Universitatea Politehnica Bucuresti
Facultatea de Automatica si Calculatoare
Catedra de Calculatoare
An universitar 2004-2005

CALCULATOARE NUMERICE
Proiect de semestru – anul III

Indrumator:  Ş.l. Dr. Ing. Decebal Popescu
Studenti:  
Cadar Filis - CB 331
Mitacu Bogdan - CB 331
Molovata Victoria - CB 331
Soltan Sebastian CB - 331
Urzica Andreea CB - 331
Project Subject

Establishing a *connection* between different wireless technologies: IrDA, Bluetooth, WiFi

There are many technologies very useful for establishing wireless connections and the most notable among them are Bluetooth, Infrared, HomeRF, IEEE 802.11b (WiFi) and HyperLAN. This technologies compete in certain fronts and are complimentary in other areas.

However, this paper will only compare Infrared (IrDA), WiFi and Bluetooth technology where all of them provide short-range communications and offer wireless connectivity services.

In the beginning, we will present an overview of Infrared (IrDA), Bluetooth and WI-FI.

IrDA (Infrared) is used for high-speed, short-range, line-of-sight and point-to-point data transfer.

Bluetooth on the other hand, is the name of a short-range radio frequency (RF) technology that replaces the need for cabled connection. Bluetooth allows computers, peripherals, and other devices to communicate with each other without having a physical connection, without needing direct line-of-sight or extra communication protocols.

Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well as data transmission. Wi-Fi stands for Wireless Fidelity. It is a way of digital data transmission over radio channels, this technique is allowing many users simultaneously to gain access to Internet (multiple wireless access).
The detail discussion is towards comparing these wireless technologies.

The demo application features a chat capability of desktop PCs connected via Bluetooth enabled devices that have implementation of the Microsoft Bluetooth Protocol Stack (due to the fact that the application uses a dynamic link library that is based on and uses the .net framework versions 1.1 and 2.0 b2 (latest stable build – microsoft msdn library) ).
Table of Contents

1. Infrared (IrDA) Technology
   a. Presentation
   b. The IrDA Standard
   c. IrDA’s Strong-points
   d. Applications Suited for IrDA

2. Bluetooth Technology
   a. Presentation
   b. History
   c. How Bluetooth Technology Works
   d. Power Consumption
   e. Bluetooth Security
   f. The Bluetooth Baseband Protocol
   g. Modes of Operation
   h. Types of Bluetooth Devices

3. Wi – Fi Technology
   a. Presentation
   b. The 802.11 Family
   c. Definition of Terms Used
      o Hot Spot
      o Virtual Private Network (VPN)
      o War driving
      o Wired Equivalent Privacy (WEP)
      o Phase-Shift Keying (PSK)
      o Ethernet
   d. Wi-Fi innovation
   e. Wi-Fi’s target
   f. Using Enterprise-Level Wi-Fi Technology
   g. Extending a Network with a Wi-Fi LAN

4. Bluetooth vs IrDA

5. Wi - Fi vs. Bluetooth
   a. 802.11b – Advantages and Disadvantages
   b. Bluetooth – Advantages and Disadvantages
   c. Conclusions

6. Bluetooth Desktop Chat

7. References
1. Infrared (IrDA) Technology

Presentation

Portable computing has become synonymous with the rapidly changing world of technology in today's work environment. Every company recognizes that in order to compete they must keep pace, as well as deploy and manage this new technology in order to maintain their competitive edge. New economic trends in the global economy will continue to push companies to find new ways to enhance productivity and maintain flexibility among their employees.

In fact, portable computing according to recent studies is poised for some very dramatic growth. Many estimates suggest that the number of portable computers sold in 1996 will double from the 5.6 million units sold in 1993. A trend that is likely to continue as companies deploy their workforce to a more "mobile office concept". One obstacle to achieving the goal of mobile connectivity has always been the limitation of the cable connection. Whether you are connecting to the printer, your network or exchanging data with the desktop, the cable connection is viewed as a hindrance to the effective and efficient use of the portable computer.

The initials IrDA stand for Infrared Data Association.

IrDA is a non-profit trade association with a membership of over hundreds of companies in the computers and telecommunications industry, including components, hardware, software, & adapters manufacturers.
The IrDA Standard

The IrDA standard is a set of specifications for providing a universal two-way wireless infrared data communications, based on a practical cost, short-range point-to-point user model.

The standard defines the physical characteristics of the interface, the communications protocols that provide for different needs, and the transmission speeds at which the infrared device communicates.

The two basics of the infrared communication standards are IrDA-Data and IrDA-Control:

**IrDA-Data** defines the standard for the wireless, two-way infrared data transmission between two devices and consists of a set of mandatory protocols: PHY (Physical), IrLAP (Link Access), and IrLMP (Link Management).

