Bluetooth Specification In Wireless Environment

Alok Goel*, Dilip Kumar* and Shomil Bansal*
* MIT, Bulandshahr, U.P., India

'Bluetooth' is a technique of Wireless Personal area network (WPAN) specially designed to support portable, mobile computing devices and a variety of consumer electronic equipment. The Bluetooth operates in the 2.4 GHz industrial, scientific and medical (ISM) radio band. Bluetooth radio characteristics include low power, short range and medium transmission speed. Bluetooth chips are already available and early applications include cordless connections from mobile phones to laptop computers and wireless headsets. Since May 1998 the Bluetooth Special Interest Group (SIG) has steered the development of the technology through the development of an open industry specification, including both protocols and application scenarios, and a qualification program designed to assure end-user value for Bluetooth products. This paper introduces the Bluetooth wireless technology and its applications and provides a concise description of its air interface, architecture, protocol stack and security.

Keywords: Pico net, Scatternet, Ad hoc networking, Security.

1. INTRODUCTION

There are three possibilities for providing various interconnections: wires, infra-red links, and wireless links. It is the goal of the Bluetooth wireless technology to achieve 'freedom from wires' by using radio links for these connections. The Bluetooth™* wireless technology is a cable replacement technology that exploits the wireless interconnectivity that is possible with radio. Bluetooth is a technique & standard of Wireless Personal Area Network (WPAN [1]) specially designed to support portable, mobile computing devices such as laptops, notebooks etc. and a variety of consumer electronic equipment.
* The 'Bluetooth' trademarks are owned by Bluetooth Special Interest Group (SIG) [2], Inc., USA.

The Bluetooth wireless technology has been developed by an industry-based association, the Bluetooth Special Interest Group (SIG). Initially the Group comprised five companies-IUM, Intel, Ericsson, Nokia and Toshiba but by the end of 1999 this number had increased to nine through the addition of 3Com, Motorola, Microsoft and Lucent. By December 2000 the Bluetooth SIG had over 2000 members.

The Bluetooth standard is an open standard published by the Bluetooth SIG. It includes an air-interface specification, a host-to-Bluetooth-device interface specification-the 'host controller interface'-and interoperability profiles. The profiles are used as part of a qualification programme that the Bluetooth SIG has established to assure interoperability between equipment from different vendors.

To be attractive to the mass market, the Bluetooth wireless technology needs to be both

easy to use and cost competitive with the cable systems it is replacing. The cost-competitive requirement has led to the view that Bluetooth terminals should cost less than $5.

In developing the Bluetooth specification a number of goals were identified for the air interface design:

(a) global applicability,
(b) low cost,
(c) low power,
(d) robust operation,
(e) high aggregate capacity,
(f) flexible usage,
(g) multiple simultaneous links,
(h) mixed voice and data.

2. CHOICE OF SPECTRUM

The choice of the Industrial, Scientific and Medical (ISM) band at 2.4 GHz enabled the goals of global applicability, low power and high aggregate capacity to be met. As it is a license-exempt band, consumers can use the equipment alter a single transaction at the point of sale. However, Bluetooth terminals do not have exclusive use of the band and therefore there is no protection from other users in the same band; both IEEE 802.11 Wireless LAN [3] and Home RF [4] products, as well as proprietary equipment, use the same band.

Although the 2.4 GHz ISM band is available globally, when the Bluetooth standard was first developed there were some variations in the exact frequencies available. This resulted in the standard having a 79 channel, see Fig.1 version and also a 23 channel version for use in those countries where the full ISM band was not available. At the time of writing, all those countries where originally only a reduced spectrum was available have announced that they will make the full ISM band available.

