PENNSTATE

Dept. of Electrical Engineering
State College, PA16802

Overview of Bluetooth Technology

Hongfeng Wang

July 3, 2001

Index

1. Overview of Bluetooth

During the past two decades, the progress in microelectronics and VLSI technology drove the cost of many consumer electronic products down to an acceptable level for average people. Only in the 1st quarter of 2001, over 32.5 million PCs were sold. The number of cellular phones is predicted to reach 1 billion in 2005. With the increase of the number of these devices, so does the need of connecting them together. Today numerous kinds of special cables are used for interconnection. It's cumbersome, not interchangeable and expensive. Bluetooth is devised to replace these cables.

Bluetooth is a low cost, low power, radio frequency technology for short-range communications. It can be used to replace the cables connecting portable/fixed electronic devices, build ad-hoc networks or provide data/voice access points.

Figure 1. A Bluetooth Module

Frequency	2.4GHz ISM band, Frequency hopping
Modulation	Gaussian shaped BFSK
Data rate	723Kbps
Operating range	10m~100m
Size	28mm x 15mm x 2mm (Mitsumi WML-C05)
Cost	Long term: $5/endpoint ($20 currently)
Power	0.1W (Active)
Security	Good. FHSS. Link layer authentication and encryption
Acceptance	SIG have about 2500 member companies

Table 1. Bluetooth Summary

The research on Bluetooth was initiated at Ericsson of Sweden in 1994. The idea of Bluetooth comes from the desire to connect cellular phones with other devices without a cable. It's named after the 10th century Viking king of Denmark Herald Bluetooth.

The advancement in microelectronics makes it possible to integrate complex functions into one small chip and thus achieve a low cost. With its low cost, low power consumption and low profile, you can virtually put one anywhere you want. This will make many concepts like smart appliances and embedded Internet possible.

The development gained support from many companies. Currently, there are about 2500 companies joined the Bluetooth Special Interest Group (SIG). There are some commercial products available, and much more are rolling out. For more information on market, see chapter 3.

A new standard for Wireless Personal Area Network (WPAN)-IEEE802.15 is being developed, and to a large extent, it's an extension of Bluetooth.

Despite its advantages, one of its key limitations so far is its speed. With a maximum data rate of 720KBps, it cannot be used to connect DVD players or HDTV, and it takes a long time to transfer large picture files to a printer. New version of Bluetooth may address this issue and have much higher data rate.

2. Technologies of Bluetooth

Like any other engineering practice, the design of Bluetooth has to compromise between different goals, like high throughput and low cost, large operation range and low power consumption. Throughout the specifications, you will find out the most deciding factors are low power and low cost. That's the key for mobile applications.

Technical Challenges	***Solutions***
Global operation	2.4GHz ISM band
Interference from other devices using ISM band and other Bluetooth devices	FHSS, Error correction coding
Low power consumption	Power control, Power-saving modes, Programmable packet length, Moderate data rate
Low cost	FHSS, TDMA, low receiver sensitivity, Relaxed link budget, Low IF
Security	FHSS, link layer security (Authentication and Encryption)
High error probability of wireless link	ARQ, FEC and CVSD (audio)
Voice/Data support	Circuit/Packet Switching

Table2. Bluetooth Technical Solutions

Figure 2 is typical hardware architecture of one Bluetooth module. Although the original goal is single chip implementation, due to difficulties of integrating RF part into CMOS chip, many vendors now use one baseband chip and one RF chip. Cambridge Silicon Radio is working on one chip solution, and already has some exciting products available. Its BlueCore™ has almost all the functions in the chip, and only needs about 10 discrete components to construct a module. This makes people believe that the $5 goal may be not very far away.

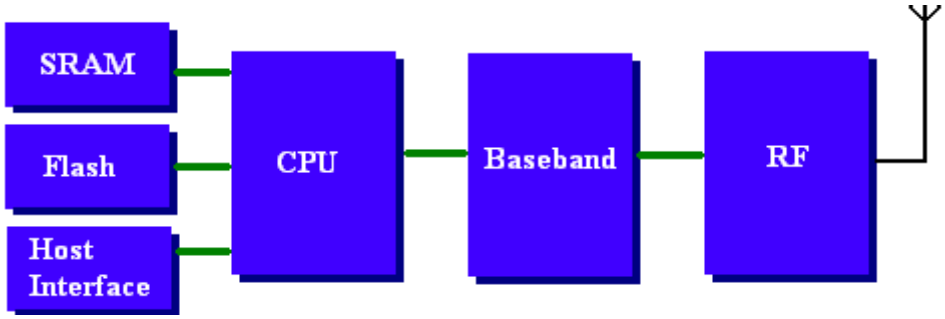

Figure 2. Bluetooth Hardware

In this paper, we will concentrate on the RF and baseband of Bluetooth.

2.1 RF of Bluetooth

2.1.1 Frequency band and RF channels

- Works in ISM band: 2.4~2.4835 GHz (US, Europe and most other countries)
- Carrier frequency: f=2402+k MHz k=0...78
- Hopping rate: 1 hop/packet. 1600 hop/s for 1 slot packet
- Channel bandwidth: 1MHz(-20dB) 220KHz(-3dB)

Bluetooth uses 2.4GHz ISM band because it is an unlicensed band, and available in most countries. At this frequency (λ=12.3cm), a very small antenna is possible. And higher frequency band may cause high cost on RF.

For some countries with different bandwidth allocations, a reduced hop (23 hops) system is defined. According to current version of Bluetooth specs, 79/23 hops system can't communicate to each other. This is a big problem for the original goal of global standard. However, Bluetooth SIG has been actively lobbying those countries with different regulations. France and Japan recently released the full ISM band. Spain is also working on it. It is very likely to use the same band globally in the future.

In the 2.4GHz ISM band, the use of spread spectrum is mandatory. Although DSSS can achieve higher data rate (11Mbps for 802.11b standard), FHSS has its advantage of low cost, low power, better security. FHSS also handles near-far problem better, since it will effectively block out-of-band signals. Considering the possible applications of Bluetooth, FHSS is a better solution.

The hopping sequence is calculated using the master's Bluetooth Device Address. It hops to every 1MHz channel with equal probability. Its 1600hops/sec fast hopping rate

is enough to overcome slow fading in most indoor environment, which has Doppler spread of 0.1~6Hz. The RMS delay spread usually ranges from 100ns to 10μs [30]. A typical 0.25μs RMS delay spread corresponds to 640KHz coherent bandwidth. So different 1MHz channels will have different radio characteristics, and the FHSS will effectively solve the multipath and fading problem.

