Bluetooth technology: Overview of the Vision, Goals, and Architecture

Shijan Handa, Vaibhav Kharbanda, Rahul Phogat
Electronics & Communication Engineering
Dronacharya college of Engineering, Gurgaon

***Abstract*-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.**

***Index Terms*- Bluetooth, architecture, packet format, authentication.**

I. INTRODUCTION

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. 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. 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.

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 email, 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 withstand interference from other sources in an unlicensed 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.

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 subject to change without notice.

The Specification draft is composed of two sets of documents: the radio and protocol definitions, and the compliance requirements.

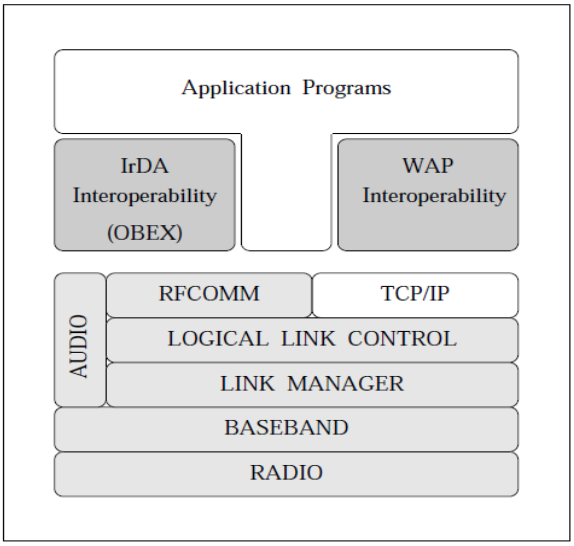

Figure 1: Application Framework

Figure 1 outlines the application framework in the context of the radio and protocol stack. The Radio takes care of sending and receiving modulated bit streams. 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.

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 a 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 coding 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 distinguishedby 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. 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 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.

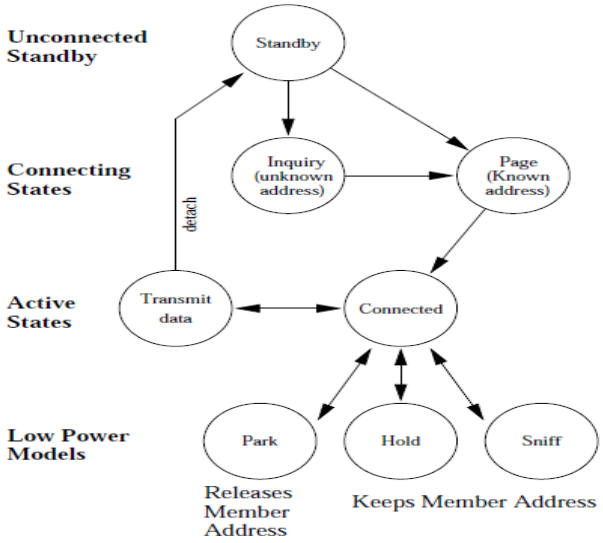

Figure 3 describes the various possible connection states.

D. 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.

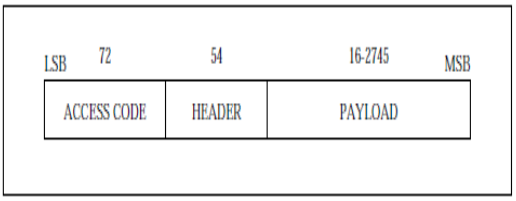

FIG.4 Typical packet format

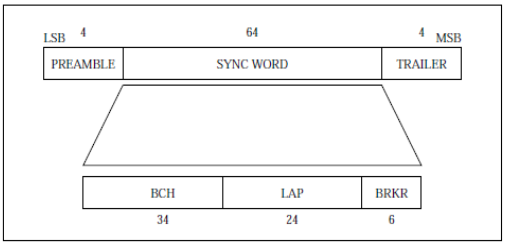

FIG.5 Channel Access Code

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. The preamble is a fixed zero-one pattern of 4 symbols used to facilitate DC compensation. The sequence is either 1010 o 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.

E. Packet types

The 4-bitTYPE 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.

F. 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 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.

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

Table 2: Protection Entities

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

TABLE 1: Packets defined for SCO and ACL link types

G. 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

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. 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.

REFERENCES

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

[2] ETSI. Terminal Equipment to Mobile Station (TEMS) multiplexer protocol.

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

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

[5] JAYANT, N., AND NOLL, P. *Digital Coding of Waveforms*.