BWT-enabled devices hop between frequencies up to 1600 times per second

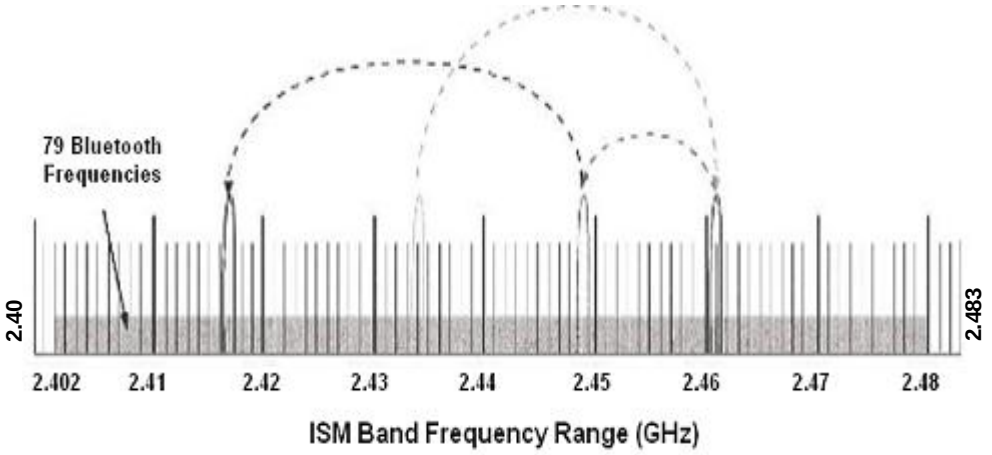

Fig.1

3. KEY SYSTEM FEATURES

3.1. PICO NETS AND SCATTERS NETS

Although the concept of 'cable-replacement' might create a vision of point-to-point communication, the Bluetooth SIC; has exploited the fact that wireless devices can communicate with other devices that are within range. A network of communicating Bluetooth devices is referred to as a 'piconet'.

The topography of a piconet is a star configuration: 'slave' devices within the net communicate with a 'master' and therefore must be within range of that master.

Bluetooth devices can be either masters or slaves. Any Bluetooth device can be the master; the concept is not tied to a specific entity. The master is often the device that initiated the first connection but the master of a specific piconet can be changed dynamically during the existence of that piconet.

Several piconets may be combined to form a 'scatternet'. This involves Bluetooth devices being members of more than one piconet, for example as a master in one and as a slave in another, as shown in Fig. 2. Although all devices are capable of acting both as a master and as a slave, they cannot be a master and a slave at exactly the same time-they must switch between modes.

Within a piconet, a piconet is an ad-hoc computer network linking a user group of devices using Bluetooth technology protocols to allow one master device to interconnect with up to seven active slave devices (because a three-bit Media Access Control (MAC) address is used). Up to 255 further slave devices can be inactive, or parked, which the master device can bring into active status at any time.

Combining Pico nets to form a scatternet

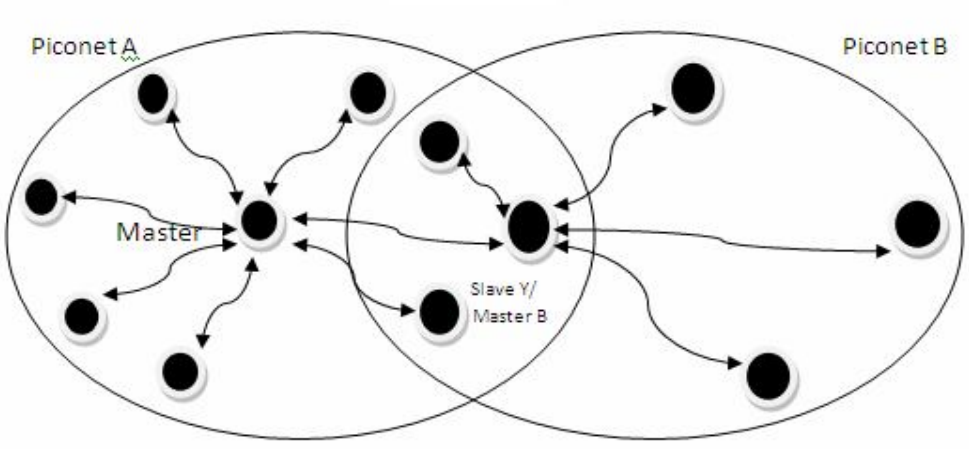

Fig. 2

3.2 AD HOC NETWORKING

The Bluetooth specification provides mechanisms for Bluetooth devices to discover each other, exchange identities and establish communications with each other, all without prior

knowledge of each other. This is referred to as 'ad hoc' networking. An example of its application is where a number of people are around a conference table; information can be shared and presentation material exchanged in a very simple way. Ad hoc networking is further facilitated by the Bluetooth Service Discovery Protocol (SDP), which allows Bluetooth devices to discover what services are available or to find a Bluetooth device that supports a specific service. This is an important feature given the dynamic nature of ad hoc networking. It allows a Bluetooth device to find a specific service without prior knowledge of the Bluetooth address of that service. For example, a laptop computer could search for a printer service when it is being used at a new location.