**IrDA-Control** is the infrared standard that allows wireless peripherals such as keyboards, mouse, game pads, joysticks, and other pointing devices to interact with many types of host devices. Host devices include PCs, home appliances, game consoles, and TV/Web set top boxes. IrDA-Control is not the same as the standard TV Remote Control. IrDA-Control has its own set of mandatory protocols: PHY (Physical), MAC (Media Access Control), and LLC (Logical Link Control).

Implementing the IrDA infrared communication standards is to ensure the interoperability in between all types of wireless digital infrared communication devices.

**Direct infrared** is a point-to-point, typically one-to-one communication. Which requires line of sight and is a secure form of data transmission and reception.

Hoya IrDA-standard wireless infrared solution is an example of direct infrared.

**Diffuse infrared** allows many-to-many connections, does not require direct line of sight and can be uni-directional or bi-directional. Since it is based on visible light, it is a secure form within a room. Financial trading floors are an example of diffuse infrared.

**Radio frequency** is not secure in that it can penetrate through walls and is subject to uncontrolled interference. It is typically higher in power consumption than directed infrared and requires FCC certification.

It is a wireless data connection using infrared light by a cost effective transceiver signaling technology for two-way digital data exchange. It provides reliable, high-speed digital communications between two devices for up to 4 Mbits/sec of data transmit rate.
IrDA’s Strong-points

The benefits for IrDA-standard infrared connection technology includes:

✓ Offers a universal wireless standard for connecting all portable infrared-enabled devices
✓ Easy, effortless implementation
✓ Economical alternative to other connectivity solutions
✓ Reliable, high speed connection
✓ Safe to use in any environment; can even be used during air travel
✓ Eliminates the hassle of cables
✓ Allows PC’s and non-PC’s devices to communicate with each other
✓ Enhances mobility by allowing users to simply “plop and connect”

Using IrDA-standard wireless infrared connection to access the LAN is as secure as using a cable at any other access point on the network. You need to be an authorized user on the subnet.

Wireless infrared connection is often more reliable than wired solutions. The infrared port will prove more reliable than wired connections because we will have eliminated wear-and-tear. No pins to bend, no plugs to jam.

The Infrared Physical Layer is defined to guarantee error-free communication from the minimum to maximum distance and a given reception or viewing angle in a typical environment where ambient light or other sources of interference may be present.

Although the IrDA-standard only specifies a connection distance from zero to one meter, many IrDA-compliant products can connect at distances greater than one meter. If the portable is farther away from the infrared access point, the connection will be slower. To be IrDA-compliant, a product must be capable of maintaining a constant connection distances.
Applications Suited for IrDA

Infrared port is showing up in many electronic products in order to provide a reliable, fast and wireless connection to the mobile workers with access to services and data exchange. Such as:

- Notebooks and Handheld computers
- PDA’s and Palm devices
- Printers
- Scanners
- Mobile phones & pagers
- Digital Cameras
- Medical and Industrial equipments
- LAN access devices
- Point-Of-Sales systems

Infrared port will soon be seen in copiers, fax machines, overhead projectors, telephones, bank ATM's, credit card readers, game controls, and headsets, etc.

Direct “beaming” of images or files between electronic devices is the most common application for IrDA-standard infrared solution. Future applications are public / business / cellular telephones, consumer electronics, electronic commerce, distribution, warehousing, grocery stores, field service, utility services, medical, automotive, and many other vertical markets.

FIR stands for Fast Infrared transmit mode (IrDA 1.1 Standard), which is the capability to transmit data up to 4 Mbits/sec. SIR stands for Serial Infrared transmit mode (IrDA 1.0 Standard), which is the capability to transmit data at 115.2 Kbits/sec.
2. Bluetooth Technology

Presentation

Bluetooth is a high-speed, low-power microwave wireless link technology, designed to connect phones, laptops, PDAs and other portable equipment together with little or no work by the user. Unlike infra-red, Bluetooth does not require line-of-sight positioning of connected units. The technology uses modifications of existing wireless LAN techniques but is most notable for its small size and low cost. The current prototype circuits are contained on a circuit board 0.9cm square, with a much smaller single chip version in development. The cost of the device is expected to fall very fast, from $20 initially to $5 in a year or two. It is envisioned that Bluetooth will be included within equipment rather than being an optional extra. When one Bluetooth product comes within range of another, (this can be set to between 10cm and 100m) they automatically exchange address and capability details. They can then establish a 1 megabit/s link (up to 2 Mbps in the second generation of the technology) with security and error correction, to use as required. The protocols will handle both voice and data, with a very flexible network topography.
History

In early 1998, a consortium of companies including Ericsson, IBM, Intel, Nokia, and Toshiba formed a special interest group, codenamed "Bluetooth". The group's goal was to develop a low-cost, flexible wireless platform for short-distance communication (< ~10 metres). The Bluetooth 1.0 specifications were released on July 26, 1999, but the technology has only recently become cheap enough for widespread use. The cost of a Bluetooth radio chip has dropped from $20 and is now approximately $5.

