Bluetooth: Vision, Goals, and Architecture

Jaap Haartsen
Jaap.Haartsen@emn.ericsson.se
Ericsson
Enschede, The Netherlands

Mahmoud Naghshineh
mahmoud@us.ibm.com
IBM Watson Research Center
Hawthorne, NY, U.S.A.

Jon Inouye
Jon.W.Inouye@intel.com
Intel Corporation
Chandler, AZ, U.S.A.

Olaf J. Joeressen
Olaf.Joeressen@nmp.nokia.com
Nokia Mobile Phones
Bochum, Germany

Warren Allen
Warren.Allen@tais.toshiba.com
Toshiba Corporation
Irvine, CA, U.S.A.

A few years ago it was recognized that the vision of a truly low-cost, low-power radio-based cable replacement was feasible. Such a ubiquitous link would provide the basis for portable devices to communicate together in an ad hoc fashion by creating personal area networks *which have similar advantages to their office environment counterpart - the local area network (LAN). Bluetooth is an effort by a consortium of companies to design a royalty free technology specification enabling this vision. This article describes the vision and goals of the Bluetooth program and introduces the radio-based technology.*

I. Vision

In recent years, wireless connectivity has been an active area of research as we have witnessed a large number of government and industry initiatives, research efforts and standard activities that have aimed at enabling wireless and mobile networking technologies. As a result, today we have a diverse set of wireless access technologies from satellite networks, to wide area cellular systems, and from wireless local loop and PCS to wireless LANs. However, most of these solutions target narrow and specific application scenarios. With all such efforts spent on wireless link technologies, we still lack a universal framework that offers a way to access information based on a diverse set of devices (e.g., PDAs, mobile PCs, phones, pagers, etc.) in a seamless, user-friendly and efficient manner.

Formed in February 1998 by mobile telephony and computing leaders Ericsson, IBM, Intel, Nokia, and Toshiba, the Bluetooth special interest group (SIG) is designing a royalty-free, technology specification where each of the founding companies has a significant stake in enabling this vision. We believe that Bluetooth can revolutionize wireless connectivity for personal and business mobile devices, enabling seamless voice and data communication via short-range radio links and allowing users to connect a wide range of devices easily and quickly, without the need for cables, expanding communications capabilities for mobile computers, mobile phones and other mobile devices, both inside and outside of the office. Considering a wide range of computing and communication devices such as PDAs, notebook computers, pagers, and cellular phones with different capabilities, we envisage Bluetooth to provide a solution for access to information and personal communication by enabling a collaboration between devices in proximity of each other where every device provides its inherent function based on its user interface, form factor, cost and power constraints. Furthermore, the Bluetooth technology enables many new usage models for portable devices. For notebook computer manufacturers, the development of a short-range radio frequency (RF) solution enables the notebook computer to connect to different varieties of cellular phones and other notebook computers. For cellular handset manufacturers, the RF solution removes many of the wires required for audio and data exchange. Wireless hands-free kits operate even while the cellular phone is stored in a purse. As an example for a new usage model, we enable a connection from a mobile computer to the Internet using a cellular phone as a bridge. In some cases, even when the cellular phone is stored out of plain sight inside a briefcase, for example. In this scenario, the connection to the Internet is automatically established and auto-configured without requiring a conscious effort on the user's part to connect the mobile computer to the cellular phone and configure these two devices to communicate. We refer to this as a *hidden computing* or an *unconscious connectivity* model that is a powerful paradigm for new and exciting applications.

A very key characteristic of Bluetooth that differentiates it from other wireless technologies is that it enables combined usability models based on functions provided by different devices. Let us consider a connection between a PDA (computing device) and a cellular phone (communicating device) using Bluetooth and a second connection between the cellular phone and a cellular base station providing connectivity for both data and voice communication. In this model, the PDA maintains its function as a computing device and the phone maintains its role as a communication device - each one of these devices provide a specific function efficiently, yet their function is separate and each can be used independently of the other. However, when these devices are near each other they provide a useful combined function. We believe that this function and connectivity model based on a combination of wireless access technologies – each matched to different device capabilities and requirements – is a powerful paradigm that will enable ubiquitous and pervasive wireless communication. Many of these wireless link technologies are available today, however there is a need to provide a wireless connectivity, networking, and application framework to realize the total solution. This is exactly the charter of the Bluetooth SIG. In addition to combining the resources of a personal network, the RF link could also connect the personal network to the wired infrastructure. A data access point in an office, conference room, or airport kiosk would act as an information gateway for a notebook computer or cellular handset.

The remainder of this paper is organized as follows. Section II describes the goals the Bluetooth SIG hopes to achieve. Section III provides an overview of the Bluetooth architecture as it currently exists. Section IV compares the Bluetooth SIG to other industry initiatives involving wireless technology and Section V summarizes the article.