For 1MHz channel, the 1Msps symbol rate is already fully exploiting the bandwidth. The 1MHz channel bandwidth was the requirement of FCC, but recent decision from FCC changed that to 5MHz. This will probably enable the future version protocol to get higher data rate. HomeRF is already taking advantage of this 5MHz channel to get 10Mbps throughput.

2.4GHz ISM band is free to all, so many applications now are using this band. These applications include digital cordless phone, WLAN (802.11b), HomeRF, RFID, microwave oven and many other proprietary technologies. Although spread spectrum is mandatory for devices with a transmit power over 0dBm, considering the possible large number of units working in the same band, many people are worrying that the interference will make this band a “garbage band”. WLAN is trying to migrate to the 5.7GHz band.

2.1.2 Transmitter characteristics

For higher bandwidth efficiency, Gaussian shaped binary FSK is used in Bluetooth. The bandwidth time product BT=0.5.

The nominal modulation index is 0.3. A binary zero is represented by negative frequency deviation, and one is represented by positive frequency deviation. The frequency deviation is no less than 115 KHz.

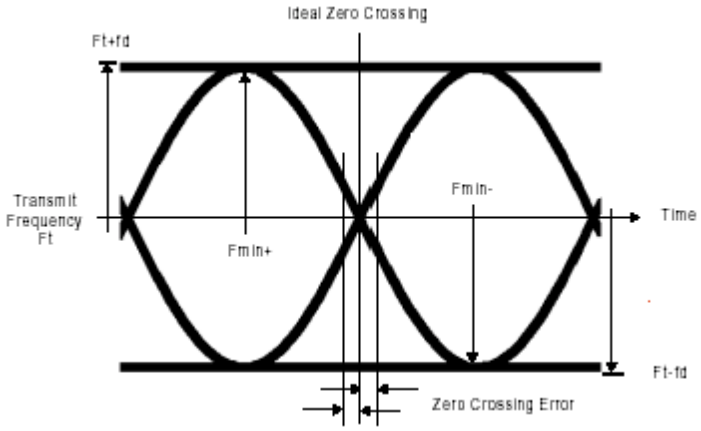

Figure 3. GFSK Modulation [Bluetooth SIG]

GFSK is constant-envelope modulation, which enables the use of class C power amplifier for high power efficiency. It's also easier to implement compared to other modulation techniques.

Bluetooth devices are divided to 3 power classes:

- Class 1: maximum output power of 20 dBm
- Class 2: maximum output power of 4 dBm
- Class 3: maximum output power of 0 dBm

Power control is mandatory for class 1 devices, and optional for others. Power control can effectively reduce the power consumption, which is critical for many portable devices. Power control can also minimize the interference to other devices.

The power is controlled by Link Management Protocol (LMP) layer.

The Bluetooth operating range depends on the environment. In an open space, the Bluetooth unit may have a large operating range.

Power Class	**Max Output Power**	**Max Output Power**	**Expected Range**	**Range in Free Space**
Class 1	100mW	20dBm	42m	300m
Class 2	2.5mW	4dBm	16m	50m
Class 3	1mW	0dBm	10m	30m

Table 3. Power Classes and Range

The range calculation is based on A. Kamerman's indoor propagation model [23]:

$$\text{Lpath} = 20 \log (4\pi r / \lambda) \qquad r \leq 8\text{m}$$

$$= 58.3 + 33 \log (r / 8) \qquad r > 8\text{m}$$

0dB antenna gain is assumed for generality, although directional antenna is applicable. 8 dB fading margin is added; this is comparable to what's assumed in many cellular systems.

2.1.3 Receiver characteristics

For a raw bit error rate of 0.1%, Bluetooth devices should have a minimum sensitivity of -70dBm, maximum-usable signal level of -20dBm. That's a dynamic range of 50dB. Compared to that of many cellular phones, the sensitivity level of Bluetooth is much higher. The purpose is to allow higher substrate noise and low current LNA, thus to minimize the cost. A noise figure as large as 23 dB is allowed in Bluetooth receiver [11]. The high noise figure allows the use of inexpensive components, and on-chip-interference for single chip implementation.

For a raw bit error rate of 0.1%, Bluetooth devices should stand a co-channel interference of carrier to interference ratio CIR=11dB, 1MHz adjacent channel interference of CIR=0dB, 2MHz adjacent channel interference of CIR=-30dB and 3MHz adjacent channel interference of CIR=-40dB. These requirements translate to phase noise requirement for the VCO of –124dBc/Hz [18], this is less demanding than most cellular systems. This allows simple on-chip VCO implementation.

Receiver Signal Strength Indicator (RSSI) is an optional feature, but most vendors selected to implement it, since this will help reduce the power consumption. It compares the received signal power to upper and lower thresholds to see if it's within the "golden range" and notifies the transmitter via LMP.

RF design currently is a big hurdle for the Bluetooth single chip implementation. The cost of RF chip is the major part of most Bluetooth solutions now. The major difficulties to integrate RF circuit to deep sub-micron CMOS chip include lack of good RF model for CMOS circuit, and making high quality passive components.

For the down converter, Very Low IF and Direct Conversion Receiver are gaining more support, because they have low requirements on filters and are easy to be integrated into CMOS chip. The low IF also eliminates the requirement for in-band image rejection filter, thus reduces the cost and power consumption.

A LIF is used in the transceiver diagram Figure1.