Bluetooth uses gaussian frequency shift keying (GFSK) to modulate the data to frequencies around 2.4 GHz. The frequency spectrum is divided up into 79 channels spaced 1 MHz apart. Data is transmitted at 1 Mbps. For security benefits and noise reduction, a Bluetooth transmitter employs frequency hopping, switching channels up to 1600 times a second.

Bluetooth is capable of point-to-point or point-to-multipoint communication. This flexibility allows Bluetooth to be used in a wide variety of applications. Because power consumption is always a concern for mobile devices, Bluetooth has three power classes that can be used depending on how far apart the communicating devices are from one another.

Over the next few years, Bluetooth's use is expected to significantly grow. The Bluetooth consortium is currently writing the specifications for Bluetooth 2.0. Bluetooth 2.0 has been designed to complement existing Bluetooth devices and will offer data transmission rates up to 12 Mbps.

How Bluetooth Technology Works

This technology achieves its goal by embedding tiny, inexpensive, short-range transceivers into the electronic devices that are available today. The radio operates on the globally-available unlicensed radio band, 2.45 GHz (meaning there will be no hindrance for international travelers using Bluetooth-enabled equipment.), and supports data speeds of up to 721 Kbps, as well as three voice channels. The bluetooth modules can be either built into electronic devices or used as an adaptor. For instance in a PC they can be built in as a PC card or externally attached via the USB port.

![Figure 1.1: Different functional blocks in the Bluetooth system](image-url)
Each device has a unique 48-bit address from the IEEE 802 standard. Connections can be point-to-point or multipoint. The maximum range is 10 meters but can be extended to 100 meters by increasing the power.

Bluetooth devices are protected from radio interference by changing their frequencies arbitrarily up to a maximum of 1600 times a second, a technique known as frequency hopping. They also use three different but complimentary error correction schemes. Built-in encryption and verification is provided.

**Power Consumption**

Moreover, Bluetooth devices won't drain precious battery life. The Bluetooth specification targets power consumption of the device from a "hold" mode consuming 30 micro amps to the active transmitting range of 8-30 milliamps (or less than 1/10th of a watt). The radio chip consumes only 0.3mA in standby mode, which is less than 3% of the power used by a standard mobile phone. The chips also have excellent power-saving features, as they will automatically shift to a low-power mode as soon as traffic volume lessens or stops.

Bluetooth devices are classified according to three different power classes, as shown in the following table.

<table>
<thead>
<tr>
<th>Power Class</th>
<th>Maximum Output</th>
<th>Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100 mW</td>
<td>(20 dBm)</td>
</tr>
<tr>
<td>2</td>
<td>2.5 mW</td>
<td>(4 dBm)</td>
</tr>
<tr>
<td>3</td>
<td>1 mW</td>
<td>(0 dBm)</td>
</tr>
</tbody>
</table>

But beyond untethering devices by replacing the cables, Bluetooth radio technology provides 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.

Designed to operate in a noisy radio frequency environment, the Bluetooth radio uses a fast acknowledgment and frequency hopping scheme to make the link robust. Bluetooth radio modules avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. Compared with other systems operating in the same frequency band, the Bluetooth radio typically hops faster and uses shorter packets. This makes the Bluetooth radio more robust than other systems. Short packages and fast hopping also limit the impact of domestic and professional microwave ovens. Use of Forward Error Correction (FEC) limits the impact of random noise on long-distance links. The encoding is optimized for an uncoordinated environment.
Bluetooth security

Bluetooth guarantees security at the bit level. Authentication is controlled by the user by using a 128 bit key. Radio signals can be coded with 8 bits or anything upto 128 bits. The Bluetooth radio transmissions will conform to the safety standards required by the countries where the technology will be used with respect to the affects of radio transmissions on the human body. Emissions from Bluetooth enabled devices will be no greater than emissions from industry-standard cordless phones. The Bluetooth module will not interfere or cause harm to public or private telecommunications network.

The Bluetooth baseband protocol

The Bluetooth baseband protocol is a combination of circuit and packet switching. Slots can be reserved for synchronous packets. Each packet is transmitted in a different hop frequency. A packet nominally covers a single slot, but can be extended to cover up to five slots. Bluetooth can support an asynchronous data channel, up to three simultaneous synchronous voice channels, or a channel, which simultaneously supports asynchronous data and synchronous voice. It is thus possible to transfer the date asynchronously whilst at the same time talking synchronously at the same time. Each voice channel supports 64 kb/s synchronous (voice) link. The asynchronous channel can support an asymmetric link of maximally 721 kb/s in either direction while permitting 57.6 kb/s in the return direction, or a 432.6 kb/s symmetric link.

Modes of operation

An interesting aspect of the technology is the instant formation of networks once the bluetooth devices come in range to each other. A piconet is a collection of devices connected via Bluetooth technology in an ad hoc fashion.