II. Goals

A. New Usage Models

The Bluetooth SIG is attempting to enable new usage models and create additional benefits for users of portable telephony and computer products. In addition to the examples presented in Section I, the SIG wants to enable the following future possibilities.

- *The Three-in-One Phone.* In this scenario, you are able to use the same phone wherever you are. When you're at the office, your phone functions as an intercom (no telephony charge). At home, it functions as a portable phone (fixed line charge). And when you're outdoors, the phone functions as a mobile phone (cellular charge).

- *The Briefcase Trick.* Use e-mail while your notebook is still in the briefcase. When your notebook receives an e-mail, you'll get an alert on your mobile phone. You can also browse all incoming e-mails and read those you select in the mobile phone's window.

- *The Automatic Synchronizer.* Automatic background synchronization keeps you up-to-date. Automatic synchronization of data on your desktop, notebook, personal digital assistant(PDA), and mobile phone. For instance, as soon as you enter your office the address list and calendar in your notebook will automatically be updated to agree with the one in your desktop, or vice versa. Collect a business card on your phone and add it to your address list on your notebook PC.

B. System Challenges

The usage models described above require various system requirements to be met. In this section, we review several requirements and the challenges they offer.

Support for both voice and data. The air protocol must support good quality real-time voice, where "good" is considered to be wired phone line quality. Voice quality is important to both end-users who are accustomed to it, and for speech recognition engines whose accuracy depends on it.

Able to establish ad hoc connections. The dynamic nature of mobility makes it difficult to make any assumptions about the operating environment. Bluetooth units must be able to detect other compatible units and establish connections to them. A single unit must be able to establish multiple connections in addition to accepting new connections while connected. Ignoring a new connection requests while connected is confusing to the user and deemed unacceptable, especially if we want to support unconscious computing while retaining the ability to perform interactive operations!

Able to withstand interference from other sources in an unlicenced band. The Bluetooth radio operates in the unlicensed 2.4 GHz band where many other RF radiators are expected to exist. The fact that microwave ovens operating at this frequency is one reason why this band is unlicensed in most countries. The challenge is to avoid significant degradation in performance when other RF radiators, including other personal area networks in nearby use, are in operation.

Worldwide use. Not only are "standard" cables equipped with a variety of connectors, different standards exists in different geographical locations throughout the world. Experienced mobile travelers are accustomed to carrying around a number of different power, phone, and network connectors. The challenge here is very regulatory in nature with many governments having their own set of restrictions on RF technology. And while the 2.4 GHz band is unlicensed through most parts of the world, it varies in range and offset in a number of different countries.

Similar amount of protection compared to a cable. In addition to the radio's short-range nature and spread spectrum techniques, Bluetooth link protocols also provide authentication and privacy mechanisms. Users certainly don't want others listening in on their conversations, snooping their data transmissions, or using their cellular phones for Internet access.

Small size to accommodate integration into a variety of devices. The Bluetooth radio module must be small enough to permit integration into portable devices. Wearable devices in particular, such as mobile phones, headsets, and smart badges have little space to spare for a radio module.

Negligible power consumption compared with the device in which the radio is used. Many Bluetooth devices will be battery powered. This requirement implies the integration of the Bluetooth radio should not significantly compromise the battery lifetime of the device.

Encourage ubiquitous deployment of the technology. To achieve this goal, the SIG is designing an open specification defining the radio, physical, link, and higher level protocols and services necessary to support the usage models in the vision. The Specification will be made available under favorable adoption terms, including royalty free, to SIG members.

C. The Specification

The Bluetooth Specification defines the requirements ensuring interoperable operation between Bluetooth devices from different manufacturers. The Bluetooth Specification is work-in-progress and any material presented here is preliminary and

