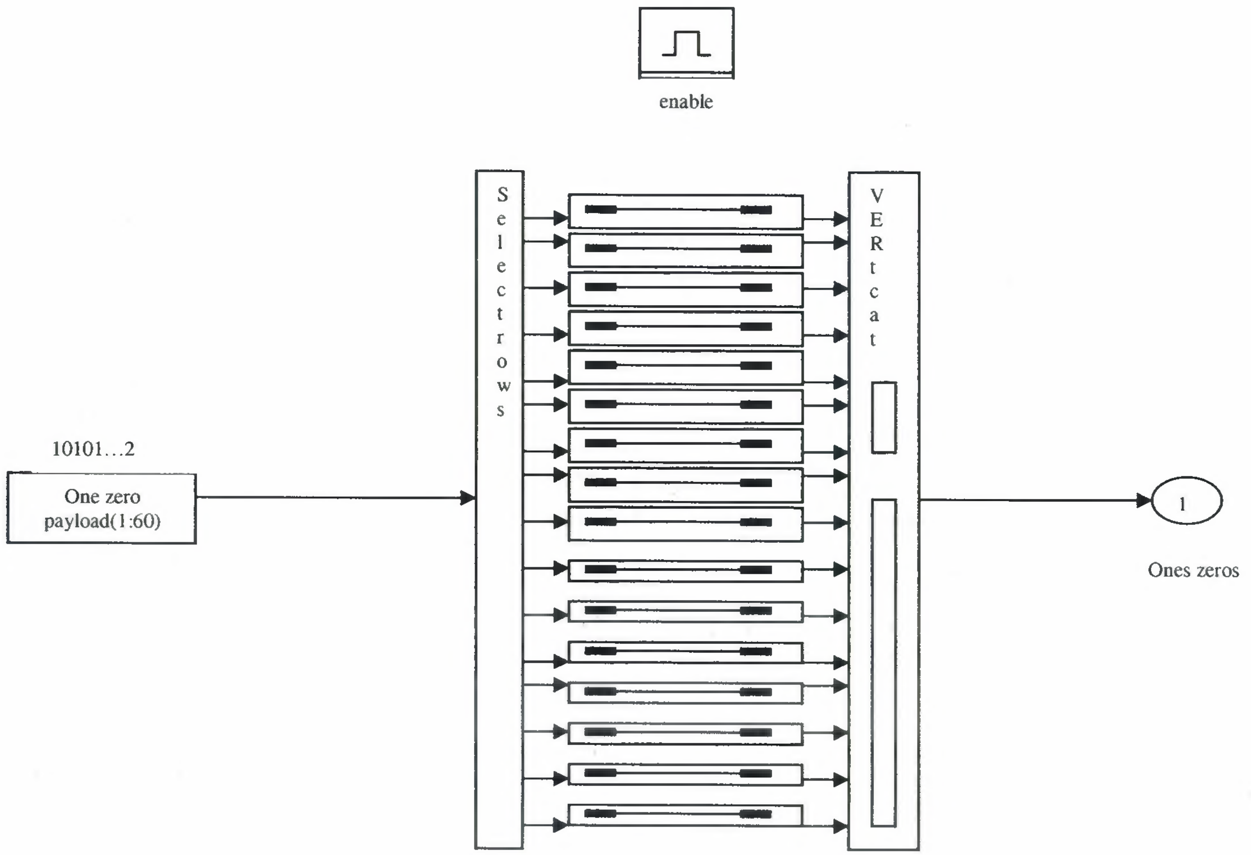


Figure 6.2.5.1.2:Demodulate and Decode/One Zeros/FEC HV2

6.2.5.1.3 One Zeros FEC HV3

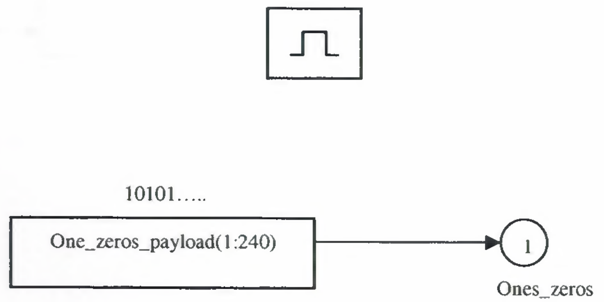


Figure 6.2.5.1.3: Demodulate and Decode/One Zeros/FEC HV3

6.2.1.6 Payload FEC Decode

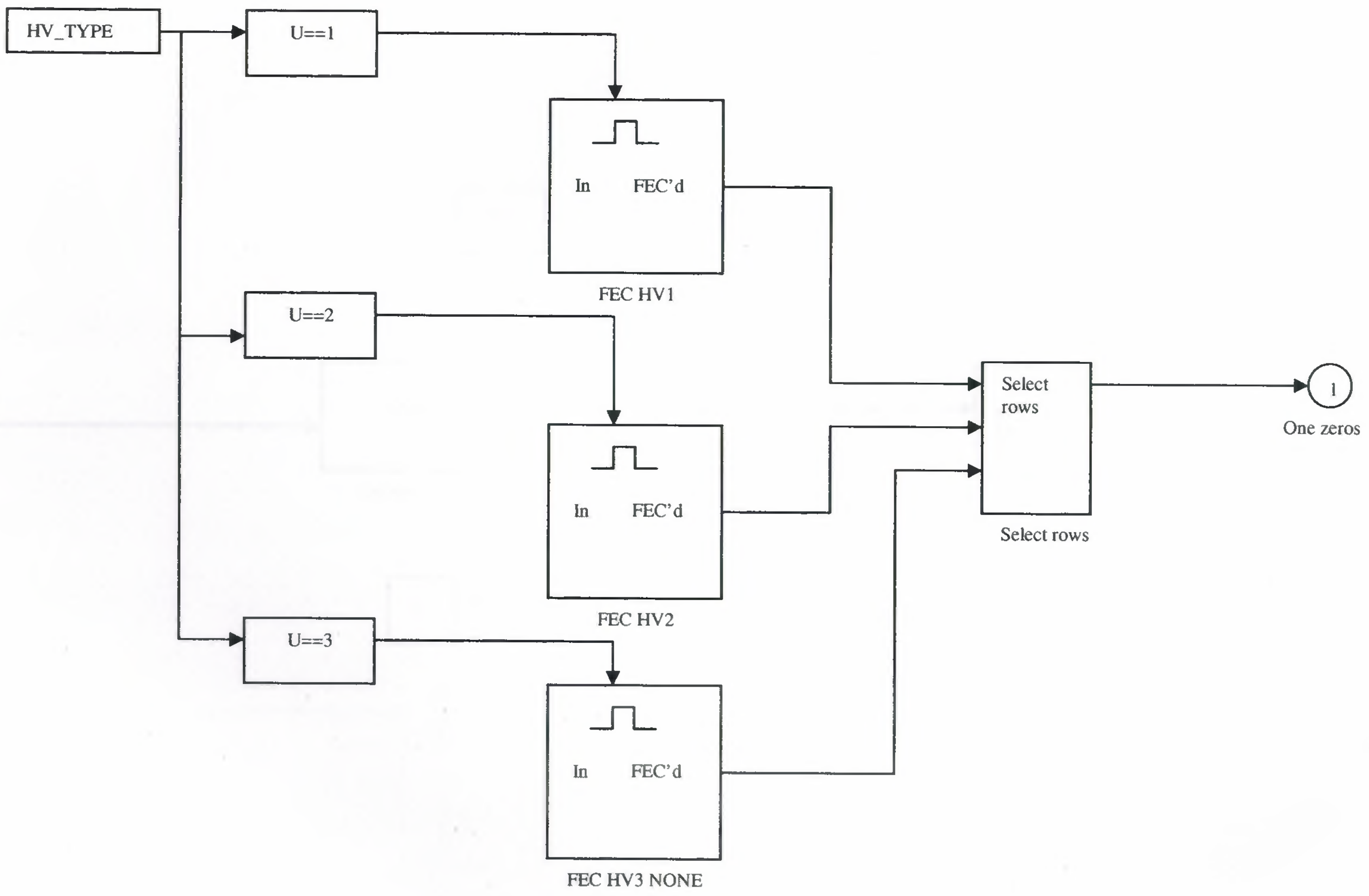


Figure 6.2.1.6: Demodulate and Decode/Payload FEC Decode

6.2.1.6.1 FEC HV1

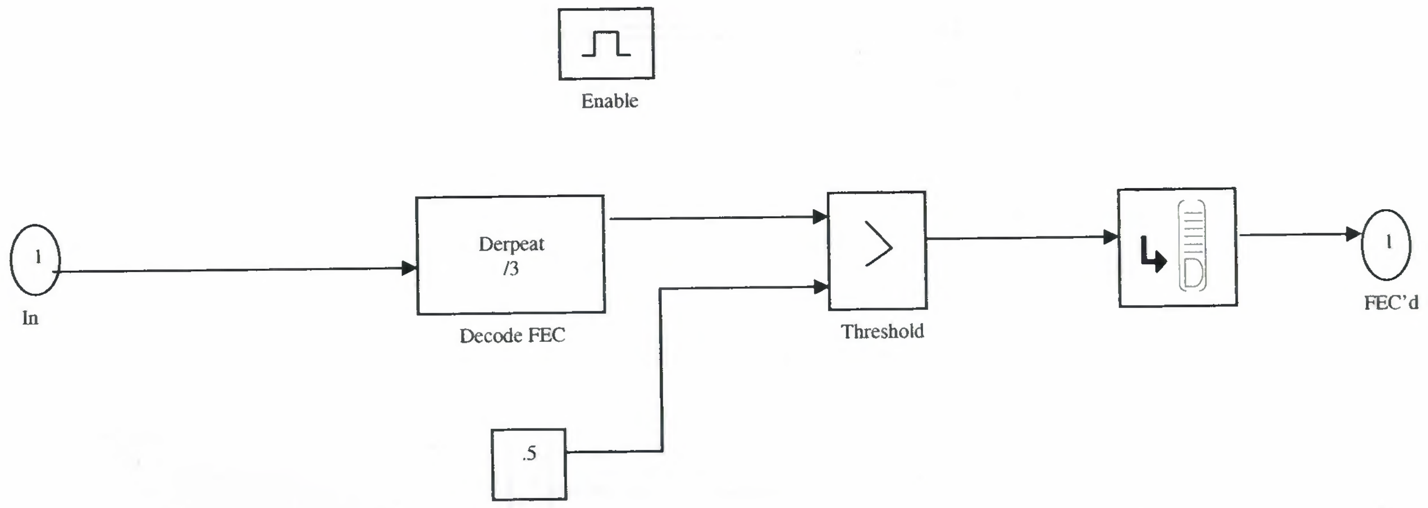


Figure 6.2.1.6.1: Demodulate and Decode/Payload FEC Decode/FEC HV1

6.2.1.6.2 FEC HV2

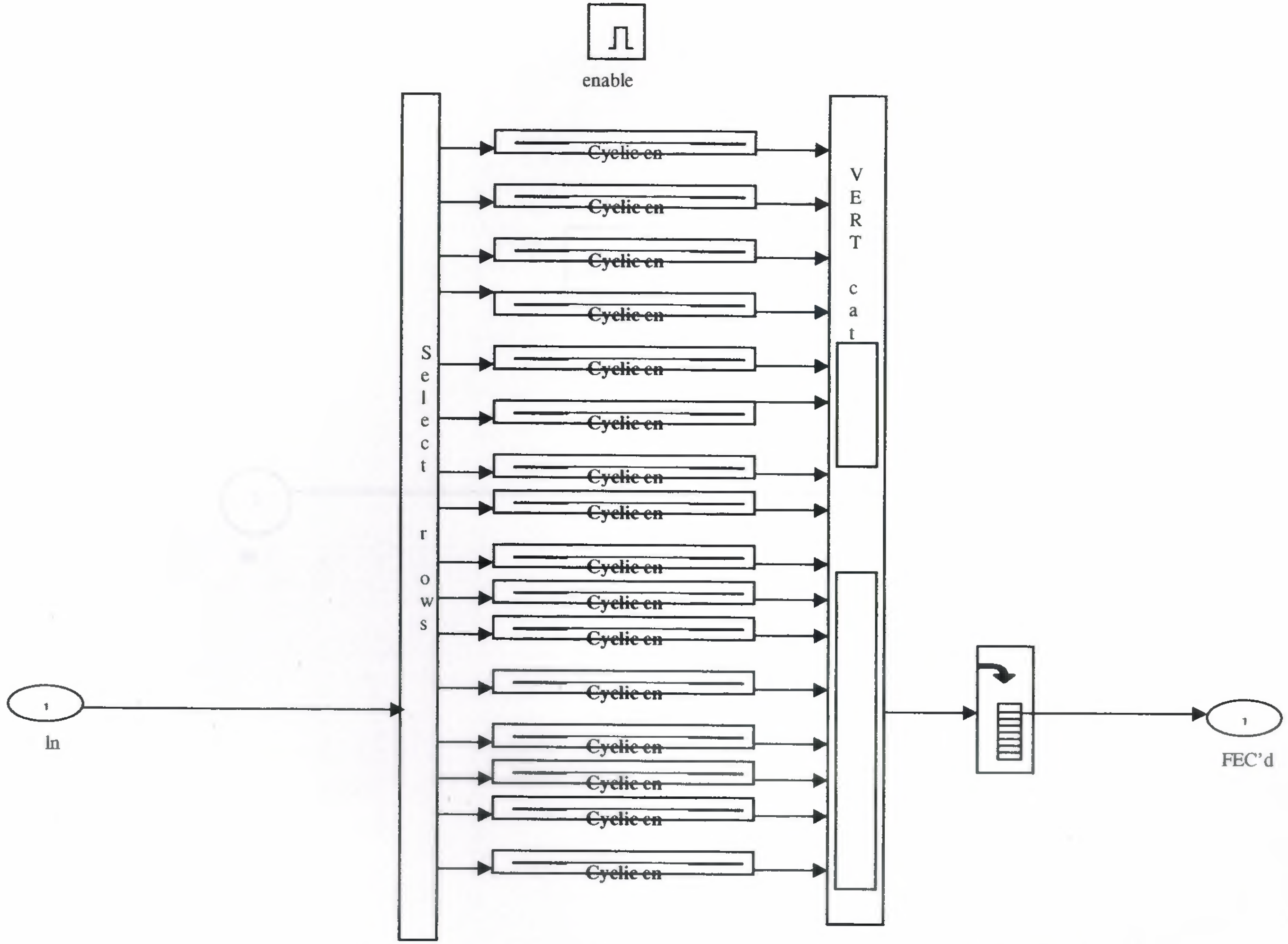


Figure 6.2.1.6.2: Demodulate and Encode/payload FEC Decode/FEC HV2

6.2.1.6.3 FEC HV3

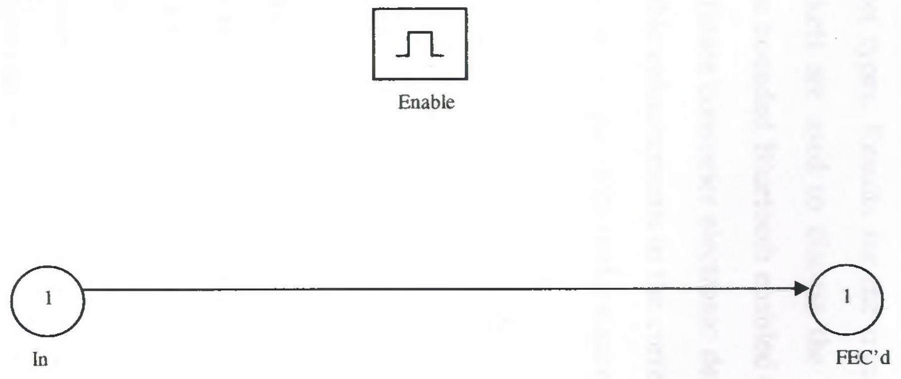