A Piconet can be a simple connection between two devices or more than two devices. Multiple independent and non-synchronized piconets can form a scatternet. Any of the devices in a piconet can also be a member of another by means of time multiplexing. i.e a device can be a part of more than one piconet by suitably sharing the time.

The Bluetooth system supports both point-to-point and point-to-multi-point connections. When a device is connected to another device it is a point to point connection. If it is connected to more that one (upto 7 ) it is a point to multipoint connection. Several piconets can be established and linked together ad hoc, where each piconet is identified by a different frequency hopping sequence. All users participating on the same piconet are synchronized to this hopping sequence.
If a device is connected to more than one piconet it communicates in each piconet using a different hopping sequence. A piconet starts with two connected devices, such as a portable PC and cellular phone, and may grow to eight connected devices.

All Bluetooth devices are peer units and have identical implementations. However, when establishing a piconet, one unit will act as a master and the other(s) as slave(s) for the duration of the piconet connection. In a piconet there is a master unit whose clock and hopping sequence are used to synchronize all other devices in the piconet.

All the other devices in a piconet that are not the master are slave units. A 3-bit MAC address is used to distinguish between units participating in the piconet. Devices synchronized to a piconet can enter power-saving modes called Sniff and hold mode, in which device activity is lowered. Also there can be parked units which are synchronized but do not have a MAC addresses. These parked units have a 8 bit address, therefore there can be a maximum of 256 parked devices.

Voice channels use either a 64 kbps log PCM or the Continuous Variable Slope Delta Modulation (CVSD) voice coding scheme, and never retransmit voice packets.

The voice quality on the line interface should be better than or equal to the 64 kbps log PCM. The CVSD method was chosen for its robustness in handling dropped and damaged voice samples. Rising interference levels are experienced as increased background noise: even at bit error rates up 4%, the CVSD coded voice is quite audible.
Types of Bluetooth Devices

Bluetooth Dongle

Installing a Bluetooth dongle is easy; simply insert the CD that came with it, follow the on screen prompts and then plug the dongle into a free USB port.

If you had a Bluetooth compatible laptop you could just plug the dongle into an internet enabled personal computer and check your e-mail, download Windows updates, or transfer files. On the same lines you could also synchronize your PDA with your personal computer and download the latest appointments, e-mails or send text messages.

Bluetooth Headset

Bluetooth headsets are mainly used with compatible cell phones, place the headset on your ear and roam freely while talking to colleagues, friends and family. You could also connect to a dongle on a personal computer and use it for voice conferencing for example. A number of products exist on the market today, which all offer good sound quality and have a similar variety of features.
3. Wi-Fi Technology

Presentation

Wi-Fi (short for "wireless fidelity") is a term for certain types of wireless local area network (WLAN) that use specifications in the 802.11 family.

The term Wi-Fi was created by an organization called the Wi-Fi Alliance, which oversees tests that certify product interoperability. A product that passes the alliance tests is given the label "Wi-Fi certified" (a registered trademark).

The Wi-Fi Alliance is a global, non-profit industry association of more than 200 member companies devoted to promoting the growth of wireless Local Area Networks (WLANs). With the aim of enhancing the user experience for mobile wireless devices, the Wi-Fi Alliance's testing and certification programs ensure the interoperability of WLAN products based on the IEEE 802.11 specification. Since the introduction of the Wi-Fi Alliance's certification program in March 2000, over 2,000 products have been designated as Wi-Fi CERTIFIED™, encouraging the expanded use of Wi-Fi products and services across the consumer and enterprise markets.
The 802.11 family

802.11 is a family of networking specifications developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). There are several specifications in the family.

802.11

- Family of specifications for wireless local area network (WLAN) use
- Employs phase-shift keying
- Provides a wireless alternative to wired Ethernet LANs
- Several enhancements as defined below

802.11a

- Enhancement to 802.11 that applies to wireless ATM systems
- Used in access hubs
- Enhanced data speed
- Frequency range 5.725 GHz to 5.850 GHz

802.11b

- Enhancement to 802.11 that employs complementary code keying (CCK)
- High data speed
- Low susceptibility to multipath-propagation interference
- Frequency range 2.400 GHz to 2.4835 GHz

802.11d

- Enhancement to 802.11 that allows for global Roaming
- Attributes similar to 802.11b
- Particulars can be set at Media Access Control (MAC) layer

802.11e

- Enhancement to 802.11 that includes Quality of Service (QoS) features
- Facilitates prioritization of data, voice, and video transmissions

802.11g

- Enhancement to 802.11 that offers wireless transmission over relatively short distances
- Operates at up to 54 megabits per second (Mbps)

802.11h

- Enhancement to 802.11a that resolves interference issues
- Dynamic frequency selection (DFS)
• Transmit power control (TPC)

802.11i

• Enhancement to 802.11 that offers additional security for WLAN applications

802.11j

• Japanese regulatory extensions to 802.11a specification
• Frequency range 4.9 GHz to 5.0 GHz

