Bluetooth

By

M. Habibullah Pagarkar

&

Chinmay Shah

1 - INTRODUCTION : ISSUES DRIVING WIRELESS DATA

In 1995, the telecommunications and information technology industries recognized that a low-cost, low-power radio based cable replacement, or wireless link, would be feasible, thus eliminating the need for communication cables for short distances. Such a ubiquitous link would provide the basis for small portable devices to communicate together in an ad-hoc fashion.

A study was done, and the technology, code named **"Bluetooth",** was soon defined. The goal was to provide reliable service for mobile and business users by means of a small, short-range radio-based technology. This would be integrated into production line models of a range of different devices.

Bluetooth technology and standards would allow for the replacement of proprietary cables that connect one device to another with a universal short-range radio link. Bluetooth radio links built into both the cellular phone and the computer would replace the cumbersome cable used today to connect a mobile computer to a cellular phone.

2 - HISTORY

Harald Bluetooth was a Viking king, named for his dark complexion, and not for any miss-colored tooth, as might be suspected. His real name was Harald Gormsson. He was king of Norway and Denmark during the 10th century. He waged war against Germany and managed to gather a huge armada of viking ships, whose crews almost overran northern Germany. The German emperor, Otto the Great, just barely managed to defeat them. Harald Bluetooth converted to Christianity and lived a very adventurous life. He was ultimately deposed in a coup, and died in exile.

So, what do a 10th-century Viking king and a new short-range wireless standard have in common? On the surface, not much. But a thousand years after King Harald Bluetooth left his mark on history by unifying Denmark, some bright marketing people at Ericsson thought his achievement could symbolize the unification of the consumer electronics world.

3 - BLUETOOTH

Bluetooth technology is being developed through the combined contributions of the members of the Bluetooth Special Interest Group founded by Ericsson, IBM, Intel, Nokia and Toshiba presently made up of around 1,800 members.

3.1) *AIM*: The aim was to arrive at a specification for a technology that optimizes the usage model of all mobile computing and communications devices, and providing:

1. Global usage
2. Voice and data handling
3. The ability to establish ad-hoc connections
4. The ability to withstand interference from other sources in open band
5. Very small size, in order to accommodate integration into variety of devices
6. Negligible power consumption in comparison to other devices for similar use
7. An open interface standard
8. Low cost

3.2) *CHARACTERISTICS*: Bluetooth is specifically designed to provide low-cost, robust, efficient, high capacity, ad hoc voice and data networking with the following characteristics:

1. 1 Mb/sec. transmission/reception rate that exploits maximum available channel bandwidth.
2. Fast frequency hopping to avoid interference.
3. Adaptive output power to minimize interference.
4. Short data packets to maximize capacity during interference.
5. Fast acknowledge, which allows low coding overhead for links.
6. **CVSD** (Continuous Variable Slope Delta Modulation) voice coding, which enables operation at high bit-error rates.
7. Flexible packet types that supports a wide application range.
8. Relaxed link budget that supports low-cost single chip integration.
9. Transmission/reception interface tailored to minimize current consumption.

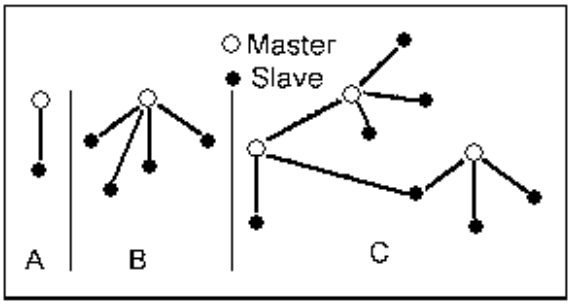
3.3) *THE BLUETOOTH SYSTEM:*

3.3.1) THE FUNCTIONAL UNITS**:** The basic units of the Bluetooth network are the all digital devices such as cellular phones, printers, PC's,etc. which are of two types. These combine to form networks that again are of two types.