Figure 6.2.1.6.3: Demodulate and Decode/Payload FEC Decode/FEC HV3

8. CONCLUSION

This paper considers issues such as residential coverage and achievable bit rate using the Bluetooth personal area network (PAN) standard. Link budget analysis is performed by combining detailed link level physical layer simulations with site specific power predictions from a state-of-the-art indoor propagation model. Assuming a 1 mW transmit unit, coverage plots are generated at 2.4 GHz for an example single and multi-storey residential environment. The investigation considers Bluetooth data medium (DM) and data high (DH) packet types. Results for the transmission of symmetric asynchronous data link (ACL) packets are used to discuss the bit rate capabilities of various time-bounded and non-time bounded Bluetooth enabled consumer electronic devices. To meet the bit rate needs of future consumer electronic devices, QPSK, 16-QAM and 64-QAM are proposed as possible enhancements to the current GFSK mode. Using physical layer simulations, the coverage and data rate performance of these new modes are analysed and compared with those of standard Bluetooth. The use of linear receive architectures and coherent modulation, although adding significantly to the unit cost, is shown to significantly improve radio sensitivity. Results indicate that high bit rate QAM operation is now possible over an extended coverage area.

There are many applications where wireless connections of various PDA devices are required. There is a demand for the mutual work of the IEEE 802.11 WLAN and Bluetooth devices. As they work on the same operating frequency of the 2.4 GHz ISM band, interference affect must be exposed on each other. In this work we investigate performance degradation due to interference effects. The performance is analyzed according the simulation that is based on network model. The results are presented in the terms of the probability of bit errors and throughput in the dependence of the signal strength.