802.11k

• Radio resource measurements for networks using 802.11 family specifications

802.11m

• Maintenance of 802.11 family specifications
• Corrections and amendments to existing documentation

802.11x

• Generic term for 802.11 family specifications under development
• General term for all 802.11 family specifications

Wi-Fi

• Originally created to ensure compatibility among 802.11b products
• Can run under any 802.11 standard
• Indicates interoperability certification by Wi-Fi Alliance

Originally, Wi-Fi certification was applicable only to products using the 802.11b standard. Today, Wi-Fi can apply to products that use any 802.11 standard. The 802.11 specifications are part of an evolving set of wireless network standards known as the 802.11 family. The particular specification under which a Wi-Fi network operates is called the "flavor" of the network. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks. These locations are known as hot spots. Many charge a daily or hourly rate for access, but some are free. An interconnected area of hot spots and network access points is known as a hot zone.
Definition of Terms Used

For users of portable computers equipped for wireless, a hot spot (or hotspot) is a wireless LAN (local area network) node that provides Internet connection and virtual private network (VPN) access from a given location. For example, a business traveler with a laptop equipped for Wi-Fi can look up a local hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.

The Wi-Fi Alliance provides a list of hot spots through its Wi-Fi Zone program. A number of companies such as Sprint and Cometa plan to provide a nationwide network of hot spots.

Unless adequately protected, a Wi-Fi network can be susceptible to access by unauthorized users who use the access as a free Internet connection. The activity of locating and exploiting security-exposed wireless LANs is called war driving. An identifying iconography, called war chalking, has evolved. Any entity that has a wireless LAN should use security safeguards such as the Wired Equivalent Privacy (WEP) encryption standard, the more recent Wi-Fi Protected Access (WPA), Internet Protocol Security (IPsec), or a virtual private network (VPN).

A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

The term derives from a somewhat similar approach to breaching the telephone system called war dialing. Breaching a private network may be illegal and at least one person has been prosecuted for it.

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy
comparable to what is usually expected of a wired LAN. A wired local area network (LAN) is generally protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.

**Phase-shift keying** (PSK) is a method of digital communication in which the phase of a transmitted signal is varied to convey information. There are several methods that can be used to accomplish PSK.

The simplest PSK technique is called binary phase-shift keying (BPSK). It uses two opposite signal phases (0 and 180 degrees). The digital signal is broken up timewise into individual bits (binary digits). The state of each bit is determined according to the state of the preceding bit. If the phase of the wave does not change, then the signal state stays the same (0 or 1). If the phase of the wave changes by 180 degrees -- that is, if the phase reverses -- then the signal state changes (from 0 to 1, or from 1 to 0). Because there are two possible wave phases, BPSK is sometimes called biphase modulation.

More sophisticated forms of PSK exist. In m-ary or multiple phase-shift keying (MPSK), there are more than two phases, usually four (0, +90, -90, and 180 degrees) or eight (0, +45, -45, +90, -90, +135, -135, and 180 degrees). If there are four phases (m = 4), the MPSK mode is called quadrature phase-shift keying or quaternary phase-shift keying (QPSK), and each phase shift represents two signal elements. If there are eight phases (m = 8), the MPSK mode is known as octal phase-shift keying (OPSK), and each phase shift represents three signal elements. In MPSK, data can be transmitted at a faster rate, relative to the number of phase changes per unit time, than is the case in BPSK.

**Ethernet** is the most widely-installed local area network (LAN) technology. Specified in a standard, IEEE 802.3, Ethernet was originally developed by Xerox from an earlier specification called Alohanet (for the Palo Alto Research Center Aloha network) and then developed further by Xerox, DEC, and Intel. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Ethernet is also used in wireless LANs. The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps. Devices are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.
Wi-Fi innovation

Wi-Fi, or Wireless Fidelity, is freedom: it allows you to connect to the Internet from your couch at home, a bed in a hotel room or a conference room at work without wires. How? Wi-Fi is a wireless technology like a cell phone. Wi-Fi enabled computers send and receive data indoors and out; anywhere within the range of a base station. And the best thing of all, it's fast. In fact, it's several times faster than the fastest cable modem connection.

A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wired networks (which use IEEE 802.3 or Ethernet). Wi-Fi networks operate in the unlicensed 2.4 and 5 GHz radio bands, with an 11 Mbps (802.11b) or 54 Mbps (802.11a) data rate or with products that contain both bands (dual band), so they can provide real-world performance similar to the basic 10BaseT wired Ethernet networks used in many offices.

Wi-Fi’s target

Everyone can use Wi-Fi, almost everywhere in the world. Home Wi-Fi networks can connect multiple computers to each other, to peripherals, and to the Internet. A Wi-Fi network can connect a family’s computers together to share such hardware and software resources as printers and the Internet. That means everyone in the family can share stored files, photos and documents and print them out on a single printer attached to one desktop computer—all without unsightly cables running throughout the home.

