Topic 10 Notes

10.1 Introduction

There are lots of different ways that electronic devices can connect to one another. For example:

i. Component cables
ii. Electrical wires
iii. Ethernet cables
iv. WiFi
v. Infrared signals

When any two devices need to talk to each other, they have to agree on a number of points before the conversation can begin. The first point of agreement is physical: Will they talk over wires, or through some form of wireless signals? If they use wires, how many are required -- one, two, eight, 25? Once the physical attributes are decided, several more questions arise:

i. How much data will be sent at a time? For instance, serial ports send data 1 bit at a time, while parallel ports send several bits at once.
ii. How will they speak to each other? All of the parties in an electronic discussion need to know what the bits mean and whether the message they receive is the same message that was sent. This means developing a set of commands and responses known as a **protocol**.

Bluetooth offers a solution to the problem.

10.2 How Bluetooth Creates a Connection

Bluetooth takes small-area networking to the next level by removing the need for user intervention and keeping transmission power extremely low to save battery power. Picture this: You're on your Bluetooth-enabled cell phone, standing outside the door to your house. You tell the person on the other end of the line to call you back in five minutes so you can get in the house and put your stuff away. As soon as you walk in the house, the map you received on your cell phone from your car's Bluetooth-enabled GPS system is automatically sent to your Bluetooth-enabled computer, because your cell phone picked up a Bluetooth signal from your PC and automatically sent the data you designated for transfer. Five minutes later, when your friend calls you back, your Bluetooth-enabled home phone rings instead of your cell phone. The person called the same number, but your home phone picked up the Bluetooth signal from your cell phone and automatically re-routed the call because it realized you were home. And each transmission signal to and from your cell phone consumes just 1 milliwatt of power, so your cell phone charge is virtually unaffected by all of this activity.

Bluetooth is essentially a networking standard that works at two levels:

i. It provides agreement at the **physical** level -- Bluetooth is a radio-frequency standard.
ii. It provides agreement at the **protocol** level, where products have to agree on when bits are sent, how many will be sent at a time, and how the parties in a conversation can be sure that the message received is the same as the message sent.

The big draws of Bluetooth are that it is wireless, inexpensive and automatic. There are other ways to get around using wires, including infrared communication. **Infrared** (IR) refers to light waves of a lower frequency than human eyes can receive and interpret. Infrared is used in most television remote control systems. Infrared communications are fairly reliable and don't cost very much to build into a device, but there are a couple of drawbacks. First, infrared is a "line of sight" technology. For example, you have to point the remote control at the television or DVD player to make things happen. The second drawback is that infrared is almost always a "one to one" technology. You can send data between your desktop computer and your laptop computer, but not your laptop computer and your PDA at the same time. These two qualities of infrared are actually advantageous in some regards. Because infrared transmitters and receivers have to be lined up with each other, interference between devices is uncommon. The one-to-one nature of infrared communications is useful in that you can make sure a message goes only to the intended recipient, even in a room full of infrared receivers.

Bluetooth is intended to get around the problems that come with infrared systems. The older Bluetooth 1.0 standard has a maximum transfer speed of 1 megabit per second (Mbps), while Bluetooth 2.0 can manage up to **3 Mbps**. Bluetooth 2.0 is backward-compatible with 1.0 devices.

10.3 How Bluetooth Operates

Bluetooth networking transmits data via low-power radio waves. It communicates on a frequency of **2.45 gigahertz** (actually between 2.402 GHz and 2.480 GHz, to be exact). This frequency band has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM).

A number of devices that you may already use take advantage of this same radio-frequency band. Baby monitors, garage-door openers and the newest generation of cordless phones all make use of frequencies in the ISM band. Making sure that Bluetooth and these other devices don't interfere with one another has been a crucial part of the design process.

One of the ways Bluetooth devices avoid interfering with other systems is by sending out very weak signals of about 1 milliwatt. By comparison, the most powerful cell phones can transmit a signal of 3 watts. The low power limits the range of a Bluetooth device to about 10 meters (32 feet), cutting the chances of interference between your computer system and your portable telephone or television. Even with the low power, Bluetooth doesn't require line of sight between communicating devices. The walls in your house won't stop a Bluetooth signal, making the standard useful for controlling several devices in different rooms.

Bluetooth can connect up to eight devices simultaneously. With all of those devices in the same 10-meter (32-foot) radius, you might think they'd interfere with one another, but it's unlikely. Bluetooth uses a technique called spread-spectrum frequency hopping that makes it rare for more than one device to be transmitting on the same frequency at the same time. In this technique, a device will use 79 individual, randomly chosen frequencies within a designated range, changing from one to another on a regular basis. In the case of Bluetooth, the transmitters change frequencies 1,600 times every second, meaning that more devices can make full use of a limited slice of the radio spectrum. Since every Bluetooth transmitter uses spread-spectrum transmitting automatically, it’s unlikely that two transmitters will be on the same frequency at the same time. This same technique minimizes the risk that portable phones or baby monitors will disrupt Bluetooth devices, since any interference on a particular frequency will last only a tiny fraction of a second.