A more private operational scenario is where the devices communicating with each other form a 'closed' group. An example is where a single person wants their mobile phone, laptop and PDA to be in communication but does not want other devices within range to participate in any way. In contrast to this 'closed' networking, ad hoc networking is 'open'.

3.3 SECURITY

To provide privacy, a number of security features are supported: encryption is used as a safeguard against eavesdropping, and authentication is used for verification of identity. By exchanging (private) keys, trusted relationships may be established between devices. For example, a headset can be 'paired' with a mobile phone by entering into each device a PIN (personal identification number), from which a (private) key is then derived for use in authentication. Subsequently the headset needs only to be authenticated to verify its identity-the PIN does not need to be entered each time the user wishes to use the headset with the phone.

Security has played a major role in the invention of Bluetooth. The Bluetooth SIG has put much effort into making Bluetooth a secure technology and has security experts who provide critical security information. In general, Bluetooth security is divided into three modes:

(a) Non-secure,
(b) Service level enforced security and,
(c) Link level enforced security.

In non-secure, a Bluetooth device does not initiate any security measures. In service-level enforced security mode, two Bluetooth devices can establish a non secure Asynchronous Connection-Less (ACL) link. Security procedures, namely authentication, authorization and optional encryption, are initiated when a L2CAP (Logical Link Control and Adaptation Protocol) Connection-Oriented or Connection-Less channel request is made. The difference between service level enforced security and link level enforced security is that in the latter, the Bluetooth device initiates security procedures before the channel is established.

Bluetooth security procedures include authorization, authentication and optional encryption. Authentication involves proving the identity of a computer or computer user, or in Bluetooth's case, proving the identity of one piconet member to another. Authorization is the process of granting or denying access to a network resource. Encryption is the translation of data into secret code. It is used between Bluetooth devices so that eavesdroppers cannot read its contents. However, even with all of these defense mechanisms in place, Bluetooth has shown to have some security risks. The next section of this paper will describe some of these vulnerabilities associated with Bluetooth technology.

4. AIR INTERFACE FORMAT

Bluetooth operates as a 79 channel frequency-hopping system in the frequency range 2.4000-2.4335 GHz with channel spacing *of* 1 MHz. The hopping rate is 1600 hops per second; see fig.1 and the hopping sequence, which is different for each piconet, is a function of both the master's Bluetooth device address and its Bluetooth clock. The Bluetooth device address is a 48 bit address that is uniquely assigned to each transceiver. Frequency hopping is used to minimize the effects of interference from other users within the same band.

Three classes of Bluetooth device have been defined, the maximum transmitter powers being 100 mW(20 dBm), 2.5 mW(4 dBm), and 1 mW 0 dKm) for class1, 2, and **3** devices, respectively. The nominal power of a class 2 device is 1 mW(0 dBm). The nominal value provides some indication of the expected performance, whereas the maximum value is that allowed in the test specification. Power control is expected to be applied for class 1 devices down to 0 dBm but is not required for class 2 and class 3 devices.

The air interface supports two basic bearer types. Asynchronous Connectionless (ACL) bearers use packet switching and a polling access scheme and provide asynchronous, (a) symmetric services. Synchronous Connection Oriented (SCO) bearers are circuit switched, use slot reservation at fixed intervals and provide symmetric synchronous services. Typically, ACL bearers are used for data and SCO bearers for speech audio services. The air interface supports a mix of packet types.

5. ESTABLISHING AND MAINTAINING A PICONET

To establish a piconet a Bluetooth device will either inquire or page. The inquiry mode is used when the address is not known; paging is used when the paging device knows the Bluetooth device address of the required unit. Although the mechanisms for inquiry and paging are similar, they are considered as separate mechanisms within the Bluetooth specification. Inquiry is used to find the Bluetooth device addresses of neighboring devices, whereas paging is used to connect with a specific device. Even though a neighboring device may respond to an inquiry, it is then up to the controlling application of the inquiring device subsequently to initiate a connection with that device, i.e. it is not automatically managed by the Bluetooth protocol.