In a home or home office, using Wi-Fi certified equipment in your wireless network gives you the ability to share a single high-speed broadband cable or DSL connection. A Wi-Fi network can easily be expanded to ten users or more.

Wi-Fi networks also work well for small businesses, providing connectivity between mobile salespeople, floor staff and behind-the-scenes finance and accounting departments. Because small businesses are dynamic, the built-in flexibility of a Wi-Fi network makes it easy and affordable for them to change and grow.

Using Enterprise-Level Wi-Fi Technology

Large corporations and campuses use enterprise-level technology and Wi-Fi certified wireless products to extend standard wired Ethernet networks to public areas like meeting rooms, training classrooms and large auditoriums. Many corporations also provide wireless networks to their off-site and telecommuting workers to use at home or in remote offices. Large companies and campuses often use Wi-Fi to connect buildings.
Service providers and wireless ISPs are using Wi-Fi technology to distribute Internet connectivity within individual homes and businesses as well as apartments and commercial complexes.

**Extending a Network with a Wi-Fi LAN**

It's easy to add another wireless computer to a Wi-Fi network. There's no need to purchase or lay more cable or find an available Ethernet port on your hub or router. Just plug in your card or USB connection, turn on your computer and you're surfing the Net.

If your business grows and you need to move, you don't have to abandon your network infrastructure investment or hire a networking company to rewire the new location. And there's no network downtime—you can be up and running even before the furniture arrives. Simply plug the system into a power outlet and it will be operational in minutes.
If you examine the benefits of each technology, you can see that Bluetooth and IrDA are both critical to the marketplace. Each technology has advantages and drawbacks and neither can meet all users' needs.

Bluetooth's ability to penetrate solid objects and its capability for maximum mobility within the piconet allows for data exchange applications that are very difficult or impossible with IrDA. For example, with Bluetooth, a person could synchronize their phone with a PC without taking the phone out of their pocket or purse (this is not possible with IrDA). The omni-directional capability of Bluetooth allows synchronization to start when the phone is brought into range of the PC.

On the other hand, in applications involving one to one data exchange, IrDA is at an advantage. Consider an application where there are many people sitting across a table in a meeting. Electronic cards can be exchanged between any two people by pointing the IrDA devices towards each other (because of the directional nature). On the other hand since Bluetooth is omnidirectional in nature, the Bluetooth device will detect all similar devices in the room and the user would have to select the intended person from say, a list provided by the Bluetooth device.

On the security front Bluetooth provides security mechanisms which are not present in IrDA. However the narrow beam (in the case of IrDA) provides a low level of security. IrDA beats Bluetooth on the cost front. A manufacturer can get an IrDA solution ready for $1 US. Bluetooth is costly in comparison but the prices are expected to fall.

The Bluetooth standard defines the layers 1 and 2 of the OSI model. The application framework of Bluetooth is aimed to achieve interoperability with IrDA and WAP. In addition, a host of other applications will be able to use the Bluetooth technology and protocols.
5. Bluetooth vs. Wi-Fi

802.11b vs. Bluetooth

The introduction of 802.11b was one of the first major steps towards the expansion of wireless networking; the jump to speeds of up to 11mbps (in reality you would however achieve something like 6mbps) contributed significantly to this. It has since grown and 802.11a and g have been released and are going strong. Because of its proven track record and relatively inexpensive hardware, 802.11b has emerged as a favorite amongst SOHO users. 802.11g has improved on the performance of 802.11b and is backward compatible.

Bluetooth was invented to get rid of wires and can be used to create a Personal Area Network (PAN). It is more of a wireless substitute for connecting devices such as digital cameras, PDAs and mobile phones with each other or a desktop computer. Bluetooth is more suited for connecting two point-to-point devices, whereas Wi-Fi is an IEEE standard intended for networking. Although it has the capability of interconnecting up to 8 devices to form a small LAN, with a low bandwidth of about 700KB/sec and a range
of about 30 feet it cannot really be considered as an honorable networking protocol.

802.11b (Wi-Fi)

Wi-Fi (Wireless Fidelity), or 802.11b, is an IEEE standard for wireless Local Area Networks. Backward compatible with 802.11, 802.11b runs on the 2.4 GHz band and is capable of working at speeds of up to 11Mbps. This allows you to surf the Internet at broadband speeds when connected to an access point or in ad hoc mode. The IEEE published 802.11 in 1997 to make it the first globally approved wireless LAN standard. In 1999 they amended the specifications to add two more speeds, 5.5 and 11Mbps.

Out of the 7 layers of the ISO Model (refer to image below), 802.11, like the other 802.x standards, centers around the Physical and Data link layer. Any application, operating system or protocol should work as well on a Wi-Fi LAN as it did on an Ethernet LAN.

An 802.11b wireless network adapter can operate on two modes, Ad-Hoc or Infrastructure.

In infrastructure mode all your traffic passes through a wireless access point and can be thought of as a wired network without cables. This is commonly setup to allow resources such as printers and files to be shared. The image demonstrates such a setup.