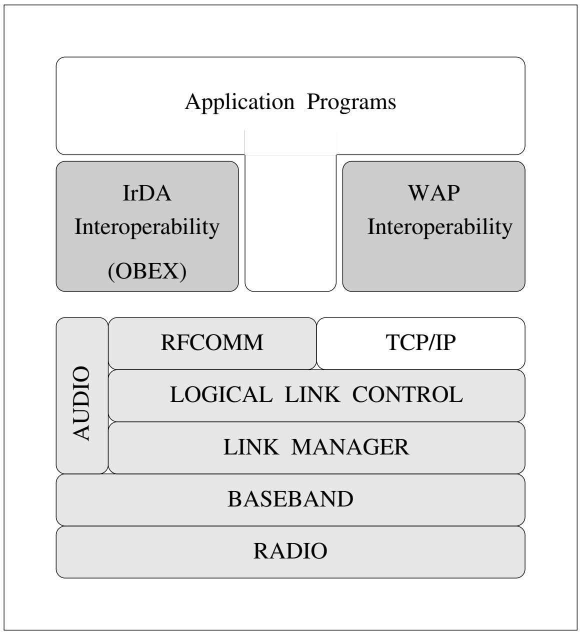

Figure 1: Application Framework

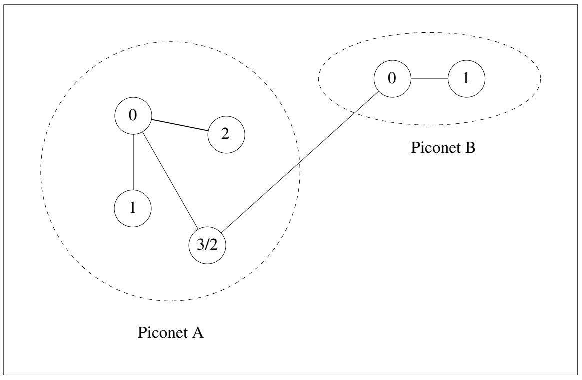

Figure 2: Scatternet Example

subject to change without notice.[1] The Specification draft is composed of two sets of documents: the radio and protocol definitions, and the compliance requirements.

Figure 1 outlines the application framework in the context of the radio and protocol stack. The Radio takes care of sending and receiving modulated bitstreams. The Baseband (BB) protocol defines the timing, framing, packets, and flow control on the link. The Link Manager (LM) assumes the responsibility of managing connection states, enforcing fairness among slaves, power management, and other management tasks. The Logical Link Control handles multiplexing of higher level protocols, segmentation and reassembly of large packets, and device discovery. Audio data is mapped directly on to the Baseband while audio control is layered above the logical link control. Above the data link layer, RFCOMM and network level protocols provide different communication abstractions. RFCOMM provides serial cable emulation using a subset of the ETSI GSM 07.10 standard [2]. Other parts of the Bluetooth Specification deal with interoperability with other protocols and protocol stacks. Defining TCP/IP over Bluetooth requires that bridging, address resolution, MTU definition, and multicast/broadcast mappings be solved. To accelerate the number of wireless-specific applications, the Bluetooth SIG is contemplating interoperability with higher layer IrDA[2] and WAP[3] protocol stacks.[4] For example, IrOBEX [4] defines a transport-independent format and session protocol for object exchange and is used as the basis for a variety of applications from exchanging files and business cards to synchronizing address book and calendar schedules.

The compliance requirements section of the Specification defines the radio and protocol features that are required for different classes of devices. Due to the wide variety of possible Bluetooth devices, different sets of requirements are needed. For example, one would not expect an audio headset to have the same minimum requirements as a notebook computer. The goal of the Specification's compliance section is ensuring that any device wearing a Bluetooth "logo" supports a minimum set of benefits for its user.

III. The Bluetooth Architecture

Bluetooth has been specified and designed with emphasis on robustness and low cost. Its implementation is based on a high-performance, yet low cost, integrated radio transceiver. Bluetooth is targeted at mobile and business users who need to establish a link, or small network, between their computer, cellular phone and other peripherals. The required and nominal range of Bluetooth radio is thus set to 10 meters (with 0 dBm output power). To support other uses, for example the home environment, the Bluetooth chipset can be augmented with an external power amplifier to extend the range (up to 100m with +20dBm output power). Auxiliary baseband hardware to support, for example, four or more voice channels can also be added. These additions to the base chip set are fully compatible with the nominal specification and may be added depending on the application.

Bluetooth operates in the international 2.4 GHz ISM band, at a gross data rate of 1 Mbit/second, and features low energy consumption for use in battery operated devices. Bluetooth uses an ad hoc, *piconet* structure hereafter referred to as *scatternet*. Figure 2 illustrates an example scatternet, with one unit participating in both piconets. With the scatternet technology described later in this document, it has been possible to achieve an aggregate throughput of over 10 Mbits/second or 20 voice channels within a fully expanded scatternet. The structure also makes it possible to extend the radio range by simply adding additional Bluetooth units acting as bridges at strategic places.

A single unit can support a maximum data transfer rate of 721 kbits/second or a maximum of 3 voice channels. A mixture of voice and data transfer is also possible in order to support multimedia applications. A robust voice coding scheme with a rate of 64kbits/second per voice channel is used. To sustain these transfer rates in busy radio environment, a packet switching protocol with frequency hopping and advanced cod-

[1] The Bluetooth SIG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this article. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

[2] Infrared Data Association. See http://www.irda.org.

[3] Wireless Application Protocol Forum. See http://www.wapforum.org.

[4] Third party brands and names are the property of their respective owners.

ing techniques are employed. It should also be mentioned that the Bluetooth features a graceful degradation of both voice and data transfer rates in busy RF environments.