The order in the network is as follows:
Single slave(device)→Master unit(device)→Piconet(network)→Scatternet

(network)

#)One could say that there are 2 Types Of Basic Devices in Bluetooth, as shown :
a) Single unit (slave to master or independent)
b) Master unit (up to 7 slave units for 1 master unit)

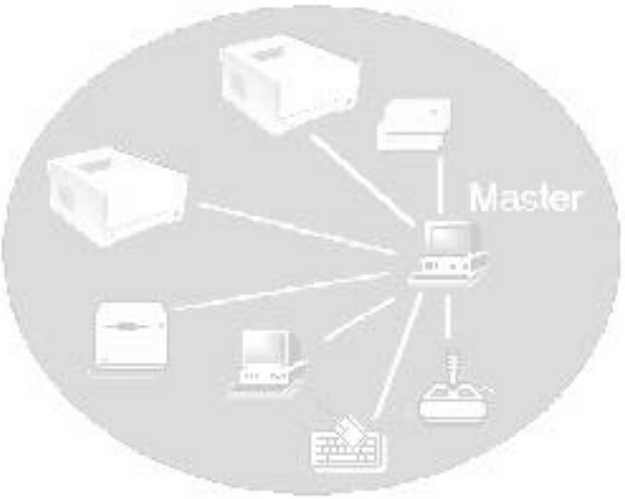


Master units are the devices in a piconet whose clock and hopping sequence are used to synchronize all other devices in the piconet.

Slave units are all devices in a piconet that are not the master (up to 7 active units for each master).

#)PICONET:

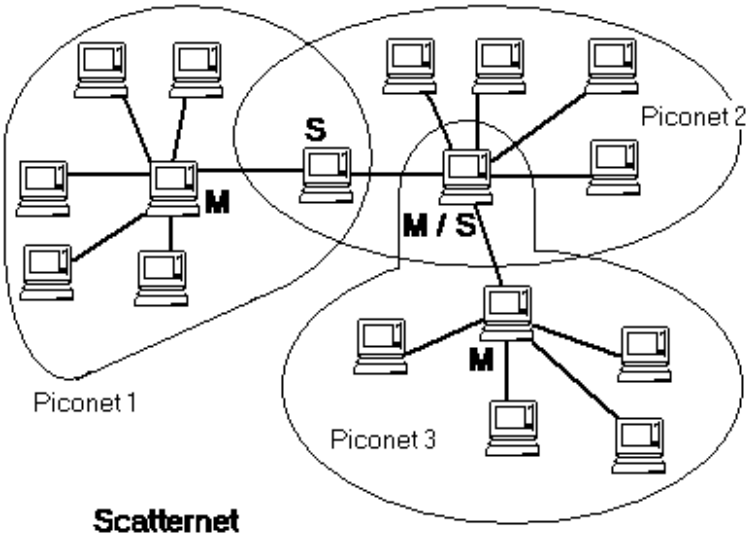
A collection of devices connected via Bluetooth technology in an ad hoc fashion. A piconet starts with two connected devices, such as a portable PC and a mobile



phone. The limit is set at 8 units in a piconet (that´s why the required address-space is limited to 3 bits).
All Bluetooth devices are **peer units** and have identical implementations. However, when establishing a piconet, one unit will act as a master for synchonization purposes, and the other unit(s) will be slave(s) for the duration of the piconet connection.

#)SCATTERNET:

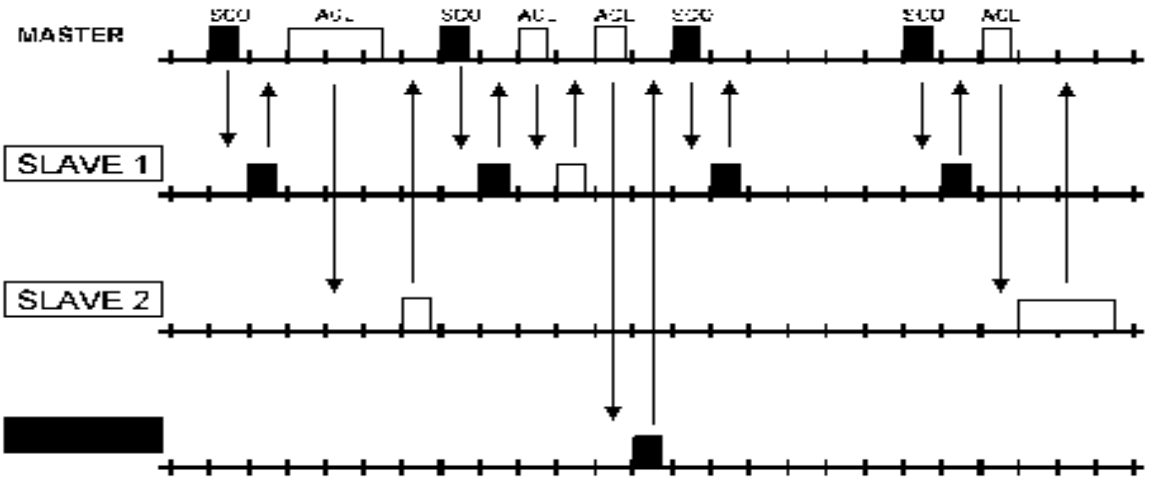
Two or more independent and non-synchronized piconets that communicate with each other. A slave as well as a master unit in one piconet can establish this connection by becoming a slave in the **other** piconet. It will then relay communications between the piconets, if the need arises.



#)COMMUNICATION ROUTES BETWEEN MASTER AND SLAVE

One thing that can be noted from the figure above is that, although Bluetooth works in an ad-hoc fashion (and not server-based) all communication is done visavis the **Master unit.** There is no direct communication between slave units. Nor is it intended for the Master to

route messages between slave units. Rather, if slave units find that they want to talk directly to each other, they would form a new piconet, with one of them acting as Master. This does not mean that they have to **leave** the previous piconet. More likely, they will be



parked in the "old" net unless they decide to quit the "old" net altogether. This is not a big decision for the slave units; reconfiguration in Bluetooth is dynamic and very fast.

#)CREATING A PICONET

A piconet can be created in one of 4 ways:

1. A page (used by Master to connect to Slave)
2. A page scan (a unit listens for its´ device access code)
3. A Master – Slave switch is made
4. An ”Unpark” of a unit is made (provided there are **no** active slaves).

In order to establish new connections the procedures **inquiry** and **paging** are used. The inquiry procedure enables a unit to discover which units are in range, and what their device addresses and clocks are. With the paging procedure, an actual connection can be established. Only the Bluetooth device address is required to set up a connection. Knowledge about the clock will accelerate the setup procedure. A unit that establishes a connection will carry out a page procedure and will automatically become the master of the connection.

For the paging process, several paging schemes can be applied. There is one mandatory paging scheme that has to be supported by each Bluetooth device. This mandatory scheme is used when units meet for the first time, and in case the paging process directly follows the inquiry process. Two units, once connected using a mandatory paging/scanning scheme, may agree on an optional paging/scanning scheme.

#)CREATING A SCATTERNET

A Master or Slave can become Slave in another piconet by being paged by the Master in this other piconet. This automatically means that any unit can create a new piconet by paging a unit that is already a member of a piconet. Any unit participating in one piconet can page the Master or Slave in another piconet. This could lead to a switch of roles between Master and Slave in this new connection. Inter-piconet communications are established over the shared unit.

3.3.2)HOW DOES BLUETOOTH WORK*:* Bluetooth uses a short-range radio link built into a 9 mm x 9 mm microchip. The protocol enables the exchange of information between many devices, including mobile telephones, PDAs, notebook PCs, handheld PCs, associated peripherals, and home hubs. The radio will operate on the globally available 2.45 GHz ISM "free band," meaning there will be no hindrance for international travelers using Bluetooth-enabled equipment.