6. PROTOCOL ARCHITECTURE

The Bluetooth protocol stack allow devices to locate, connect, and exchange data with each other and to execute interoperable, interactive applications against each other. The Bluetooth specification has adopted a layered model for the protocol slack, see Fig.3. The following points are noteworthy. The Host Controller Interface (HCI) is a defined interface within the protocol stack. The Bluetooth specification allows a physical separation between the link manager and the higher layers at the HCI, which is common in most Bluetooth implementations. The HCI supports the transmission of SCO (audio) and ACL data types across it. In addition, the HCI provides a management interface for control of the link manager and baseband, using the specified HCI commands and events. L2CAP, the Logical Link Control and Adaptation Layer Protocol, is a multiplexing protocol that supports a number of different protocols above it. The Service Discovery Protocol (SDP) is one such protocol, but this protocol is itself a feature of Bluetooth in that it provides a service to other Bluetooth devices to allow them to search for application services on a device.

Bluetooth protocol architecture baseband

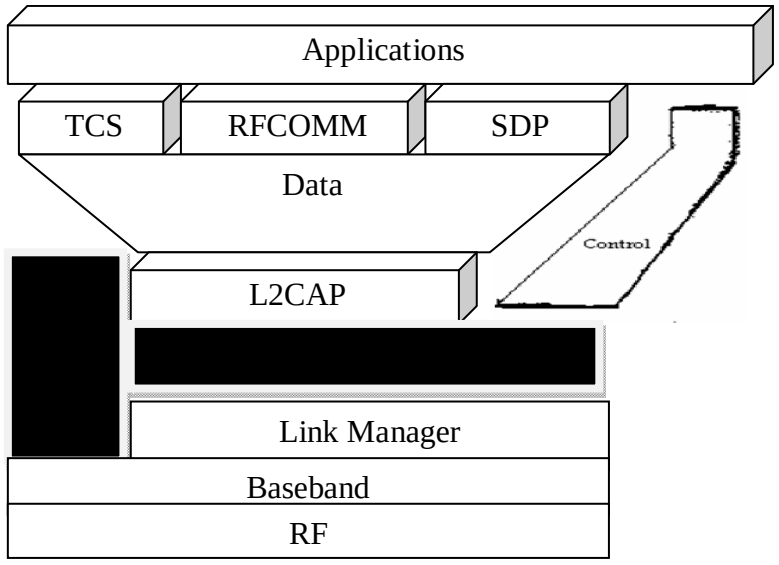

Fig. 3

The baseband section of the Bluetooth specification includes the air interface packet framing and link control. It provides the 'lower layer' functionality required to establish and to maintain piconets, including some messaging. These messages are transmitted using the link control packets. This functionality is placed at such a low level as it is closely coupled with the frequency-hopping sequence, which is derived from the Bluetooth clock and the Bluetooth address of a device.

6.1. LINK MANAGER

The link manager is responsible for link set-up and control. This is achieved by the Link Management Protocol (LMP). The link manager assumes that the link control provides a guaranteed delivery mechanism for the LMP messages. It provides the protocol support for a number of procedures, including:

(a) authentication,
(b) encryption control,
(c) link physical parameter control, e.g. power control, timing accuracy,
(d) Master-to-slave switching (and vice versa).

6.2. HOST CONTROLLER INTERFACE

The HCI is a specified interface within the protocol stack that can be implemented over a physical transport mechanism. Within the Bluetooth specification the choice of physical transport mechanism is left as implementation dependent, with three physical transports provided as standard: RS232, UART and IJSB.

The HCI supports ACL, SCO and HCI command and event logical channels.

Both ACL and SCO packets are supported bi-directionally. The control information is less symmetrical the HCI is driven from the host, with commands being sent to the host controller. The host controller may send events to the host. The commands that can be sent from the host fall into a number of categories:

(a) link control, for setting up inquiry and connections,
(b) link policy, for controlling modes such as park and sniff,
(c) host controller and baseband, for reading and writing various parameter values, such as timer values,
(d) informational parameters, for reading parameters,
(e) the local Bluetooth device address, that cannot be written locally,
(f) status parameters, such as RSSI (received signal strength indicator) levels,
(g) testing, for placing the device into a test mode.

Commands sent from the host to the host controller are responded to immediately with the result or the, request, if it can be returned by the host controller from information stored locally. Otherwise, the host controller responds with a command status event indicating that the request is pending. This is used where an over-the-air operation is involved. A further event will be sent to the host once the information requested has been supplied by the remote device. Flow control is specified across the HCI for commands and events, and independently for SCO and ACL data. Flow control is provided for in both directions within the specification; however it is only mandated in one direction. This is a reflection or the assumed base case where the host controller has physically fewer resources than the host and thus potentially is more likely to be 'flooded' with data. The HCI provides for a mechanism whereby the higher layers of the protocol stack can delegate the decision on whether to accept connections to the link manager and whether to switch on filters at the link manager. This is to reduce the volume of signaling traffic that is sent across the HCI.

