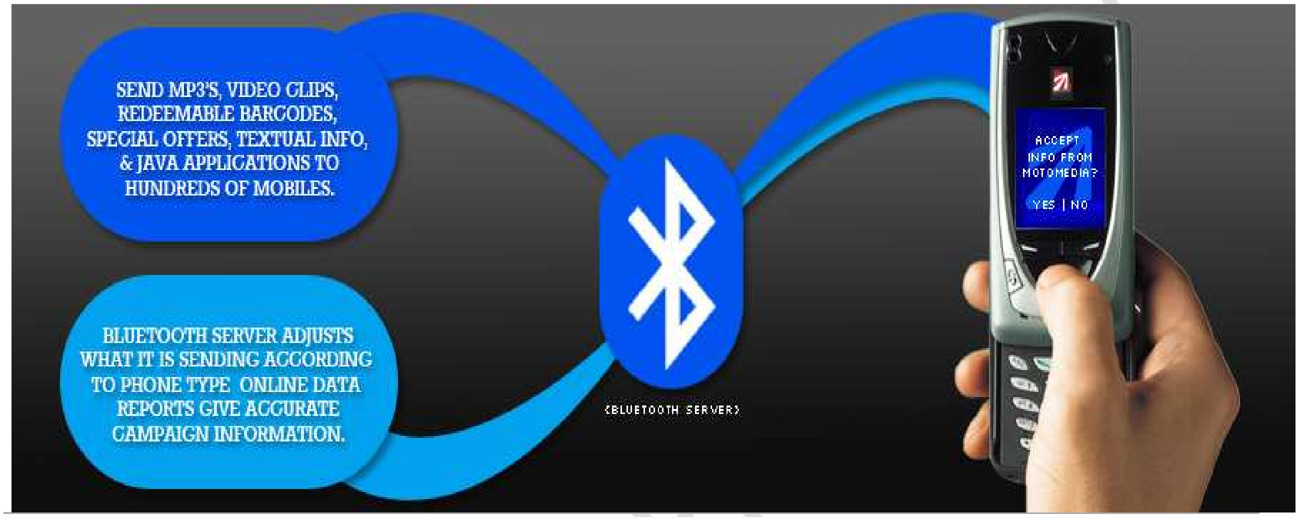
A Seminar Report On Bluetooth Technology


SEND MP3'S, VIDEO CLIPS, REDEEMABLE BARCODES, SPECIAL OFFERS, TEXTUAL INFO, & JAVA APPLICATIONS TO HUNDREDS OF MOBILES.
BLUETOOTH SERVER ADJUSTS WHAT IT IS SENDING ACCORDING TO PHONE TYPE ONLINE DATA REPORTS GIVE ACCURATE CAMPAIGN INFORMATION.
(BLUETOOTH SERVER)
ACCEPT INFO FROM MOTOMEDIA?
YES | NO

Submitted By – Sanjay Dudani

Roll No. - 419

Under The Guidance of Prof. P.B. Dehenkar

Bluetooth is a wireless protocol for exchanging data over short distances from fixed and mobile devices, creating personal area networks (PANs). It was originally conceived as a wireless alternative to RS232 data cables. It can connect several devices, overcoming problems of synchronization.

Origin of the name and Logo-

Bluetooth was named after a 10th Century King, Harald Bluetooth, King of Denmark and Norway.

The Bluetooth Logo contains the Latin letters H and B (H for Harald, B for Bluetooth)

ᚼ	means H
ᛒ	means B

Working of Bluetooth-

Bluetooth uses a radio-technology frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 frequencies. In its basic mode, the modulation is Gaussian frequency-shift keying (GFSK). It can achieve a gross data rate of 1Mbps. Bluetooth provides a way to connect and exchange information between devices such as mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles.

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 GPSsystem 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:

- It provides agreement at the **physical** level -- Bluetooth is a radio-frequency standard.
- 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 controlsystems. 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. (SeeHow Remote Controls Work to learn more about infrared communication.)

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.

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.

Bluetooth Security

In any wireless networking setup, security is a concern. Devices can easily grab radio waves out of the air, so people who send sensitive information over a wireless connection need to take precautions to make sure those signals aren't intercepted. Bluetooth technology is no different -- it's wireless and therefore susceptible to spying and remote access, just like WiFi is susceptible if the network isn't secure. With Bluetooth, though, the automatic nature of the connection, which is a huge benefit in terms of time and effort, is also a benefit to people looking to send you data without your permission.

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. SeeHow Cell-phone Viruses Work to learn more.

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.

If communications security is a concern of yours, then click here to learn how phone conferencing security works. To learn more about Bluetooth security issues and solutions, see Bluetooth.com: Wireless Security.

Applications Of Bluetooth-

1) Wireless control of and communication between a mobile phone and a hands-free headset. This was one of the earliest applications to become popular.
2) Wireless networking between PCs in a confined space and where little bandwidth is required.
3) Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
4) Transfer of files, contact details, calendar appointments, and reminders between devices with **OBEX** i.e. **Ob**ject **Ex**change technology.
5) Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
6) For controls where infrared was traditionally used.
7) Two seventh-generation game consoles, Nintendo's Wii and Sony's PlayStation 3, use Bluetooth for their respective wireless controllers.
8) Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a modem.

Advantages Of Bluetooth Technology-

1) **Bluetooth Technology is Inexpensive-**

Bluetooth technology is cheap for companies to implement, which results in lower over-all manufacturing Costs. These savings are then passed on to you, the consumer.

The end result: Bluetooth devices are relatively inexpensive.

2) **Bluetooth is Automatic-**

Bluetooth doesn't require you to think about setting up a connection or to push any buttons. When two or more Bluetooth devices enter a range (Up to 30 feet) of one another, they automatically begin to communicate without you having to do anything. Once the communicating begins, Bluetooth devices will setup Personal Area Networks or Piconets.

The best part is: The devices take care of the entire setup process, and you can go about your business.

3) **Low Energy Consumption -**

Bluetooth uses low power signals. As a result, the technology requires little energy and will therefore use less battery or electrical power. Obviously, this is a great benefit for mobile devices because Bluetooth won't drain the life of your device's battery.

4) **Information Privacy is in your control -**

Even though you are able to exchange data across your cell phones, you still have the ability to keep your information private. In this technology, a password is sent to the receiver by the sender, and the information is sent to the receiver if and only if the both ends' passwords are matched correctly.

Disadvantages Of Bluetooth Technology-

Every coin has its both ends i.e. positive and negative. So, Bluetooth has its Disadvantages as follows:

1) Battery Use –

This problem occurs on your cell phones. Your cell phone’s battery will be rapidly decreasing rapidly when you leave your phone’s Bluetooth enabled for number of hours. The best way to overcome this is disable the Bluetooth immediately after completing the data transfer. It takes only a few seconds to enable and disable it.

2) Slow Bluetooth Internet-

Throughout all devices, when using Bluetooth Internet, the connection can run sometimes run very slow, so Bluetooth Internet is not highly suggested for all cases.

Conclusion-

As you can notice that there are lot of advantages and few disadvantages of Bluetooth Technology.

Overall, Bluetooth is a great thing to be using on all your devices that supports it. You can do so much with it and includes cutting all the wires and cords attached to your phone.