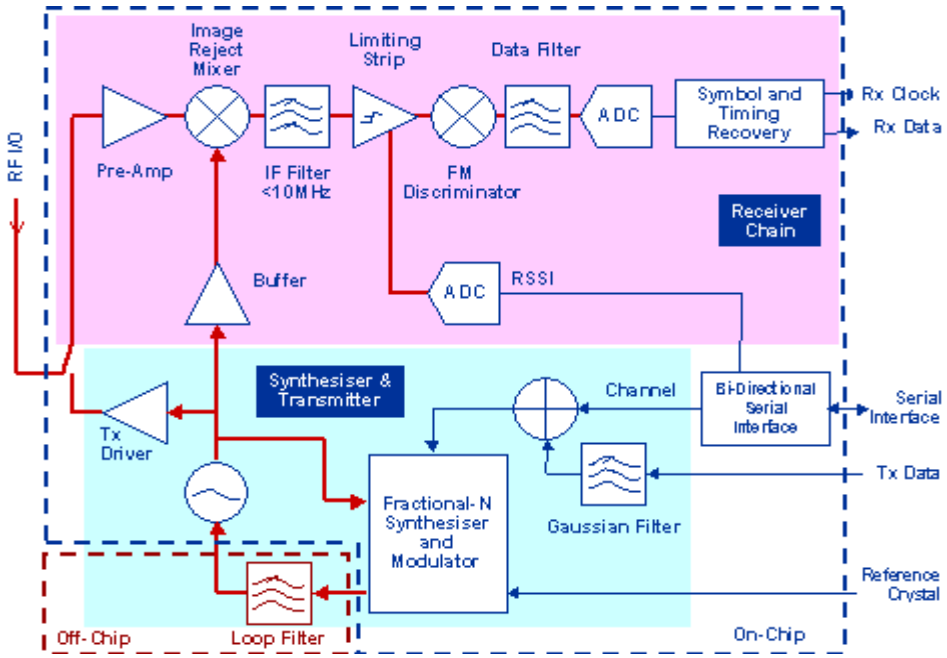

Figure 4. Diagram of a Bluetooth Transceiver

2.2 Baseband of Bluetooth

2.2.1 Networking

Bluetooth provides point-to-point and point-to-multipoint connections. Several Bluetooth devices sharing the same channel (hopping sequence) form a piconet. The unit that initiates the connection acts as the master, and it can have up to 7 active slaves and 256 parked slaves. Physically the master and slave units are the same.

The master unit and one of it slave units may switch their roles in some cases. This capability is useful when the master wants to accommodate other piconets or setup a new piconet.

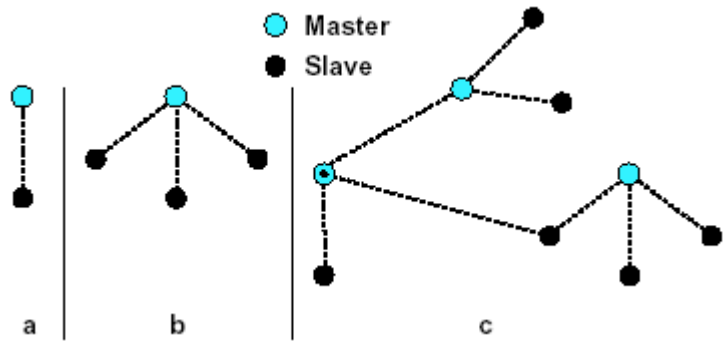

Figure 5. Bluetooth Network Topology [Bluetooth SIG]

Bluetooth provides ad hoc connectivity. Every Bluetooth unit can connect to other Bluetooth devices without the need of any infrastructure support or access points.

A member of one piconet could also be a member of another piconet. A unit participating multiple piconets do so on time division basis. Before one unit leaves one

piconet, it tells the master it will not be available for a predetermined interval and places itself in sniff, hold or park mode, and then it adjusts its clock to another piconet and joins the conversation there. Such a unit may act as the bridge between two piconets.

A master could also be a slave of another piconet, but the communications of the whole piconet has to come to a full stop when it leaves, unless it switched its role with a slave. One unit cannot be the masters of two piconets at the same time; otherwise these two piconets will have the same hopping sequence and timing.

Bluetooth doesn't support handoff between different piconets, since its target market is not Wireless LAN, but cable replacement and ad hoc network. However, such capability could be implemented in the network built on Bluetooth. Some research in this topic is going on [19].

Many piconets together form a scatternet. Up to 10 piconets can work together with minimal impact on each other. The throughput degradation in the presence of multiple piconet is given by [11]:

$$TH=(1-1/79)^{N-1}$$

So the overall throughput of the scatternet could reach well above 10Mbps. The topology of scatternet will also effectively extend the operation range when some units act as bridge.

Slaves in the same piconet cannot communicate with each other directly. If one slave wants to talk to another, it can page that slave and set up a new piconet, or request to change its role from slave to master.

Each Bluetooth unit has a unique 48-bit Bluetooth Device Address; this address is derived from IEEE802 standard.

A single Bluetooth channel has about 1Mbps data rate. Discussion of higher data rate version is underway. It's believed the future version will have a 10Mbps data rate to accommodate applications like real time video.

2.2.2 Physical links

Each piconet has a unique frequency hopping sequence. The sequence is determined by the Bluetooth Device Address of the master of the piconet. Since different piconets have different hopping sequence, they can communicate without interfering with each other, when the number of adjacent piconets is small. In typical office environment, up to 10 overlapped piconets can work very well with little impact on one another.

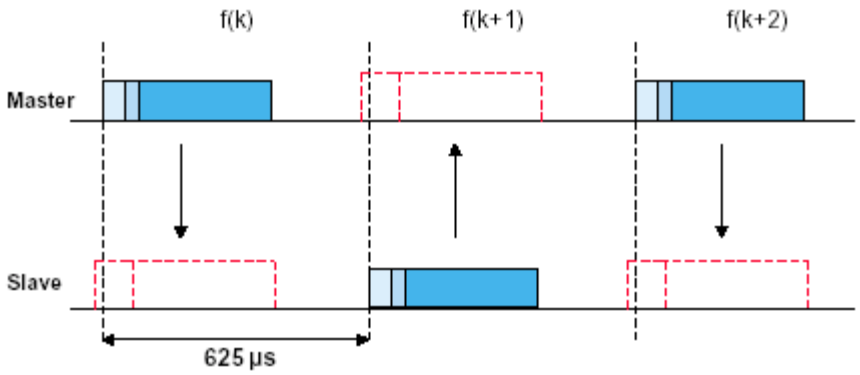

Figure 6. Bluetooth MAC scheme [Bluetooth SIG]

The channel is time divided to slots of length 625 µS. Each packet can occupy 1, 3 or 5 slots. The hopping frequency keeps constant within a packet. The master uses the odd-numbered slots to transmit packets and the slaves use the even numbered slots. Duplex between master and slaves is achieved by time division. One slave is only allowed to send packet to the master if the preceding packet is addressed to it. So this is a centralized TDD scheme totally controlled by the master unit.

Regular polling from the master is needed; otherwise the slave may not be able to get access to the channel for a long time if the master doesn't communicate with it.

Compared to 802.11's CSMA/CA, TDD is easier to implement. Its hopping nature also makes the back-off algorithm less efficient, because it will meet different interferers at different frequencies.