6.3 L2CAP

The purpose of the Logical Link Control and Adaptation layer Protocol (L2CAP) is to provide connection-oriented and connectionless data services to higher layer protocols. To achieve this L2CAP provides the following functionality:

(a) multiplexing of higher layer protocols,
(b) establishment, maintenance and clearing of logical connections for connection-oriented services,
(c) segmentation and re-assembly services to allow packets of up to 64 kilobytes to be transported between L2CAP entities.

Additional features include support for groups and QoS (quality of service) negotiation for connections.

6.4 SERVICE DISCOVERY PROTOCOL

The Service Discovery Protocol (SDP) allows Bluetooth devices to discover what services are available on a device. It has a client-server architecture that uses the Service Discovery Database at the server. The Service Discovery Database (or SDP server) contains a number

of Service Records, and each Service Record contains attributes of the service. One of the attributes is the Service Record Handle, which uniquely identifies each service record within the SDP server.

The SDP supports both searching for services and browsing. Searching allows a client to search for a specific service, which is subsequently identified by the Service Record Handle attribute. Browsing allows a client to discover what services are supported; these are identified by the service attributes, including the Service Record Handle. Once a service has been identified, its attributes can be requested using the Service Record Handle. The attributes include information on how to connect to the service via the protocol stack, e.g. the RFCOMM server channel number with which the service is registered.

The Service Discovery Protocol is run over L2CAP.

6.5 RFCOMM

Radio Frequency communication (RFCOMM) is a protocol that provides an emulation of serial ports over the L2CAP protocol. It is based on the El31 GSM mobile telephone specification TS 07.10 [5]. The concept is basically to allow a laptop, or other computing device, to connect to, say, a GSM phone, which is used as a radio modem for remotely accessing data services via the GSM network. The emulation of E-232 serial ports by RFCOMM includes the transfer of the state of non-data circuits, for example clear to Send (CTS).

RFCOMM supports two device types. A Type 1 device is a communication end point, such as a computer. A Type 2 device is a part of a communication segment, for example a GSM phone acting as a radio modem.

Communication between two Type 1 devices is possible with RFCOMM. Within the Bluetooth specification this is used for services such as object exchange, for example where business card information is passed between two devices.

RFCOMM emulates up to 60 serial ports between two devices. Radio frequency communications (RFCOMM) is a cable replacement protocol used to create a virtual serial data stream. RFCOMM provides for binary data transport and emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer.

RFCOMM provides a simple reliable data stream to the user, similar to Transmission Control Protocol (TCP). It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth.

Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM.

6.6 TELEPHONY CONTROL SPECIFICATION (TCS)

Telephony Control is an adaptation layer that enables Q.931 (ISDN) call control services to be supported via L2CAP It provides synchronization between the call control and the SCO service used to transport the telephony speech. It essentially provides the Layer 3 Protocol functionality required to realize a Bluetooth cordless telephone.

Telephony Control provides the following services:

(a) call control
(b) group management
(c) Connectionless signaling.

There is support for three supplementary services as defined by TCS: Calling Line Identity Presentation (CLIP), DTMF (dual tone multiple frequency) start arid stop and register recall.

Call control provides the mechanism to signal between calling and called parties to establish, maintain and release voice calls. The establishment of the calls also requires synchronization internally between the call control instance and the called/calling parties. This is particularly important in a Bluetooth cordless base station, where more than one call may be possible concurrently. Call control operates over L2CAP.

Group management provides procedures for managing a group of devices, referred to as a wireless user group (UWG). The procedures include access rights management, configuration distribution and fast inter member access.

The connectionless service allows signaling information to be exchanged without the need to establish a TCS call. The concept of 'connectionless' exists only at the TCS layer for the purposes of this service; it is actually realized via a connection-oriented L2CAP service across the air interface.

7. LIMITATIONS OF BLUETOOTH SECURITY

(a) Only a device is authenticated, and not its user. There is no mechanism to preset authorization per service. However, a more flexible security policy can be implemented with the present architecture without a need to change the Bluetooth protocol stack.
(b) It is not possible to enforce unidirectional traffic.
(c) Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER block cipher.
(d) Bluetooth key generation is generally based on a Bluetooth PIN, which must be entered into both devices. This procedure might be modified if one of the devices has a fixed PIN (e.g., for headsets or similar devices with a restricted user interface).
(e) During pairing, an initialization key or master key is generated, using the E22 algorithm. The E0 stream cipher is used for encrypting packets, granting confidentiality and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.