In Ad-Hoc mode, your computers or mobile devices talk to each other directly and do not need an access point. This type of structure can support up to 8 devices connected to each other and is useful when you want to setup a wireless connection quickly or when you have a few computers in your network. The image below demonstrates a typical ad-hoc network.
Advantages

- Interoperability
- Higher data rates (11Mbps)
- Longer range (approx. 100 meters)
- Relatively inexpensive hardware

Disadvantages

- Security
- RF Band is shared

Most new laptops are Wi-Fi enabled and have the technology built in. If they don’t, or you own an older laptop, then you can purchase a wireless NIC card which would fit into an empty PCMCIA slot or USB port (the same goes for Personal Digital Assistants).

Bluetooth

Bluetooth, named after the Danish king Herald Blatand, is a user friendly radio frequency wireless technology initially conceived by Ericsson in 1994. It is a short-range data communications protocol, known also as the IEEE 802.15 standard. A number of large companies, namely Nokia, Ericsson, Intel and Toshiba formed the Bluetooth SIG group in 1998. Since then many other heavyweights such as Microsoft, 3Com, Motorola, and so on have joined and the number of participating companies has now reached 1500.

Bluetooth operates on the unlicensed 2.4 GHz band and uses a frequency hopping spread spectrum technique - which is one of two basic modulation techniques used in spread spectrum signal transmission. Frequencies are switched repeatedly during radio transmission to help reduce unlawful access or other means of telecommunications to cross paths and cause interruption. It also makes Bluetooth communication more robust and secure. Interference from other devices will not cause the transmission to stop, but the speed to be reduced.

Advantages

- Interoperability
- Scalability
- Inexpensive
- Voice/data compatible
- Allows for the formation of an Ad-hoc network
• Low power consumption

Disadvantages

• Short Range
• Low data rate
• RF Band is shared

Bluetooth’s advantage over Infrared (IrDA - Infrared Data Association) is its ability to connect 1-to-many devices rather than 1-to-1. Infrared requires a direct line of sight in order to operate and has a range of approximately one meter. Bluetooth developers have said they did not intend to create an alternative to IrDA but so many companies are now replacing the devices IrDA slot with Bluetooth. Although Bluetooth use is becoming more and more popular and IrDA is being phased out, I do believe that Infrared will, in some way, still be around in the near future.

Bluetooth technology can be found in many devices. Nowadays, if you purchase a laptop, PDA or mobile phone it is bound to be Bluetooth enabled.

Conclusion

Wi-Fi is really for when cabling is not a feasible option and Bluetooth is for intercommunication between devices without the need for a PC.

Bluetooth makes connecting various devices to each other without the need for cables a fairly easy task, whereas 802.11-based products can extend, or replace, a wired Local Area Network. From a personal user’s point-of-view, I would suggest - if possible - having both available if your everyday life requires you to travel to different destinations and meet different people. This way you will always be ready, if one isn’t available then you can use the other.

It’s no secret that the overall performance of a wired LAN is more superior to a wireless network. However, expect improvements, in the coming years things will get bigger and better. Having said this, the word that comes to my mind when I think of wireless - especially Wi-Fi - is Convenience. This technology makes sitting out on the porch or in the garden on a hot summer’s day and browsing the Internet a possibility.
Bluetooth is a wireless networking technology that today is available in a wide variety of devices such as desktop PCs, laptops, PDAs, smartphones and many more. Bluetooth is designed to support up to 8 devices operating within a very small radius of 30 feet from each device (class 2 operation) or up to 300 feet (class 1 operation). Bluetooth is known to be able to do things that are outside of the specifications here. Bluetooth class 2 devices operate at 1 megabit per second for high speed communications. The 1 megabit connection is divided between a 64k connection for synchronous voice and a 768k connection for data so you can’t get a true 1 megabit data connection. It uses the 2.4 gHz frequency spectrum so you need to consider other devices that may interfere with communications such as microwaves, cordless phones, and 802.11b,g Wireless LANs. Microsoft has announced support for Bluetooth in Windows CE and the Pocket PC (mobile handheld devices such as smartphones and PDAs).

**Bluetooth Desktop Chat** has been designed as a simple application, to demonstrate how two Bluetooth enabled Desktop PCs can communicate with one another via Bluetooth. The application was written in Visual Basic .NET and uses Microsoft .NET framework 2.0 beta 2 (latest available) and OpenNETCF library (OpenNETCF.NET.Bluetooth.dll). The application requires Windows XP compatible devices running the Microsoft Bluetooth stack, because it uses the Microsoft Bluetooth stack. The Bluetooth stack in Windows XP Service Pack 2 is designed to help prevent a Bluetooth device from connecting until you explicitly configure that device. This requirement
helps prevent unauthorized access to your computer through a Bluetooth device. The stack is also present within a small ROM chip that is embedded within the device. All Bluetooth adapters and all Bluetooth enabled devices have a stack that is preinstalled into the ROM of the device and it can not simply be removed and replaced. As such, the device must be compatible with the Microsoft’s Bluetooth Protocol Stack. Microsoft’s Bluetooth Protocol Stack supports client and server connections and device discovery using an object model which will be familiar to developers who have used the IrDA and Tcp equivalent.