A slave synchronizes its clock to the master whenever it receives a packet from the master, and this packet is not necessarily addressed to it, since the access code in every packet can be used for synchronization.

Actually a one-slot packet doesn't occupy the slot fully. For example, a DH1 packet only has 366 bits, so it will only last 366 μS, much smaller than the 625 μS slot length. This will reduce the system throughput somewhat, but this will give the transceiver enough turn-around time to switch between transmit and receive modes. So only one oscillator is needed, this will help reduce the cost. Also the low dwell time will reduce the probability of collision with other applications accessing the channel.

There are two types of physical links: SCO (Synchronous Connection-Oriented) link and ACL (Asynchronous Connection-Less) link. One unit can have 1 ACL link and up to 2 (3 for master) SCO links simultaneously.

The master maintains one SCO link by reserve slots of regular interval. It can be considered as a circuit switched connection, so it's ideal to transmit time-bounded information like voice. The maximum data rate for one SCO link is 64Kbps.

The SCO link is point-to-point and symmetric. The slave can always respond to the master following the reserved master to slave slot.

Both the master and the slaves can initiate a SCO link.

The ACL link uses all the slots not reserved by SCO links to exchange data between master and all slaves. Master can use ACL link to talk to any single slave as well as to do a broadcast to all slaves.

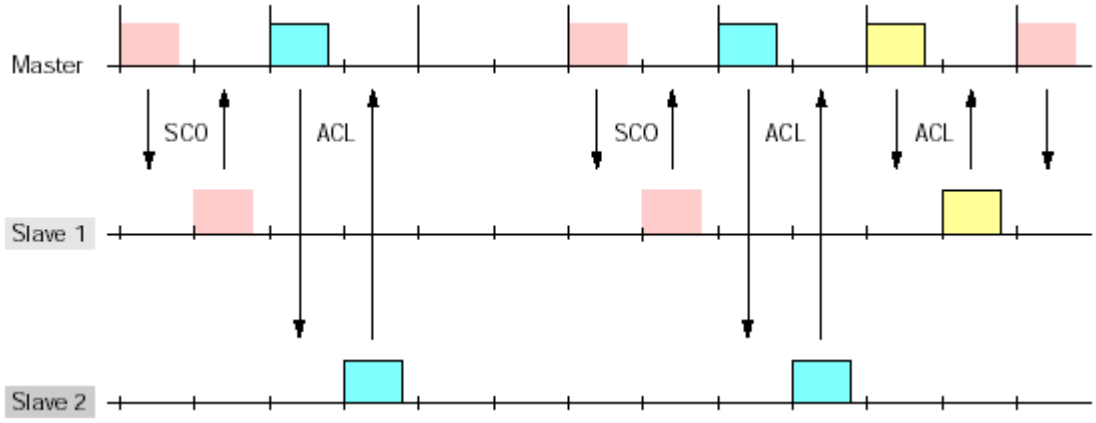

Figure 7. Bluetooth MAC scheme [Ericsson]

The packets on ACL link use different FEC schemes (see Table 5), the selection of FEC scheme depends on the quality of the link. This provides applications flexibility to communicate in different environments and get maximum throughput.

By using both circuit switching and packet switching, Bluetooth can provide better support to mixed voice and data communications. This capability also gets Bluetooth a wide range of application: from data access points to headsets.

The SCO and ACL links setup and configuration are managed by Link Manager Protocol (LMP).

2.2.3 Packets

Each packet has 72-bits access code, 54-bits header and payload of variable size. Compared to 802.11b, the packet of Bluetooth is much smaller, giving it advantage of lower probability of error.

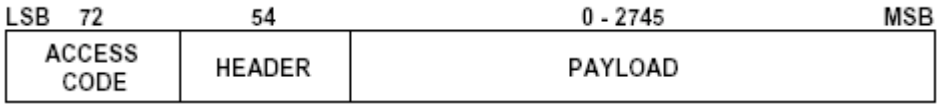

Figure 8. Bluetooth Packet Format [Bluetooth SIG]

The access code is the same for all packets transmitted in one piconet. It consists of a 4-bit preamble, a 64-bit synchronization word and possibly a 4-bit trailer. The receiver of one Bluetooth unit uses a slide correlator to correlate against the sync word to determine the timing. Depending on the state of the piconet, the sync word is generated in different ways. The preamble and trailer are used for DC compensation.

One unit can find if the packet is addressed to it simply by looking at the header, it will go back to sleep for the rest of the slot if it is not for it. This design will reduce the power consumption even in the active mode.

The packet header has six fields:

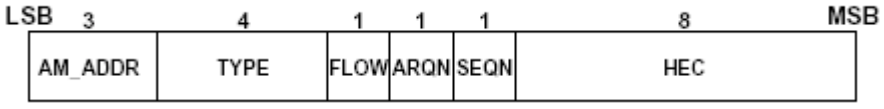

Figure 9. Format of Packet Header [Bluetooth SIG]

- The AM_ADDR is the address of the active member the master used to distinguish them.

- The TYPE field contains information like how long the packet will last, the error correction scheme it uses and the type of the packet, for example it may be used to poll the slave or synchronization only.
- The FLOW bit is used for flow control in the ACL link.
- The ARQN is used for ARQ. See 2.2.4 for details.
- The SEQN bit is used to differentiate retransmitted packets from new ones.
- The HEC is an 8-bit header error check.

For further protection, the whole header including the HEC is encoded to 1/3 rate FEC of 54 bits to achieve more robustness.

The payload is of variable size, depending on the type of packet. The SCO link has only fixed-length voice field (with exception of DV packet, which has both voice and data field). On the ACL link, the data field itself contains a payload header, a payload body and possibly a payload CRC code.

The payload header contains 3 fields:

- 2-bit L_CH, used to identify logical channels
- 1-bit FLOW for flow control
- 5-bit LENGTH (8-bit for multi-slot packets) to indicate the variable payload size

There are seven types of data packets providing different error-correction scheme and throughput capability. The use of different types of packets depends on the negotiation result between the sender and receiver through the LMP.