This is discussed under 5 main sub-divisions:

1)medium of communicaton used
2)transmission power levels used
3)how networks are controlled and formed
4)error correction
5)software architecture
6)authenticaton and privacy

→ MEDIUM OF COMMUNICATION USED:

a) The Bluetooth base band protocol is a **combination** of **circuit** and **packet** switching. Time slots can be reserved for synchronous packets. A frequency hop is done for each packet that is transmitted. A packet nominally covers a single time 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 that simultaneously supports asynchronous data and synchronous voice.

b) Bluetooth uses **frequency hopping in timeslots.** Bluetooth has been designed to operate in noisy radio frequency environments, and uses a fast acknowledgement and a frequency-hopping scheme to make the communications link robust, communication-wise. Bluetooth radio modules avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet.

c) Compared with other systems operating in the same frequency band, the Bluetooth radio typically hops faster and uses shorter packets. This is because **short packages** and **fast hopping** limit the impact of microwave ovens and other sources of disturbances. Use of **Forward Error Correction** (FEC) limits the impact of random noise on long-distance links

d) The link type defines what type of packets can be used on a particular link. The Bluetooth base band technology supports 2 LINK TYPES:

- Synchronous Connection Oriented (**SCO**) type

(used primarily for voice).

- Asynchronous Connectionless (**ACL**) type

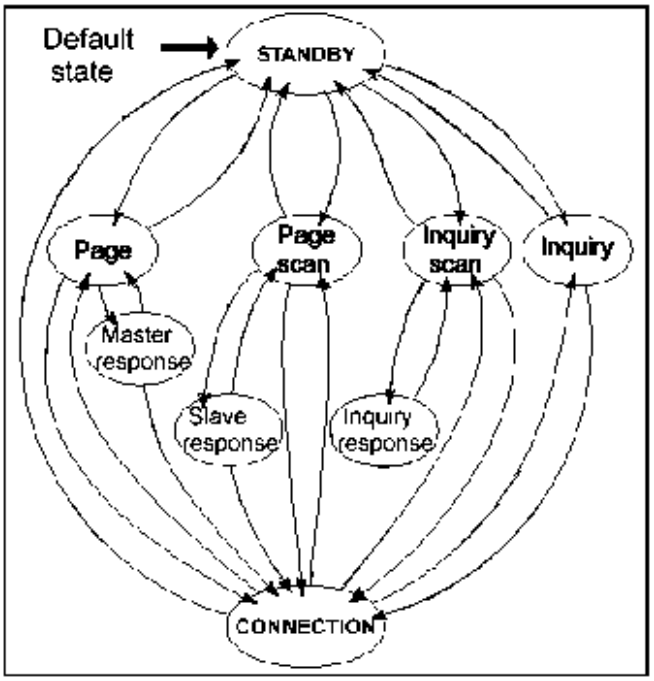
(used primarily for packet data).

Different master-slave pairs of the same piconet can use different link types, and the link type may change arbitrarily during a session. Each link type supports up to sixteen different packet types. Four of these are control packets and are common for both SCO and ACL links. Both link types use a Time Division Duplex (TDD) scheme for full-duplex transmissions.

The SCO link is symmetric and typically supports time-bounded voice traffic. SCO packets are transmitted over reserved intervals. Once the connection is established, both master and slave units may send SCO packets without being polled. One SCO packet type allows both voice and data transmission - with only the data portion being retransmitted when corrupted. The ACL link is packet oriented and supports both symmetric and asymmetric traffic. The master unit controls the link bandwidth and decides how much piconet bandwidth is given to each slave, and the symmetry of the traffic. Slaves must be polled before they can transmit data. The ACL link also supports broadcast messages from the master to all slaves in the piconet.

→ TRANSMISSION POWER LEVELS USED

The Bluetooth radio is built into a small microchip and operates in a globally available frequency band ensuring communication compatibility worldwide. The Bluetooth specification has two power levels defined;



- a lower power level that covers the shorter personal area within a room, and
- a higher power level that can cover a medium range, such as within a home.

Software controls and identity coding built into each microchip ensure that only those units preset by their **owners** can communicate.