A. Master/Slave definitions

In the Bluetooth network all units are peer units with identical hardware and software interfaces distinguished by a unique 48-bit address. At the start of a connection, the initializing unit is temporarily assigned as a master. This assignment is valid only during this connection. It is the master which initiates the connection and controls the traffic on the connection. Slaves are assigned a temporary 3-bit member address to reduce the number of addressing bits required for active communication.

B. Network topology

The Bluetooth network supports both point-to-point and point-to-multipoint connections. A piconet is the network formed by a master and one or more slaves. Each piconet is defined by a different frequency hopping channel. All units participating in the same piconet are synchronized to this channel.

C. Robust Air Protocol and Adaptive Range

To achieve the highest possible robustness for noisy radio environments, Bluetooth uses a packet-switching protocol based on a frequency hop scheme with 1600 hops per second. The entire available frequency spectrum is used with 79 hops of 1 MHz bandwidth, defined analogous to the IEEE 802.11 standard [3]. This frequency hopping gives a reasonable bandwidth and the best interference immunity by utilizing the entire available spectrum of the open 2.4 GHz Industrial, Scientific, and Medical (ISM) band. Virtual channels are defined using pseudo-random hop sequences.

The frequency hopping scheme is combined with fast Automatic Repeat Request (ARQ), cyclic redundancy checks (CRC), and Forward Error Correction (FEC) for data. For voice a continuous variable slope delta modulation (CVSD) scheme is used. All of this results in a very robust link for both data and voice.

To save power and minimize radio interference problems, a RSSI (Received Signals Strength Indicator) with a 72 dB dynamic range will be employed. The RSSI will measure the signal received from different units and adapt the RF output power to the exact requirement in each instance. That is, with a mouse or headset, the output power could be limited to a 1 m range, whereas a handset may need a range of 100 m or more.

D. Establishing network connections

When first establishing a network or adding components to a piconet, the units must be identified. Units can be dynamically connected and disconnected from the piconet at any time. Two available options lead to connection times of typically 0.64 and 1.28 seconds respectively. This applies when the unit address is known and not more than about 5 hours have elapsed since the previous connection. A unit does not need to be connected at all times since only a typical delay of under one second is required to start a transaction. Hence, when not in use, the unit can be in a sleep state (STANDBY) most of the time where only a Low Power Oscillator (LPO) is running. This is, of course, beneficial for battery operation.

Before any connections are made, all units are in standby mode. In this mode, an unconnected unit will only listen to messages every 1.28 seconds or 2.56 seconds depending on the selected option. Each time a unit wakes up, it will listen on one of 32 hop frequencies defined for this unit.

The connect procedure is initiated by one of the units, the master. A connection is made either by a PAGE message if the address is already known, or by the INQUIRY message followed by a subsequent PAGE message if the address is unknown. In the initial PAGE state, the paging unit (which is the master) will send a train of 16 identical page messages on 16 different hop frequencies defined for the unit to be paged (the slave). The train covers half the sequence of frequencies in which the slave can wake up. It is repeated 128 or 256 times (1.28 or 2.56 seconds) depending on the needs of the paged unit. If no response is received after this time, the master transmits a train of 16 identical page messages on the remaining 16 hop frequencies in the wake-up sequence. The maximum delay before the master reaches the slave is 2 times 1.28 seconds or 2.56 seconds if a periodicity of 1.28 seconds was chosen for paging and 5.12 seconds with 2.56 seconds periodicity respectively. This allows devices to trade off between access delay and standby power savings.

The hop frequencies in the first page train are based on the master's slave clock estimate. The train will include the estimated wake-up hop, and 8 hops before and 7 hops after this hop. As a result, the estimate can be $\pm$ 7 hops in error and still the master reaches the slave with the first page train. Because the estimate is updated at each connection establishment, the acquisition delay is shorter when a shorter time has elapsed since the units were last connected. With a Low Power Oscillator (LPO) inaccuracy better than $\pm$ 250 ppm, the first train is still valid after at least 5-hours lapse with no connection.

That is, for a time period of at least 5 hours since the last connection, the average acquisition times are 0.64 seconds and 1.28 seconds respectively. If the first train does not cover the slave's wakeup frequency, the second train does and the average acquisition delays are 1.92 seconds and 3.84 seconds.

The INQUIRY message is typically used for finding public printers, faxes and similar equipment 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.

If no data needs to be transmitted, the units may be put on HOLD where only an internal timer is running. When units go out of HOLD mode data transfer can be restarted instantaneously. Units may thus remain connected, without data transfer, in a low power mode. The HOLD is typically used when connecting several piconets. It could also be used for units where data needs to be sent very infrequently and low power consumption is important. A typical application would be a room thermostat which may need to transfer data only once every minute.

Two more low power modes are available, the SNIFF mode and the PARK mode. If we list the modes in increasing order of power efficiency, then the SNIFF mode has the higher duty cycle, followed by the HOLD mode with a lower duty cycle, and finishing with the PARK mode with the lowest duty cycle.