For a better understanding of the Bluetooth Protocol Stack, some of the terms used have been detailed and explained:

**HCI** Host Controller Interface
**L2CAP** Logical Link Control and Adaptation Protocol
**LM or LMP** Link Manager (Protocol)
**OBEX** Generalised Multi-Transport) Object Exchange Protocol
**OS** Operating System
**RFCOMM** Serial Port Emulation
**RTOS** Real Time Operating System
**SCO** Synchronous Connection Oriented
**SDP** Service Discovery Protocol
**TCS** Telephony Control protocol Specification

**OBEX** (*Object Exchange*) is an object exchange protocol that is implemented on top of Winsock over Bluetooth and IRDA transports. For more information, see Object Exchange Protocol.

- Obex client module: Obexapi.dll
- Obex server module: Obexsvr.dll

**TDI** (*Transport Driver Interface*), in the Microsoft® Windows® CE operating system (OS) architecture, is an interface that serves as an adaptation layer
to Winsock-based user APIs. It isolates the highly asynchronous callback-based architecture of the stack presenting a Windows Sockets Specification 1.1 interface.

**COM Port Emulation**, in Windows CE, enables virtual COM ports to be created over RFCOMM (explained below) channels. It hosts dial-up and LAN access profiles. For more information, see Creating a Connection to a Remote Device Using a Virtual COM Port. The port emulation facility is included in Btd.dll.

**SDP (Service Discovery Protocol)** is a Bluetooth service discovery protocol that handles publishing and discovery of services running on top of the Bluetooth stack. The port emulation is included in Btd.dll.

- SDP client module: Btdrt.dll
- SDP server module: Btd.dll

**RFCOMM (Serial Cable Emulation Protocol)** is Bluetooth's adaptation of the TS07.10 protocol. It serves as a base for COM port emulation facilities and derived point-to-point protocols. Multiplexing and flow control between devices and applications are also implemented here. The RFCOMM layer is included in Btd.dll.

**PAN (Personal Area Network)** profile defines procedures to support standard IP-based network services deployed over the Bluetooth transport layer. For more information, see Personal Area Networking (PAN) Profile.

**HID (Human Interface Device)** profile defines procedures to support human interface devices such as keyboard and mouse. For more information, see Human Interface Device (HID) Profile.

**L2CAP (Logical Link Control and Adaptation Protocol)** is a lower connection-based Bluetooth communication protocol that implements multiplexing.
L2CAP does not implement flow control. It relies on a reliable device-to-device baseband link provided by Bluetooth hardware. The L2CAP layer is included in Btd.dll.

**HCI (Host Controller Interface)** is a basic interface to Bluetooth hardware, responsible for controller management, link establishment, and maintenance. For more information, see Host Controller Interface. The HCI layer is included in Btd.dll.

**Bluetooth Universal Transport Manager (BthUniv)** is an intermediate transport driver between the HCI layer and the transport layer. It detects the Plug and Play (PnP) device and loads the appropriate transport driver. For more information, see Supported HCI Transport Drivers. The Bluetooth Universal Transport Manager is in Bthuniv.dll.

**HCI Transport Layer** is a transport layer that delivers HCI commands to the Bluetooth hardware. For more information, see Bluetooth HCI Transport Layer. For more information about the modules that implement this layer, see Supported HCI Transport Drivers.

**LMP (Link Manager Protocol)** is the protocol that handles link establishment between Bluetooth devices, which include authentication and encryption.

**BB (Baseband)** enables the physical radio frequency (RF) link between Bluetooth units that form a piconet.

Each layer, with the exception of the **HCI** transport, is implemented as a separate entity that exposes its interfaces up and down through tables of callbacks. Each interface is well defined. There are no other interrelationships between parts of the stack; every layer is replaceable.
Class view of **OpenNETCF.Bluetooth** library:
**Bluetooth Desktop Chat Interface**

The **Commands** menu contains two items:

> *Discover Devices* (used to call DiscoverDevices(parameter), where parameter is currently set to 5) – this enables the application to tell the Bluetooth adapter to search for other Bluetooth enabled devices that are nearby.

> *Clear chat history* – empties message history.

> *Exit* – used to exit the application.

The **About** menu displays an information box with details about the project and its creators.
7. References

- www.mit.edu
- www.whatis.com
- www.wirelessdevnet.com
- www.windowsnetworking.com
- www.wi-fi.org
- www.windowsnetworking.com
- searchmobilecomputing.techtarget.com
- standards.ieee.org/getieee802
- www.bluetooth.org
- www.opennetcf.org
- www.papyrus.co.il
- www.activesys.net