→ HOW NETWORKS ARE FORMED AND CONTROLLED

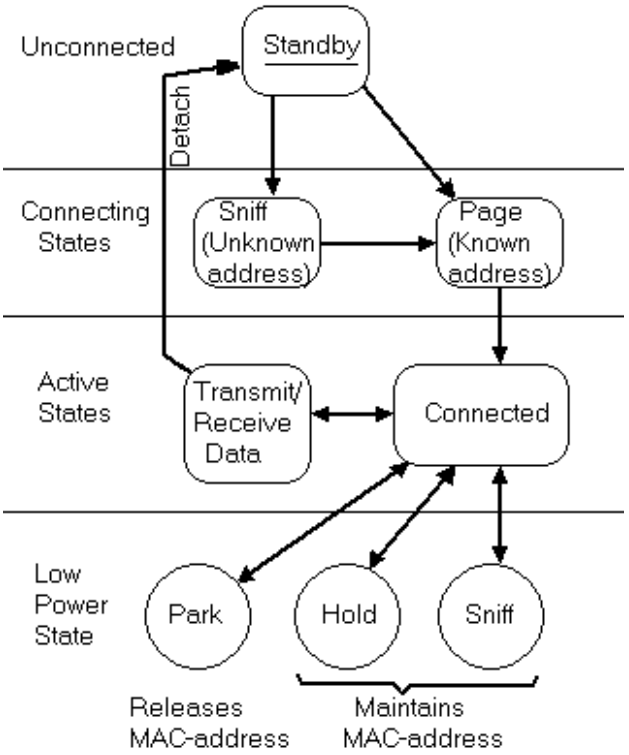
Bluetooth supports both point-to-point and point-to-multi-point connections. Several **piconets** (see definition above) can be established and linked together ad hoc, where each piconet is identified by a different frequency hopping sequence. All users participating on the same piconet are synchronized to this hopping sequence.

a) Before any connections in a piconet are created, all devices are in **STANDBY** mode. In this mode, an unconnected unit periodically "listens" for messages every 1.28 seconds. Each time a device wakes up, it listens on a set of **32 hop frequencies** defined for that unit. The number of hop frequencies varies in different geographic regions; 32 is the number for most countries.

b) The connection procedure for a **non-existent** piconet is initiated by **any** of the devices, which then becomes **master of the piconet thus created.** A connection is made by a **PAGE** message being sent if the **address** is **already known,** or by an **INQUIRY** message followed by a subsequent PAGE message if the **address** is **unknown.**

c) In the initial **PAGE** state, the master unit will send a train of 16 identical page messages on 16 different hop frequencies defined for the device to be paged (slave unit). If no response, the master transmits a train on the remaining 16 hop frequencies in the wake-up sequence.
The maximum delay before the master reaches the slave is twice the wakeup period (2.56 seconds) while the average delay is half the wakeup period (0.64 seconds).

d) The **INQUIRY** message is typically used for finding Bluetooth devices, including public printers, fax machines and similar devices with an unknown address. The INQUIRY message is very similar to the page message, but may require one additional train period to collect all the responses.
A power saving mode can be used for connected units in a piconet if no data needs to be transmitted. The master unit can put slave units into HOLD mode, where only an internal timer is running. Slave units can also demand to be put into HOLD mode. Data transfer restarts instantly when the units transition out of HOLD mode. The HOLD is used when connecting several piconets or managing a low power device such as a temperature sensor.



e) In the **SNIFF** mode, a slave device listens to the piconet at reduced rate, thus reducing its duty cycle. The SNIFF interval is programmable and depends on the application.

f) In the **PARK** mode, a device is still synchronized to the piconet but does not participate in the traffic. Parked devices have given up their MAC address and only occasionally listen to the traffic of the master to re-synchronize and check on broadcast messages. It can thus receive broadcasts, but not addressed while parked.

→ ERROR CORRECTION

There are 3 error-correction schemes defined for Bluetooth baseband controllers:

- 1/3 rate forward error correction code (FEC).
- 2/3 rate forward error correction code (FEC).
- Automatic repeat request (ARQ) scheme for data.