Figure 3 describes the various possible connection states.

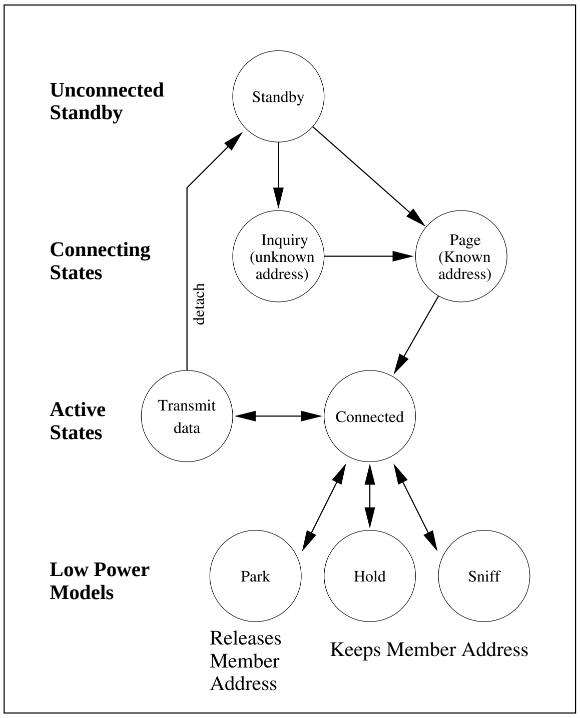

Figure 3: Connection State Machine

E. Link types

Once a Bluetooth unit has been connected to a piconet it may communicate by means of two link types. That is, between any two members of the piconet forming a master-slave pair. Two link types are supported. These links are:

- Synchronous Connection Oriented (SCO) link
- Asynchronous (or isochronous) Connectionless (ACL) link.

Different link types may apply between different master-slave pairs of the same piconet and the link type may change arbitrarily during a session. The link type defines what type of packets can be used on a particular link. On each link type, 16 different packet types can be used. The packets differ in function and data bearing capabilities. For full duplex transmissions a Time Division Duplex scheme is used. Each packet is transmitted in a different hop channel than the previous packet.

An SCO link is a point-to-point full-duplex link between the master and a slave. This link is established once by the master and kept alive until being released by the master. The SCO link is typically used for a voice connection. The master reserves the slots used for the SCO link on the channel.

The ACL link makes a momentary connection between the master and any of the slaves for the duration of one frame (master-to-slave slot and slave-to-master slot). No slots are reserved. The master can freely decide which slave to address and in which order. The member subaddress in the packet header determines the slave. A polling scheme is used to control the traffic from the slaves to the master. The link is intended for asynchronous or isochronous data. However, if the master uses this link to address the same slave at regular intervals, it becomes a synchronous link. The ACL link supports both symmetric and asymmetric modes. In addition, modes have been defined with or without FEC, and with or without CRC and ARQ.

F. Packet Definition

A packet (see Figure 4 consists of three fields: a 72-bit access code, a 54-bit header, and a payload of variable length (2-342 bytes). Packets may consist of the (shortened) access code only, the access code and the header, or the access code, header and payload.

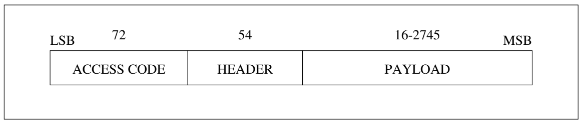

Figure 4: Typical packet format

The packet starts with a 72-bit channel access code. This access code is used for synchronization, DC offset compensation and identification. The access code identifies all packets exchanged on the channel of the piconet: all packets sent in the same piconet are preceded by the same channel access code. In the receiver of the Bluetooth unit, a sliding correlator correlates against the access code and triggers when a threshold is exceeded. This trigger signal is used to wake up the entire signal processing of the receiver. In addition, it is used to fix the receive timing. The correlator remains active during the entire search window: when a new correlation value is found which is larger than a previous correlation value which initially triggered the receiver, the entire receiver is reset and triggered again. The channel access code consists of a preamble, a sync word, and a trailer, see Figure 5. Both preamble and trailer are fixed bit patterns.

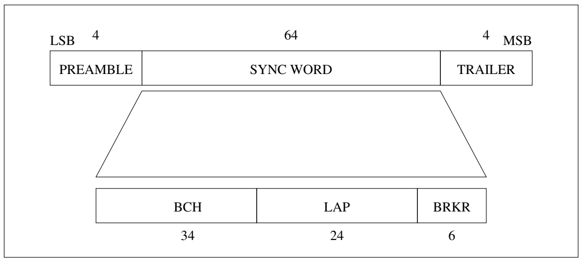

Figure 5: Channel Access Code

The preamble is a fixed zero-one pattern of 4 symbols used to facilitate DC compensation. The sequence is either 1010 or 0101, depending on whether the LSB of the following access code is 1 or 0 respectively. The sync word is a 64-bit code and is derived from the master's lower address part (LAP) of its 48-bit unique address. The code guarantees large Hamming distance between sync words based on different addresses. In addition, it has good auto- and cross-correlation properties which improves the timing synchronization process. Like the preamble, the trailer is a fixed zero-one pattern of four symbols used for fine compensation. The sequence is either 1010 or 0101 depending on whether the MSB of the sync word is 0 or 1 respectively.