7.1 BLUEJACKING

Bluejacking is the sending of either a picture or a message from one user to an unsuspecting user through Bluetooth wireless technology. Common applications include short messages. Bluejacking does not involve the removal or alteration of any data from the device. Bluejacking can also involve taking control of a mobile wirelessly and phoning a premium rate line, owned

by the bluejacker.

8. ERROR CORRECTIONS IN BLUETOOTH

Three error correction schemes are defined for the Bluetooth baseband controller:

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

The purpose of the FEC scheme on the data payload is to reduce the number of retransmissions. However in a reasonably error-free environment, FEC creates unnecessary overhead that reduces the throughput. Therefore, the definitions have been kept flexible as to whether or not to use FEC in the payload. The packet header is always protected by a 1/3 rate FEC. It contains links information and should survive bit errors. An unnumbered ARQ scheme is applied in which data transmitted in one slot is directly acknowledged by the recipient in the next slot. For a data transmission to be acknowledged, both the header error check and the cyclic redundancy check must be satisfied, otherwise a negative acknowledgement is returned.

9. PRODUCT AVAILABILITY

Bluetooth products are now available. The range of products available at the end of 2000, or planned for release early in 2001, includes: cordless headsets and the associated mobile phone dongle, PC Cards, LAN access ports, and PDA communication products. During 2001, it is expected that the number of manufacturers offering these products will rise significantly. New products will include domestic cordless telephones and Bluetooth modems. The Bluetooth website (www.Bluetooth.com) includes a list of qualified products.

10. BLUETOOTH APPLCATIONS

The following are some of the areas where Bluetooth can be used:

(a) Replacing serial cables with radio links,
(b) Wearable networks/WPANs,
(c) Desktop/room wireless networking,
(d) Hot-spot wireless networking,
(e) Medical: Transfer of measured values from training units to analytical systems, patient monitoring,
(f) Automotive: Remote control of audio/video equipment, hands-free telephony,
(g) Point-of-sale payments: Payments by mobile phone.

11. WAP AND BLUETOOTH

Bluetooth can be used with WAP like any other wireless networks. Bluetooth wireless networks can be used to transport data from a WAP client to a WAP server. The WAP client can make use of Bluetooth's SOP to find the WAP server/gateway. This is very useful when the WAP device is a mobile phone and when it comes into the range of a WAP server, it can use Bluetooth's SDP to discover the gateway. The Bluetooth SDP must be able to provide

some details about the WAP server to the WAP client.

The other feature that can be supported is the reverse of the above. The WAP server can periodically check for the availability of WAP-enabled clients in its range. It can use Bluetooth's SDP to do this. If there are any clients, the server can push any data to the client. The client of course is not required to accept the data pushed to it.

12. CONCLUSION

In this paper we discussed Bluetooth technology that allows for replacing many proprietary cables that connect one device to another with one universal short-range radio link. Bluetooth radio technology provides a universal bridge to exiting data networks, a peripheral interface, and a mechanism to form small, private ad hoc groupings of connected devices away from fixed network infrastructures. The Bluetooth technology has a number of advantages including minimal hardware dimensions, low cost of components, and low power consumption. These advantages make it possible to introduce Bluetooth in many types of devices at a low cost. The 720 kbps data capability provided by Bluetooth can be used for cable replacement and several other applications, such as LAN.

13. REFERENCES

[1] IEEE802.15 Working Group, http://www.ieee802.org/15/pub/TG1.html .

[2] Shepherd R., "*Bluetooth wireless technology in the home*", Electron. Commun. Eng. J., Vol. 13, No. 5, pp.195–203, October 2001 .

[3] "*IEEE Standards Interpretation for IEEE Std 802.11™-1999 Information technology-Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*", http://standards.ieee.org/findstds/interps/802.11-1999.html.

[4] "*Home RF Technical Specification*", www.palowireless.com/homerf/homerf4.asp.

[5] Pecen M., Howell A., "*Simultaneous voice and data operation for GPRS/EDGE: class A dual transfer mode*", Personal Communications, IEEE, Vol. 8, No. 2, pp. 14-29, Apr 2001.