The purpose of the FEC scheme on the data payload is to reduce the number of retransmissions. However, in a reasonably error-free environment, FEC creates unnecessary overhead that reduces the throughput. Therefore, the packet definitions have been kept flexible as to whether or not to use FEC in the payload. The packet header is always protected by a 1/3 rate FEC; it contains valuable link information and should survive bit errors. An unnumbered ARQ scheme is applied in which data transmitted in one slot is directly acknowledged by the recipient in the next slot.

→ SOFTWARE FRAMEWORK

Bluetooth devices will be required to support baseline interoperability feature requirements to create a positive consumer experience. For some devices, these requirements will extend from radio module compliance and air protocols, up to application-level protocols and object exchange formats. For other devices, such as a headset, the feature requirements will be significantly less. Ensuring that any device displaying the Bluetooth "logo" interoperates with other Bluetooth devices is a goal of the Bluetooth program.

Software interoperability begins with the Bluetooth link level protocol responsible for protocol multiplexing, device and service discovery, and segmentation and reassembly. Bluetooth devices must be able to recognize each other and load the appropriate software to discover the higher-level abilities each device supports. Interoperability at the application level requires identical protocol stacks. Different classes of Bluetooth devices (PC's, handhelds, headsets, cellular telephones) have different compliance requirements. More functionality would be expected from cellular phones, handheld and notebook computers. To obtain this functionality, the Bluetooth software framework will reuse existing specifications such as OBEX, Human Interface Device (HID), and TCP/IP rather than invent yet another set of new specifications.

→ AUTHENTICATION AND PRIVACY

The Bluetooth baseband provides user protection and information privacy mechanisms at the physical layer. Authentication and encryption is implemented in the same way in each Bluetooth device, appropriate for the ad hoc nature of the network. Connections may require a one-way, two-way, or no authentication. Authentication is based on a challenge-response algorithm. Authentication is a key component of any Bluetooth system, allowing the user to develop a domain of trust between a personal Bluetooth device, such as allowing only the owner's notebook computer to communicate through the owner's cellular telephone. Encryption is used to protect the privacy of the connection. Bluetooth uses a stream cipher well suited for a silicon implementation with secret key lengths of 0, 40, or 64 bits. Key management is left to higher layer software.

The Bluetooth system is fully compliant and based on the standards laid down by the IEEE, namely the IEEE 802.11 standard. The IEEE manages most of the standards for wired LANs. The IEEE 802.11 represents the first standard for WLAN products from an internationally recognized, independent organization.The IEEE 802.11 defines physical layer options for wireless transmission and MAC layer protocol.

The balance of the SPECIFICATIONS are as follows1:

Frequency Band: 2.4 GHz (unlicensed ISM Band)

Transmitter Power: 1 milliWatt (0 dBm)

Technology: Spread Spectrum

Hybrid Direct sequence and frequency hopping

Maximum Voice Channels: 3 per piconet

Maximum Data Channels: 7 per piconet

Data speed: 721 Kbps per piconet

Expected System Range: 10 meters (40 feet)

Number of Devices Supported: 8 per piconet, 10 piconets in coverage area2

Security: Yes, link layer

Power Requirement: 2.7 volts

Power Consumption: 30 uA sleep, 60 uA hold, 300 uA standby

8-30 mA transmitting

Module size: 0.5 square inches

Interference: Bluetooth minimizes potential interference by employing fast frequency hopping-1600 times a second

4 - ADVANTAGES AND DISADVANTAGES

4.1)*ADVANTAGES:*

a) The Bluetooth chips communicate on the 2.4 Ghz radio frequency ISM which doesn't have to be licensed.Thus it can be used freely all over the world.

b) It has a range of upto 30 feet, sufficient for most home and office use.

c) Bluetooth does not require line of sight for connection, provided they are within operational range of other Bluetooth-enabled devices.

d) The Bluetooth baseband protocol is suitable for both voice and data.Each voice channel supports a 64 Kbit/s synchronous (voice) link, and the asynchronous channel can support an asymmetric link of up to 721 Kbit/s in either direction, while permitting 57.6 Kbit/s in the return direction.

e) It will also be possible to send digital images via Bluetooth-compliant digital devices and as the bandwidth and frequency range increases, full-length movies and clips can be transmitted.

f) It offers the unification of all the electronic devices
to make a truly wireless and connected world.