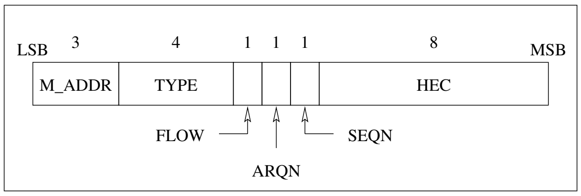

Figure 6: Header format

The header, shown in Figure 6, contains lower-level link control information. It consist of 6 fields: a 3-bit sub address (M_ADDR), a 4-bit packet type (TYPE), a 1-bit flow control bit (FLOW), a 1-bit acknowledge indication (ARQN), a 1-bit sequence number (SEQN), and an 8-bit header error check (HEC). The total header information consists of 18 bits, but is protected with a 1/3 forward-error correction coding resulting in a 54-bit header length.

M_ADDR: This field represents a member address used to distinguish the active participants on the piconet. With the M_ADDR, the master can separate the different slave active on the piconet. This M_ADDR is assigned temporarily to a unit for the time it is active on the channel. Packets exchanged between the master and the active slave all carry the M_ADDR of this slave. The all-zero address is reserved for broadcasting purposes. Slaves in the PARK mode are inactive but are still locked to the FH channel. The parked slaves do not use an M_ADDR but their full 48-bit unique address.

TYPE: Sixteen different types of packets can be distinguished. The 4-bit TYPE code specifies which packet type is used. Important to note is that the interpretation of the TYPE code depends on the physical link type associated with the packet. First, it shall be determined whether the packet is a SCO or an ACL packet. Then, it shall be determined which of the SCO packet types or ACL packet types we are dealing with. The TYPE code also reveals how many slots the current packet will occupy. This allows the non-addressed receivers to go to sleep for the duration of the occupied slots.

FLOW: This bit is used for flow control over the ACL link. When the RX buffer for the ACL connection in the recipient is full and is not emptied by the link support unit, a STOP indication (FLOW=0) is returned to stop the transmission of data temporarily. Note, that the STOP signal only concerns ACL packets. Packets including only link control (POLL and NULL packets) or SCO packets can still be received. When the receive buffer is empty, a GO indication (FLOW=1) is returned. When no packet is received or the received header is in error, a GO is assumed implicitly.

ARQN: This is an acknowledge field to inform the sender whether the reception of the packet in the preceding slot was successful (ARQN=1) or unsuccessful (ARQN=0). When no valid ARQN field is received, ARQN=0 is assumed implicitly. ARQN=0 is the default value. The ARQN is piggy-backed in the return packet. The success of the reception is checked by means of a cyclic redundancy check (CRC) which is added to each payload that contains data. An unnumbered ARQ scheme is used which means that the ARQN relates to the packet just received.

SEQN: This is a numbering field to distinguish new packets from retransmitted packets. The SEQN bit is toggled for each new packet transmission. A retransmitted packet keeps the same SEQN bit. If two consecutive packets are received with the same SEQN bit, the second packet is ignored.

HEC: Each header has a header-error-check to check the header integrity. The HEC consist of an 8-bit word generated by the polynomial 647 (octal representation). Before generating the HEC, the HEC generator is initialized with the 8-bit upper address part (UAP) of the master identity. The HEC is then calculated over the 10 header bits. Before checking the HEC, the receiver must initialize the HEC check circuitry with the proper 8-bit UAP. If the HEC fails, the entire packet is discarded.

G. Packet types

The 4-bit TYPE code in the packet header specifies 16 different packet types. The packet types have been divided into 4 segments. The first segment consists of 4 packets and is reserved for control packets common to all physical link types. The second segment consists of 6 packets and is reserved for packets occupying a single time slot. The third segment consists of 4 packets and is reserved for packets occupying three time slots. The fourth segment consists of 2 packets and is reserved for packets occupying five time slots. The slot occupancy is reflected in the segmentation and can directly be derived from the type code. Table 1 summarizes the packets defined for the SCO and ACL link types.

At this moment, four different SCO packets have been defined. So far, only single-slot packets have been defined. SCO packets are typically used for synchronous information like voice. The packets differ in the amount of FEC coding applied and whether part of the packet is reserved for data as well as voice. For the ACL link, 6 different packet types have been defined. They differ in the in the amount of data carried, in the presence of absence of FEC coding, and whether ARQ is applied or not.