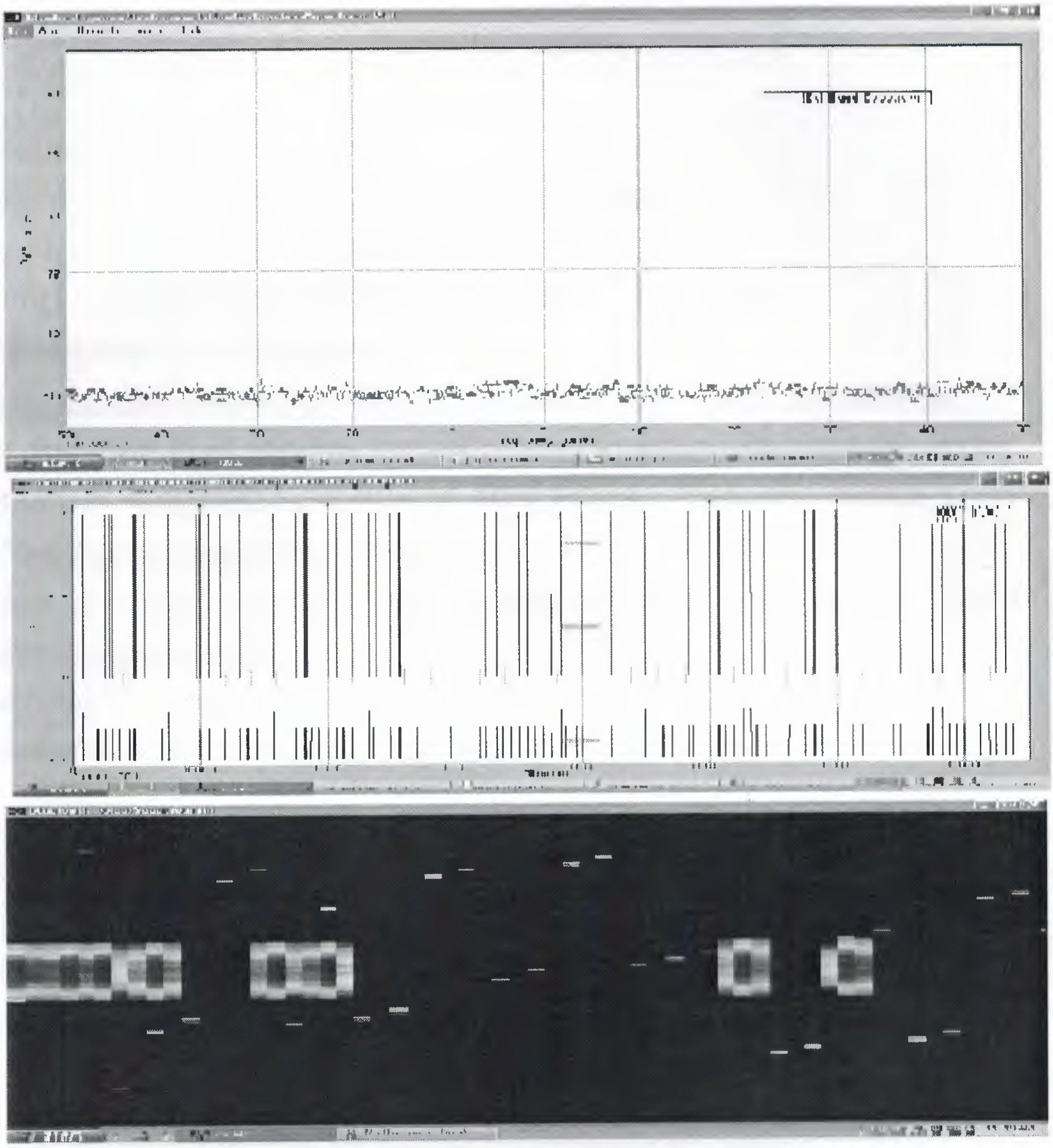


Figure 6.3 Output

REFERENCES

[1] Vineet Sachdev, System Engineer

[2] Trueposition Inc. 1111 West DeKalb Pike Wayne, PA 19087

[3] Asha Mehrotra, "GSM System Engineering"

[4] MOBILE COMMUNICATIONS SERIES, Artech House Publishers.

[5] Brian McIntosh "Telecommunications" http://telecomindustry.about.com/business/telecomindustry/library/weekly/aa1115999.ht

[6] Dick Tracy "The Applications We Promote...." http://www.comm-nav.com/commnav.htr

[7] GRAYSON WIRELESS, a division of Allen Telecom. "Geometrix Wireless Location Sensor" http://java.grayson.com/geodatasheet.htrr

[8] Louis A. Stilp "Examining the Coming Revolution in Location Services" http://www.trueposition.com

[9] Paul J, Bouchard "AccuCom Wireless Service Inc." http://www.Global-Images.com

[10] Tutorial "How GPS works?" http://www.trimble.com