LESS WIRE …..MORE LIFE.

OVER OTHER COMPETING TECHNOLOGIES:

a) Bluetooth vs. WAP: ”WAP - Wireless Application Protocol - is a framework specified by industry leaders supporting mobile IT-solutions”. It is a communications protocol for mobile phones, meant as an extension of available, Internet-based services. WAP only covers the higher protocol levels. There is no connection to the IEEE 802.11 standard with which Bluetooth is compliant. WAP might not survive for long; Japan has a corresponding service that is far more extensive.

b) Bluetooth vs. Infrared: One of the 3 IrDa-standards that are used today is called ”IrDa-Data”, and this standard is primarily meant for data transmission. But the main differences as compared to Bluetooth are:

- IrDa is not omnidirectional, as is Bluetooth. The IrDa-beam has to be aimed at the receiving antenna.
- IrDa must hav a free line of sight which Bluetooth does not require
- IrDa is point-to-point; only 2 units at a time can communicate where as in Bluetooth upto 8 can commubnicate in any given piconet at one time.

c) Bluetooth vs. Smart Cards: . Contactless "smart" cards are the basis of some Bluetooth-applications. But Bluetooth goes much further than that. Smart cards:

- are point-to-point
- are not session-oriented
- have no inherent reliability when transmitting/receiving information. They are better compared with the contactless transmission-mode on the Internet.

All the functionality that ”smart cards” have can be included in Bluetooth´s functionality.

d) Bluetooth vs. Wireless LAN: WLANs are essentially ordinary LAN-protocols modulated on carrier waves. Bluetooth is more complex than that.

- Bluetooth´s essence is dynamically configured units. That´s not how LANs work.
- Bluetooth hops very fast (1600 hops/second) between frequencies, which does not allow for long datablocks. A Bluetooth channel cannot handle as high data throughput as a WLAN.
- Bluetooth relies on ad-hoc-connectivity. This does not square well with (predominantly) server-based LANs.

Moreover, when a Bluetooth connection collides with a wireless LAN connection, either or both connections can jam! Bluetooth may be a boon to mobile devices, but to wireless LANs, it's a bully!!

4.2) *DISADVANTAGES:*

a) Bluetooth is by its nature **not** designed to carry heavy traffic loads. It would thus **not** be a suitable technology for replacing LAN-, WAN- and Backbone cables.

b) Bluetooth is not suitable in server-based applications since the emphasis in Bluetooth is on mobile, re-configurable computerized units that need sporadic contact with each other.

c) A proliferation of devices and technologies translates into growing number of potential vulnerabilities. Thus a lot of care has to be taken to develop end-to-end security in order to make such huge complex interoperable networks.

However, we can anticipate the Bluetooth SIG to evolve the Bluetooth technology to provide greater bandwidth and distances, thus increasing the potential platforms and applications used in the emerging personal area-networking marketplace. Also, the Bluetooth SIG is spending 50 % of its resources on making the network more secure.

5-USES OF BLUETOOTH

In order to grasp the scope of a groundbreaking technology such as Bluetooth, we will give the uses in the form of a world of wireless devices around you.

In the Office ...

You arrive at the office and put down your briefcase. While in your office, your Personal Digital Assistant (PDA) automatically synchronizes with your desktop PC and transfers files, e-mails and schedule information. While in a meeting, you access your PDA to send your presentation to

the electronic whiteboard. You record meeting minutes on your PDA and wirelessly transfer these to the attendees before they leave the meeting.

You are the factory supervisor for Widgets, Inc. As you walk through the factory, you are able to check the status of every piece of test equipment you encounter because you can instantly download a user interface for every machine. You request product defect rates and piece part failures at selected workstations.

In the Home ...