H. Error correction

There are three error-correction schemes defined for Bluetooth: 1/3 rate FEC, 2/3 rate FEC, and an ARQ scheme for data. The purpose of the FEC scheme on the data payload is to reduce the number of retransmissions. However, in a reasonable error-free environment, FEC gives unnecessary overhead that reduces the throughput. Therefore, the packet definitions given in Section G have been kept flexible to use FEC in the payload or not, resulting in the DM and DH packets for the ACL link and the HV packets for the SCO link. The packet header is always protected by a 1/3 rate FEC; it contains valuable link information and should survive more bit errors.

Table 1: Packets defined for SCO and ACL link types

Segment	TYPE	SCO link	ACL link
Control Packets	0000	NULL	NULL
	0001	POLL	POLL
	0010	FHS	FHS
	0011	DM1	DM1
Single Slot Packets	0100		DH1
	0101	HV1	
	0110	HV2	
	0111	HV3	
	1000	DV	
	1001		AUX1
3-Slot Packets	1010		DM3
	1011		DH3
	1100		
	1101		
5-Slot Packets	1110		DM5
	1111		DH5

I. Speech coding

In the Bluetooth system, two speech coding schemes are supported, Continuous Variable Slope Delta (CVSD) Modulation, and logarithmic Pulse Coded Modulation (logPCM), both operating at 64 kbits/second. The default speech coder is the more robust CVSD coder.

The CVSD coder is a waveform coder applying a delta modulation scheme[5]. To reduce slope-overload effects, syllabic companding is applied: the delta step size is adapted according to the average signal slope. The interface to the CVSD speech coder is 8000 samples/second linear PCM. The CVSD degrades gracefully in a noisy environment. Increasing interference is experienced as a growing background noise.

The alternative speech coding is basic logPCM. The 16-bit linear PCM at 8000 samples/second is compressed to 8-bit logPCM at 8000 samples/second using A-law or μ-law compression.

J. Authentication and Privacy

In order to provide user protection and information secrecy, the system has to provide security measures both at the application layer and the physical layer. These measures shall be appropriate for a peer environment. This means that in each Bluetooth unit, the authentication and encryption is implemented in the same way. Bluetooth specifies a base level encryption, which is well suited for silicon implementation, and an authentication algorithm, which also provides devices which don't necessarily have host processing capabilities a level of security. In addition, future ciphering algorithms can be supported in a backwards compatible way using version negotiation.

The main features are:

- Challenge-response routine for authentication
- Session key generation. Session keys can be changed at any time during a connection
- Stream-cipher

Table 2: Protection Entities

Entity	Size
Bluetooth address	48 bits
private user key	64 bits
RAND	128 bites

In general security problems, three entities are used: a public entity which is unique for each user, a secret entity, and a random entity which is different for each new transaction. The three entities and their sizes as used in Bluetooth are summarized in Table 2.

The Bluetooth address is 48-bits in length and unique for each Bluetooth unit. Bluetooth addresses are publicly known, and can either be obtained via Man-Machine interactions (MMI), or automatically via an inquiry routine. The user key is a 64-bit secret key which is derived during initialization but is further never disclosed. The RAND is a random number which will be derived from a pseudo-random process in the Bluetooth unit.

IV. Other Wireless Initiatives

This section describes the history and focus of several other wireless industry groups and compares their vision and goals to those of the Bluetooth SIG.

A. IrDA (http://www.irda.org/)

The Infrared Data Association (IrDA) is a non-profit corporation established in 1993 to set and support hardware and software standards for infrared communication links. The IrDA protocol stack is designed to support usage models similar to those of Bluetooth. Legacy serial-cable-oriented applications are supported via cable emulation while new IR-specific APIs support the development of applications able to take advantage of the full capabilities of the IR link management and transport protocols. There are already IrDA-compliant interfaces on many printers, handheld computers, notebook computers, and digital still image cameras. The advantages of IR over RF include reduced cost, lower standby power, higher bandwidth, and less regulations governing global use. The most significant disadvantage of IR is the line-of-sight restriction that constrains Bluetooth's vision of hidden and unconscious computing.

The Bluetooth SIG believes in promoting the development of applications that work over either IR or RF. The application developer, and especially the user, should not care what physical medium is used. To achieve this, the Bluetooth SIG is working on interfacing with the higher-level IrDA protocols and has approached the IrDA to achieve interoperability across both wireless media.