Packet Type	FEC	CRC	Slot	Max Symmetric rate (two way)	Max Forward (Asymmetric) rate	Max Reverse (Asymmetric) rate
DM1	2/3	Yes	1	108.8	108.8	108.8
DH1	No	Yes	1	172.8	172.8	172.8
DM3	2/3	Yes	3	258.1	387.2	54.4
DH3	No	Yes	3	390.4	585.6	86.4
DM5	2/3	Yes	5	286.7	477.8	36.3
DH5	No	Yes	5	433.9	723.2	57.6
AUX1	No	No	1	185.6	185.6	185.6

Table 4. Data packets type and their throughput

DV packet is a special packet transferred over SCO link. It contains an 80 bits voice field and an up to 150 bits data field. Up to 10 bytes of data could be sent in one DV packet. The data and a 16 bits CRC together are encoded using 2/3 rate FEC.

The DV packet format provides some time-bounded applications an effective means to transfer data through circuit switched data path.

There are 4 types of control packets used: ID, NULL, POLL and FHS. They are common to both SCO and ACL links. They are used for synchronization, polling and other channel control functions.

Packet Type	Length	Content	Use
ID	68 bits	Access code	Inquiry, page and response routines
NULL	126 bits	Access code + header	ARQ acknowledgement, flow control
POLL	126 bits	Access code + header	Regular polling of slaves
FHS	366 bits	Bluetooth device Address sender clock	Synchronization

Table 5. Types of control packets

2.2.4 Error Correction

Due to various inferences, a wireless RF link has high probability of error. Bluetooth has 5 error correction measures:

- 8-bit Header Error Correction (HEC).

  It is only used in header.

  Its generator polynomial: $g(D)=D^8+D^7+D^5+D^2+D+1$

- 16-bit CRC

  It is used to protect data payload.

  Its generator polynomial: $g(D)=D^{16}+D^{12}+D^5+1$

- 1/3 rate FEC

  It simply uses 3-times repetition code. It's usually used in links with very high probability of error.

- 2/3 rate FEC

  It uses a (15,10) shortened Hamming code, with the generator polynomial of $g(D)=D^5+D^4+D^2+1$. This scheme is used in medium rate data transmission.

- ARQ

  The ARQ scheme of Bluetooth uses unnumbered fast ARQ. Whenever the slave received the packet from master successfully, it acknowledges the master by set the ARQN bit to 1 in the packet it replies to the master. Based on this information the master decides if to transmit a new packet or retransmit the previous one. The master will keep retransmitting the packet until it gets an indication of successful reception (or a timeout occurs). It's similar for the master to slave packets. This is a stop-and-

wait scheme, with a minimal wait period. This fast ARQ scheme will help to minimize the overhead of retransmission.

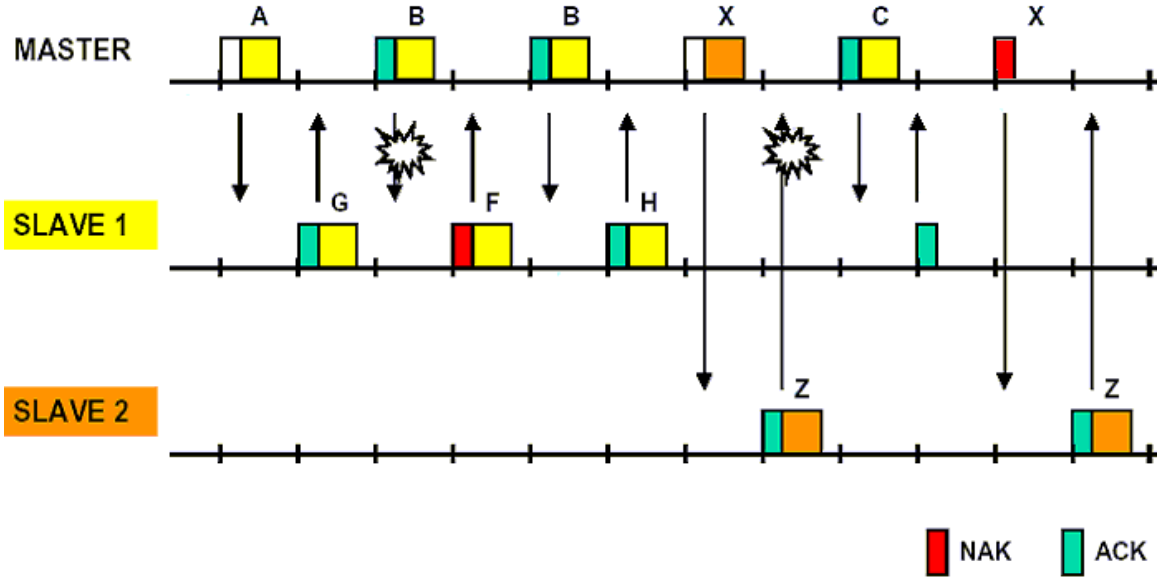

Figure 10. ARQ [Courtesy of Ericsson]

Depending on the quality of the link, 1/3 rate FEC, 2/3 FEC or no FEC at all may be used. The selection of different error correction schemes (so different packet types) is done by LMP, that monitors the link quality and negotiates for appropriate data rate between the sender and the receiver. The change could be dynamic during one connection session.

Sometimes more than one error correction scheme is used. For example the header of one packet is protected by 8-bit HEC, but then the whole header including the HEC is encoded using 1/3 rate FEC. They are like inner code and outer code. If the receiver gets the packet corrupted, then the ARQ will ask for retransmission. These measures make Bluetooth very robust against errors.

2.2.5 Channel Control

There are two major states for Bluetooth units: Connection and Standby, and seven substates: **page**, **page scan**, **inquiry**, **inquiry scan**, **master response**, **slave response**, and **inquiry response**. These substates are interim states that are used to establish a new piconet or add new slaves to one existing piconet.

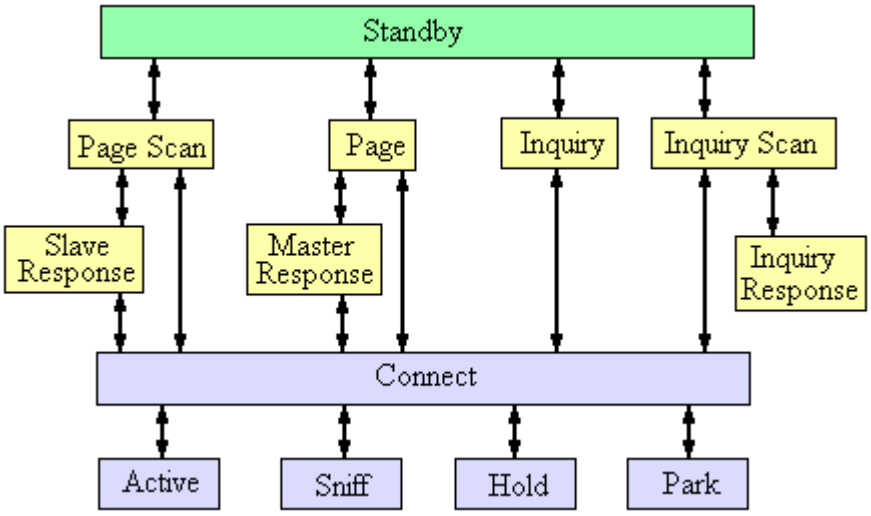

Figure 10. Link States

The default state for a Bluetooth unit is Standby. The unit in Standby state is in low power mode, and only wakes up to scan for paging or inquiring message for it. The period is under the control of LMP. In the Standby mode, the duty cycle of the Bluetooth unit is under 1%.