When Bluetooth-capable devices come within range of one another, an electronic conversation takes place to determine whether they have data to share or whether one needs to control the other. The user doesn't have to press a button or give a command -- the electronic conversation happens automatically. Once the conversation has occurred, the devices -- whether they're part of a computer system or a stereo -- form a network. Bluetooth systems create a personal-area network (PAN), or **piconet**, that may fill a room or may encompass no more distance than that between the cell phone on a belt-clip and the headset on your head. Once a piconet is established, the members randomly hop frequencies in unison so they stay in touch with one another and avoid other piconets that may be operating in the same room. Let's check out an example of a Bluetooth-connected system.

10.3.1 Bluetooth Piconets

Let's say you have a typical modern living room with typical modern stuff inside. There's an entertainment system with a stereo, a DVD player, a satellite TV receiver and a television; there's also a cordless telephone and a personal computer. Each of these systems uses Bluetooth, and each forms its own piconet to talk between the main unit and peripheral. The cordless telephone has one Bluetooth transmitter in the base and another in the handset. The manufacturer has programmed each unit with an address that falls into a range of addresses it has established for a particular type of device. When the base is first turned on, it sends radio signals asking for a response from any units with an address in a particular range. Since the handset has an address in the range, it responds, and a tiny network is formed. Now, even if one of these devices should receive a signal from another system, it will ignore it since it's not from within the network. The computer and entertainment system go through similar routines, establishing networks among addresses in ranges established by manufacturers. Once the networks are established, the systems begin talking among themselves. Each piconet hops randomly through the available frequencies, so all of the piconets are completely separated from one another.

Now the living room has three separate networks established, each one made up of devices that know the address of transmitters it should listen to and the address of receivers it should talk to. Since each network is changing the frequency of its operation thousands of times a second, it's unlikely that any two networks will be on the same frequency at the same time. If it turns out that they are, then the resulting confusion will only cover a tiny fraction of a second, and software designed to correct for such errors weeds out the confusing information and gets on with the network's business.

10.4 Bluetooth Security

Bluetooth offers several security modes, and device manufacturers determine which mode to include in a Bluetooth-enabled gadget. In almost all cases, Bluetooth users can establish "trusted devices" that can exchange data without asking permission. When any other device tries to establish a connection to the user's gadget, the user has to decide to allow it. Service-level security and device-level security work together to protect Bluetooth devices from unauthorized data transmission. Security methods include authorization and identification procedures that limit the use of Bluetooth services to the registered user and require that users make a conscious decision to open a file or accept a data transfer. As long as these measures are enabled on the user's phone or other device, unauthorized access is unlikely. A user can also simply switch his Bluetooth mode to "non-discoverable" and avoid connecting with other Bluetooth devices entirely. If a user makes use of the Bluetooth network primarily for synching devices at home, this might be a good way to avoid any chance of a security breach while in public.

Still, early cell-phone virus writers have taken advantage of Bluetooth's automated connection process to send out infected files. However, since most cell phones use a secure Bluetooth connection that requires authorization and authentication before accepting data from an unknown device, the infected file typically doesn't get very far. When the virus arrives in the user's cell phone, the user has to agree to open it and then agree to install it. This has, so far, stopped most cell-phone viruses from doing much damage.

Other problems like "bluejacking," "bluebugging" and "Car Whisperer" have turned up as Bluetooth-specific security issues. **Bluejacking** involves Bluetooth users sending a business card (just a text message, really) to other Bluetooth users within a 10-meter (32-foot) radius. If the user doesn't realize what the message is, he might allow the contact to be added to his address book, and the contact can send him messages that might be automatically opened because they're coming from a known contact. **Bluebugging** is more of a problem, because it allows hackers to remotely access a user's phone and use its features, including placing calls and sending text messages, and the user doesn't realize it's happening. The **Car Whisperer** is a piece of software that allows hackers to send audio to and receive audio from a Bluetooth-enabled car stereo. Like a computer security hole, these vulnerabilities are an inevitable result of technological innovation, and device manufacturers are releasing firmware upgrades that address new problems as they arise.

Revision questions

1. Define Bluetooth
2. What are the advantages of using Bluetooth technology?
3. How does Bluetooth enable communication between two devices?
4. What are the requirements for using Bluetooth?