Upon arriving at your home, the door automatically unlocks for you, the entryway lights come on, and the heat is adjusted to your pre-set preferences. An alarm notifies you that your toddler has just left the house. Your PDA morphs from business to personal as you enter your home. An electronic bulletin board in the home automatically adds your scheduled activities to the family calendar, and alerts you of any conflicts. You have a home security system composed of Bluetooth-enabled devices. You have just upgraded the system and added devices. Because they are all Bluetooth-enabled, they automatically reconfigure and recognize each other.

On the Road ...

You arrive at the airport. A long line is formed for ticketing and seat assignment. You avoid the line, using your PDA to present an electronic ticket and automatically select your seat. The airline's on-line system checks identification via the "ID-tag" feature built into your PDA and confirms your reserved seat. You enter the airport-waiting lounge, equipped with Bluetooth-enabled Internet ports. Via the ports, you and other guests use Bluetooth-enabled laptops, PDAs, and other devices to access your office or home-based servers via the airline server. Using voice-over IP, you also make "free" Internet voice calls courtesy of your airline. You get on the Rent-A-Car bus. Your reservation is automatically transferred to the Rent-A-Car database, and you are dropped off at your car. You get in the Bluetooth-enabled rental car. Your hotel reservations are automatically queried from your PDA and the GPS system offers you directions to your hotel.

You arrive at the hotel. As you enter, you are automatically checked in and your room number and electronic key are transferred to your PDA. As you approach the room, the door automatically opens.

In the Car ...

As you enter a national park, a map of the park appears on your display. You can view the schedule of activities for the park and your own personal electronic tour guide is downloaded to your vehicle. As you approach your vehicle, the door unlocks automatically, the radio tunes in your favorite station, and the seat adjusts to your preferred settings. As you enter your vehicle, you are reminded of the items on your daily calendar and the results of a recent diagnostic test of your vehicle. You receive a new message en route, which is verbally transmitted to you via the vehicle's speakerphone.

In Social Settings ...

Anxious to see the first run movie, you arrive at the theater to find a long line at the ticket counter. Using your Bluetooth-enabled PDA to wirelessly confirm and pay for your tickets, you avoid the long line, enter the theater, and take your preferred seat. At the racetrack, your PDA is used to download information on selected horses and jockies, to perform statistical analysis using historical information, to place bets, to request slow-motion replays, and to order food and beverage. You are attending an industry trade show. You have preloaded your preferences for product information into your PDA. As you walk through the exhibits, your PDA detects other Bluetooth-enabled PDAs and exchanges preference information. Bluetooth facilitates the exchange of information, and enables you to meet others with common interests.

As you enter an up-scale bar, you are handed a Bluetooth-enabled device. This device allows you to send messages and communicate with others in the bar, to order and pay for food and beverage, and to participate in games such as Trivia and Clue.

7 - REFERENCES:

1)www.abc.se

2)www.nokia.com

3)research.ibm.com

4)www.mit.edu

5)www.bluetooth.com

6)scis.nova.edu

7)intercai.co.uk

8)services.ask.com

9)www.ericsson.com

10)The Economic Times(Corporate Dossier)

11)www.intel.com

6 - GLOSSARY

Mac address:A 3-bit Media Access Control address used to distinguish between units participating in the piconet.

Parked units:Devices in a piconet which are regularly synchronized but do not have MAC addresses. They are woken up by the Master with a ”beacon signal”.

Sniff mode and hold mode:Devices that are synchronized to a piconet, and which have temporarily entered power-saving modes in which device activity is lowered. They keep their MAC-addresses.

The Beacon-channel: To support slave s, the Master establishes a beacon channel when one or more slaves are parked. This channel consists of one beacon slot, or a train of equidistant beacon slots transmitted at constant time interval.

TCP/IP: Transmission Control Protocol/Internet Protocol

HID : Human Interface Device

Ad-hoc network: is a simple network where communications are established between multiple stations in a given coverage area without the use of an access point or server.

FEC: Forward Error Correction

WWW: World Wide Web

SIG: Special Interest Group

PIN: Personal Identification Number