To establish a new connection, the slave must know the timing of the master and the master need to know the Bluetooth Device Address of the slave unit.

The connection setup procedure is like this: The unit (master) who wants to build a connection with other units enters the **inquiry** state to see if there are others nearby. If another unit happens to be in **inquiry scan** state and receives its inquiry message, it will respond to the master with information of its Bluetooth device address. The master unit then enters **page** state, and uses the slave's Bluetooth device address to construct a paging message. The slave in the **page** scan state will be able to receive this paging, and return a response. The master will send a FHS packet to help the slave to synchronize to the master clock. By now, a connection is established between the master and the slave.

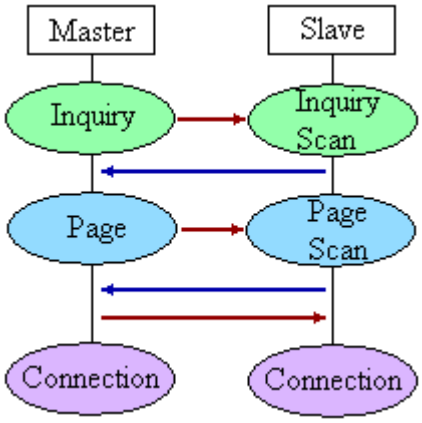

Figure 11. Connection Establishment Procedure

The unit in the connection state can be in **active** mode, **sniff** mode, **hold** mode or **park** mode.

In the **active** mode, the slave listens to the master-to-slave slot to see if the packet is addressed to it. If not, it will sleep until next master-to-slave slot. The master polls the slaves regularly.

In the **sniff** mode, the slave reduces its activity by listening only to slots of interval T_{sniff}, which is mutually agreed by both the slave and the master. **Sniff** mode has the highest duty cycle among 3 power saving modes.

In the **hold** mode, the slave sleeps for some preset period, and then restarts data transfers instantly. Also, the time of the **hold** mode is negotiated between the slave and the master.

In the **park** mode, the slave gives up its active-member-address and gets a new 8-bit parked-member-address. The parked slave has very little activity. It only listens to the beacon channel to synchronize and checks for broadcast messages. The unit in **park** mode has the lowest power consumption among all connected states.

One piconet has up to 256 parked members. By switching between **active** and **park** mode, a piconet can accommodate much more units than 8. Also, one unit can participate multiple piconets by putting itself into **park** mode in some piconets.

Bluetooth uses different hopping sequences for inquiring, paging and active channel. Both inquiring and paging use a 32 chip hopping sequence, which lasts 10 ms. It changes the phase of hopping every 1.28S. The unit in the inquiry scan or page scan mode will listen only to 1 frequency. Usually the connection establishment will take several seconds.

Operation Type	Minimum Time	Average Time	Maximum Time
Inquiry	0.00125s	5.12s	15.36s
Paging	0.0025s	0.64s	7.68s
Total (paging +inquiry)	0.00375s	5.78s	23.04s

Table 6. Time for connection setup

We can see the time to set up a connection may be as long as 20seconds. This is largely due to the low duty cycle of the idle unit. Once again here, the design has to compromise due to the low power requirement. In most cases, the 5.78s average connection time is satisfying.

Some new scheduling policies are being studied. One policy, using random wake-up interval instead of regular interval, is proposed in [17], it's declared to have shorter connection establishment time.

For better understanding of how a piconet is set up, let's look at one user scenario. A customer carrying a Bluetooth-enabled cellular phone went into Wal-Mart to buy something. When he enters the gate of Wal-Mart, one Bluetooth unit installed in the store may be constantly inquiring for other Bluetooth units nearby. When the customer's cellular phone responds to this inquiry with its Bluetooth device address (if the user enabled it to do so), a connection will be set up after following procedures for paging, paging scan, slave response and master response. Now, the customer's Bluetooth device address is stored in the Wal-Mart server's database. Then this connection might be terminated. When he approaches the clothes area, the Bluetooth server in that area probably will page him directly. After the connection setup, the user can get specific information about commodities in that area.

2.3 Upper layers

The RF and baseband of Bluetooth corresponds to the physical layer of OSI 7 layers model.

The LMP layer is responsible for link setup and detachment, authentication, encryption, power control and link configuration.

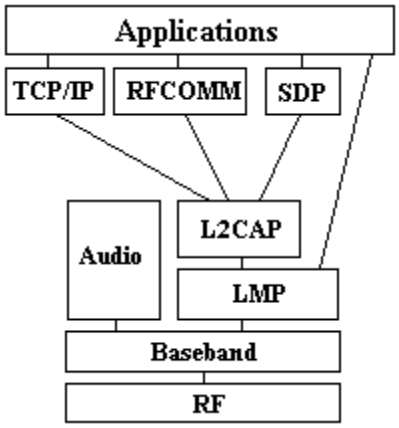

Figure 12. Protocol Layers

The Logical Link Control And Adaptation Layer Protocol (L2CAP) provides connection-oriented and connectionless data services to upper layer. Its duties include protocol multiplexing, segmentation and reassembly of upper layer PDUs of length up to 64KB, QoS support and Groups abstraction.

RFCOMM is a protocol used to emulate RS232 serial ports; this is useful since many existing applications are based on serial communications. Up to 60 simultaneous connections can exist between 2 Bluetooth devices. RFCOMM is based on a subset of TS07.10. It can transfer non-data circuit states and emulate a null modem.

The Service Discovery Protocol (SDP) enables mobile devices to find what services are available in proximity and the characteristics of the services. The SDP allows the client to search services with specific attributes (represented by a number UUID), or browse the services the server provides. The SDP only provides means for discovering the services, not for accessing those services.