B. IEEE 802.11 (http://www.ieee.org/)

The IEEE 802.11 standard defines RF and IR physical layers, Media Access Control (MAC) layer for LAN connectivity and additional access point and security protocols. Generally speaking, IEEE 802.11 defines a larger set of physical layers consisting of two radio solutions (frequency hopping and direct sequence) and an IR solution while Bluetooth uses a fast frequency hopping radio solution. Regarding the MAC layer, Bluetooth uses a connection-oriented TDMA scheme while IEEE 802.11 uses a carrier sense multiple access with collision avoidance (CSMA/CA) scheme. The goal of IEEE 802.11 is enabling LAN based applications with a larger radio coverage while Bluetooth's paradigm is enabling wireless connectivity between diverse types of devices including an access point to a wired LAN in a piconet environment. Finally, IEEE 802.11 has been recently considering a short range solution similar to the Bluetooth under its PAN working group.

C. HomeRF (http://www.homerf.org/)

The HomeRF[5] Working Group (HRFWG) is developing an open specification targeting the home environment [6]. HomeRF focuses on both stand-alone and wireless extensions to home networking technologies. In its current draft, the HomeRF specification defines an air protocol based on a combination of CSMA/CA for data and cordless telephony [1] technology for voice. On the voice side, HomeRF uses an ADPCM coding at 32 Kbps compared to Bluetooth's more robust CVSD coding at 64 Kbps. However, HomeRF does have the ability to retransmit a voice packet while Bluetooth never retransmits voice. Another distinguishing factor is all HomeRF voice traffic is channeled through a "control point" while Bluetooth's voice traffic, like the data traffic, uses ad hoc connections between any two Bluetooth units. On the data side, Bluetooth views HomeRF as a relaxed version of IEEE 802.11.

V. Summary

By developing the Specification for a low-cost, low-power radio-based cable replacement, the Bluetooth SIG hopes to drive an evolution in personal networking. In this article, we have shared some of the vision, challenges, and architecture the SIG is contemplating. For more information, readers are encouraged to explore http://www.bluetooth.com.

By the time of this publication, the first release of the Bluetooth Specification (0.6) will be available to SIG members for review and comments. The release of the Bluetooth Specification 1.0 is planned for the first quarter in 1999 and products compliant to that Specification are expected in late 1999.

Acknowledgements

The authors would like to thank all the people within the SIG who have, and continue to, contribute valuable ideas, solutions, and effort to move the Specification towards completion. The authors would also like to thank Victor Bahl and SIGMOBILE for the invitation to share the program with the research community, and the Bluetooth SIG program management for permitting the publication of this article at this stage of the Specification . The name Bluetooth is inspired by the Danish Viking King Harald Bluetooth (910-986), son of "Gorm the Old" and father of "Sven Forkbeard". The codename is credited to Jim Kardach (Intel) and the authors refer all name-related inquiries to Jim for explanation.

[5] Third party brands and names are the property of their respective owners.

References

[1] ETSI. Digital European Cordless Telephon Common Air Interface, 1991.

[2] ETSI. Terminal Equipment to Mobile Station (TE-MS) multiplexer protocol (GSM 07.10 version 6.1.0), July 1998. TS 101 369.

[3] IEEE. Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 1997.

[4] IRDA. IrDA Object Exchange Protocol (IrOBEX), January 1997.

[5] JAYANT, N., AND NOLL, P. *Digital Coding of Waveforms*. Prentice-Hall, 1984.

[6] NEGUS, K., ET AL., HomeRF and SWAP: Wireless Networking for the Connected Home. *ACM Mobile Computing and Communications Review 2*, 4 (October 1998).

Biographies

Jaap Haartsen received his M.S.E.E and Ph.D in 1986 and 1990, respectively, from the Delft University of Technology, The Netherlands. In the past eight years, he worked in the research departments of Ericsson in the US and in Sweden in the area of wireless technology. Currently, he is located in The Netherlands and chairs the Bluetooth SIG Air Protocol working group.

Mahmoud Naghshineh is with the IBM Thomas J. Watson Research Center, Yorktown Heights, New York, where he currently manages the communication systems group. He has been working at IBM since 1988 on a variety of research and development projects dealing with design and analysis of communication protocols, and fast packet-switched/broadband networks, wireless and mobile ATM, wireless radio and infrared access broadband and local area networks. He received his doctoral degree from Columbia University, New York.

Jon Inouye in an engineering manager in Intel's Mobile Communications Operations, part of the Mobile and Handheld Products Group (MHPG), where his responsibilities include chairing the Bluetooth SIG software working group.

Olaf J. Joeressen received the Dipl.-Ing. degree from Aachen University of Technology (RWTH) in 1990. He received the Dr.-Ing. degree from the RWTH in 1995 for work on the VLSI implementation of Soft-Output Viterbi-Decoders. After that he joined Nokia R&D in Bochum, Germany where he is now responsible for the Bluetooth core technology development.

Warren Allen is a Senior Product Planner at Toshiba America Information Systems, Inc. of Irvine, CA, where he has been employed since 1989. He currently has responsibility for discovering and integrating communications technologies into Toshiba's product lines of portable, desktop and server computers.