It's possible to run TCP/IP over L2CAP directly, but currently, there are no profiles defined for them yet. So far, most vendors' TCP/IP implementations are based on PPP running on RFCOMM.

Due to the great popularity of TCP/IP, its performance over Bluetooth links is of much interest to many people.

Traditional IP is designed for stationary computers, and can't deal with the mobility demands of Bluetooth units. Issues like address resolution, bridging, multicast/broadcast mapping have to be solved. New protocols based on Mobil IP and Cellular IP are being studied [16].

Usually TCP interprets packets loss as the result of congestion of the network and cuts back its transmit window size. This is true for wired networks, where the major cause of packets loss is buffer overflow. But for wireless links, this algorithm is not as effective, since most packet loss are caused by interference. Some new scheduling algorithms are being studied [15].

3. Marketing and competition

3.1 Market projection

According to the statistics of In-Stat Group, Bluetooth-enabled equipment shipments will reach 955 million units in 2005. The Bluetooth semiconductor market will rise to $4.4 billion in 2005.

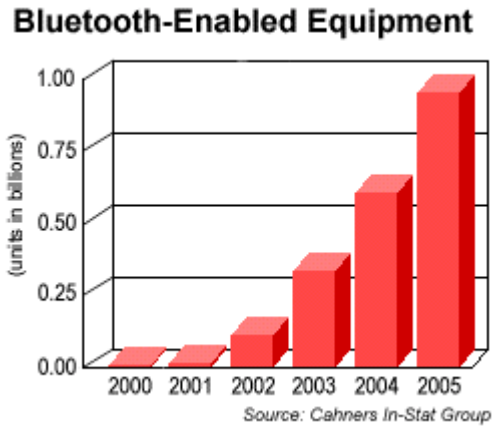

Figure 13. Market Projection

The potential markets include

- Digital mobile phones
- Digital cordless phones
- Wireless headsets
- Data access points (hot spots)
- Laptop, desktop and PDA
- Computer peripherals
- Digital cameras
- Home networking

Some “hot spots” have already appeared in some hotels, shopping malls, airports and much more are coming. It’s expected that there will be a big leap in the market next year.

Besides the market need, the vendors' support will also play an important role. Bluetooth have great support from manufacturers. Currently, Bluetooth SIG has about 2500 members, including almost all the key players in this market. It's estimated that in year 2000 over 60 million dollars was invested into Bluetooth R&D.

The expectation for Bluetooth is huge, but so far very few commercial products are available, and they cannot interoperate very well as they are expected to be. One of the major reasons is the qualification program is not complete, and no official test facilities are listed so far. The number of profiles, which define guidelines for different applications, is also very limited.

Bluetooth was promoted well before the technology was ready for commercial release to get enough support to become the industry standard. Now it falls short of the high expectation people have. After all, people still believe that Bluetooth will see a great market penetration by 2005.

3.2 Bluetooth vs. IrDA

The Infrared Data Association (IrDA) has 2 standards: IrDA-Data and IrDA-Control, the latter one is used for lower speed communications like wireless keyboard, joystick and etc. Here, we are only interested with the IrDA-Data.

IrDA is used for high-speed, short-range, line-of-sight and point-to-point data transfer. The range of IrDA is larger than 1 meter. It requires a narrow angle (30degree) point-and-shoot operation. The maximum data transfer speed is 4Mbps and 16Mbps is under development. It doesn't interfere with other wireless communications and also it's immune to interference from others.

IrDA gained great acceptance worldwide. Currently over 150 million units are installed worldwide and this number is growing 40% annually. Its major applications are laptop computers, printers and LAN access among others.

The biggest advantage of IrDA over Bluetooth is its high throughput, which makes it suitable for high-speed applications. The IrDA is also cheaper. One manufacturer can get a whole solution with cost of about $1.

Bluetooth provides users more mobility. For class 2 Bluetooth devices, its range can reach 10 meters, and it is omni-directional. It can effectively penetrate clothes and soft partitions. For examples, the user can leave his cellular phone in his pocket while using dial-up networking. This is impossible for IrDA.

Both of them have their advantages and disadvantages, and neither can fully replace the other. In Bluetooth specifications, IrOBEX is defined to enable applications to work on both RF and IR media.

	Bluetooth	IrDA
Technology	2.4GHz FHSS Point to point/multipoint	Infrared, PPM Point to point
Data Rate	1Mbps	4Mbps, 16Mbps underway
Range	100m(class 1)	1m, line of sight
Directionality	Omni-directional	30 degree
Cost	$5(long term)	$1
Global Standard	Most countries	Yes
Security	Very good	Good

Table 7. Bluetooth vs. IrDA

3.3 Bluetooth vs. WLAN (802.11)

As part of 802.x standard, the 802.11 standard covers the MAC and physical layer. It supports 3 kinds of physical media: DSSS at 2.4GHz, FHSS at 2.4 GHz and IR. Unlike Bluetooth's time-division scheme, 802.11 uses CSMA/CA to access the media. Current version 802.11b (also called Wi-Fi) provides up to 11Mbps throughput, 50m operating range. The future version will use 5.7GHz band and can achieve date rates of up to 40Mbps.

802.11b uses DSSS on three 22MHz channels. It uses QPSK and CCK (complementary code keying) to achieve high data rate. It uses 1.375Msps symbol rate and a chip rate of 8. The largest packet size is 1500 bytes.

Compared to Bluetooth, WLAN has higher implementation cost because its higher throughput need more powerful DSPs and also more power consumption. Currently, the cost of one WLAN card can be as high as $150.

802.11b uses DSSS technology, which is more sensitive to interference. There are reports that both Cisco and Lucent's WLAN product failed to work when you use a Panasonic 2.4GHz cordless phone nearby. So Bluetooth is more suitable for applications in noisy environments, like in a factory environment.

These two technologies are not only competing for market share, but also fighting physically in the same 2.4GHz ISM band. According to Intersil's test, the throughput of a 802.11 system could drop to 3.5Mbps in a Bluetooth dense environment [8]. Bluetooth seems performing better. According to Ericsson's test report, in a typical office environment with a large number of 802.11 terminals deployed, one Bluetooth unit

operating in 10m range is likely to possess a 24% probability of a 10% throughput reduction. But the Bluetooth throughput reduction will never be greater than 22% due to limited bandwidth overlapping [7]. So the effect of 802.11 on Bluetooth is much less severe than that of Bluetooth on 802.11.

A group of companies in the WLAN camp is petitioning the FCC to request Bluetooth to use adaptive hopping. The adaptive hopping will avoid the frequencies that are used by WLAN, thus a frequency division may be achieved. But there are still many issues to address for this approach [20].

	Bluetooth	**802.11b**
Technology	2.4GHz FHSS 79 1MHz channels TDMA	2.4GHz DSSS 3 22MHz channels CSMA/CA
Data Rate	1Mbps	11Mbps
Range	100m(class 1)	50m
Power	20mA(active)	200mA(active)
Cost	$5(long term)	$50
Robustness to interference	Good	Not so good

Table 8. Bluetooth vs. 802.11b

3.4 Bluetooth vs. HomeRF

The HomeRF is aimed at the home networking market. It provides up to 8 toll-quality (32ADPCM) voice channels, 8 prioritized streaming media sessions and data rate up to 10Mbps(20Mbps in 2002). This makes it very suitable for media-rich home environment. It could be used to connect audio and video sources, where Bluetooth is not capable.

Its MAC layer is optimized for combined data and voice traffic. It uses reserved slots (TDMA) for voice and CSMA/CA for data. Its physical layer uses 2.4GHz ISM band FHSS. Similar to Bluetooth, it has 75 1MHz channels, but it can combine five channels together to form a 5MHz SuperChannel for high-speed traffic. And also unlike Bluetooth's fixed hopping sequence, it can adapt its hoping sequence to the environment. This technique is very useful to reduce the interference from other static interferers like microwave oven.

HomeRF also provides very good security. It uses 32-bit IV (initialization vector) and 128-bit encryption. Bluetooth uses 8-128 bits variable size encryption, and 802.11b uses 64-bit encryption.

HomeRF is a very promising technology; it has gained support from over 100 companies including Compaq, Intel and Motorola.

HomeRF has many advantages over Bluetooth, but they do not come for free. The physical layer specification of HomeRF is largely adopted from 802.11 and modified to reduce cost. But its high throughput and complex MAC layer make it impossible to compete with Bluetooth on price. Currently, one can get a HomeRF adapter for about

$80. Also its power consumption is much larger than that of Bluetooth. So it's believed that Bluetooth will dominate the mobile applications like cellular phones and laptop computers.

	Bluetooth	**HomeRF**
Technology	2.4GHz FHSS 1MHz channels TDMA	2.4GHz FHSS 1MHz/5MHz channels TDMA, CSMA/CA
Data Rate	1Mbps	10Mbps(20Mbps in 2002)
Range	100m(class 1)	50m
Power	20mA(active)	350mA(transmit)
Cost	$5(long term)	$20
Robustness to interference	Good	Very good
Streaming media support	3 64kbps voice channels	8 stream sessions 8 32kbps ADPCM channels

Table 9. Bluetooth vs. HomeRF

4. Summary

Bluetooth is a low cost, low power RF technology for short-range communications. It could be used to replace cables connecting portable devices.

Compared to other similar wireless technologies, its biggest advantage is the low power and low cost, which makes it suitable for mobile applications. But its low data rate keeps it away from high-speed applications like real time video. A higher data rate version of Bluetooth is under discussion.

It shares the 2.4GHz ISM band with many other products. Interference among these units is an important topic for research.

There is huge market potential for Bluetooth products. The market will reach $1 billion around 2005. It has gained support from thousands of companies. There are a few commercial products available, and it's believed many more will roll out next year.

References

1. Bluetooth Specifications (V1.1) [http://www.bluetooth.com]
2. Bluetooth Profiles (V1.1) [http://www.bluetooth.com]
3. Infrared Data Association Serial Infrared Physical Layer Specification (V1.3)
4. HomeRF Overview, [HomeRF]
5. Digital Communications, *John G. Proakis*
6. Microwave and RF design for wireless systems, *David M. Pozar*
7. Bluetooth Voice and Data Performance in 802.11 DSSS WLAN Environment, *Jaap C. Haartsen,* [Bluetooth SIG]
8. Reliability of IEEE 802.11 Hi Rate DSSS WLANs in a High Density Bluetooth Environment, *Jim Zyren*, [Intersil 1999]
9. Interference Immunity of 2.4 GHz Wireless LANs, [HomeRF 2001]
10. A Comparison of Security in HomeRF versus IEEE802.11b, [HomeRF 2001]
11. Bluetooth—A New Low-Power Radio Interface Providing Short-Range Connectivity, *Jaap C. Haartsen,* [Proceedings of IEEE, Oct 2000]
12. BLUETOOTH—The universal radio interface for ad hoc, wireless connectivity, *Jaap C. Haartsen,* [Ericsson Review No. 3, 1998]
13. Hardware Architecture Overview, *Jaap C. Haartsen*, [Tokyo Conference 1999]
14. Reducing the component count in Bluetooth systems, [Cambridge Silicon Radio]
15. Enhancing Performance of Asynchronous Data Traffic over the Bluetooth Wireless Ad-hoc Network, *Abhishek Das*, [IEEE InfoComm 2001]

16. IP services over Bluetooth: leading the way to a new mobility, *Markus Albrecht*, [LCN 1999]
17. Proximity Awareness and Fast Connection Establishment in Bluetooth, *Theodoros Salonidis*, [MobiHOC 2000]
18. Low Power Considerations in the Design of Bluetooth, *Sven Mattisson*, [ISLPED 2000]
19. Handoff Support for mobility with IP over Bluetooth, *Simon Battz,* [LCN 2000]
20. Wi-Fi™ (802.11b) and Bluetooth™: An Examination of Coexistence Approaches, [Mobilian Corporation]
21. FHSS vs. DSSS in the Broadband Wireless Access and WLAN Arenas, *Sorin M. SCHWARTZ*, [http://www.breezecom.com]
22. IrDA and Bluetooth: A Complementary Comparison, *Dave Suvak*, [Extended Systems]
23. A. Kamerman, "Coexistence between Bluetooth and IEEE 802.11 CCK solutions to avoid mutual interference," *Lucent Technologies Bell Laboratories*, Jan 1999.
24. http://www.palowireless.com
25. http://www.anywhereyougo.com
26. http://www.ericsson.com/bluetooth
27. http://www.irda.org
28. http://www.homerf.org
29. http://www.sss-mag.com
30. http://www.baltzer.nl/wicom/