6 - Wireless Personal Area Networks (WPAN)

A Wireless Personal Area Network (WPAN) is a term given to describe the collection of mobile and fixed devices that are able to be connected to a network and are within close proximity of each other. A WPAN is able to be constructed and de-constructed at will by the individual. Equipment in the WPAN may not necessarily be connected to fixed network equipment. This type of network provides for truly mobile computing and connectivity.

The international standard developed by the Institute of Electrical and Electronic Engineers (IEEE) for this wireless technology is known as IEEE 802.15. However, the basics for this technology were developed initially by Ericsson and later through collaboration with a group of other companies who are known as the Bluetooth Special Interest Group. The IEEE standard was developed after this group developed the technology. The term Bluetooth is the name given to a 10th century Danish King, Harald Blatland (meaning Bluetooth) who united the areas of Scandinavia currently known as Denmark and Norway.

This technology has been designed to "unite" separate mobile and fixed devices such as notebook computers, personal digital assistants, mobile telephones, accessories and printing devices. Primarily the technology was designed for file sharing and interconnectivity between devices on a random and *ad hoc* basis. Due to the inherent difficulties of establishing a random network using cables to connect the devices, a wireless or radio frequency solution was employed.

As radio spectrum is licensed throughout the world, the developers chose to use the generally unlicensed spectrum in the 2.4 to 2.4835GHz band thus avoiding licensing issues. Interestingly this is the same spectrum band termed as the Industrial, Scientific and Medical (ISM) band. Each device that is enabled for this technology is able to communicate with other similarly enabled devices to form networks termed "piconets". In a piconet, one device is termed the master with the other devices termed as slaves. There can be up to eight devices in any one piconet with these devices able to be in other piconets simultaneously.

BOX: 6.1 – WHAT IS THE IEEE?

The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 377,000 individual members in 150 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organisation is most popularly known and referred to by the letters I-E-E-E. Through its members, the IEEE is a leading authority in technical areas ranging from computer engineering, biomedical technology and telecommunications, to electric power, aerospace and consumer electronics, among others. Through its technical publishing, conferences and consensus-based standards activities, the IEEE produces 30 percent of the world's published literature in electrical engineering, computers and control technology, holds annually more than 300 major conferences and has nearly 900 active standards with 700 under development.
http://www.ieee.org

History

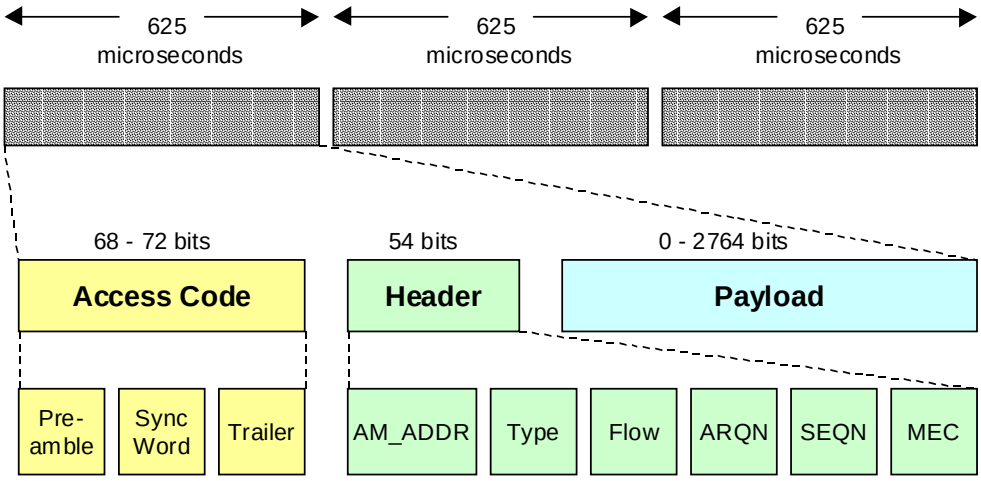
The Bluetooth Special Interest Group utilised the design proposed by Motorola's Piano for personal area networks to allow for greater functionality and to increase the usefulness of Bluetooth beyond cable replacement.[1] A focus of WPANs is on mobility and short-duration networks. This includes a decentralised control of content; lower power consumption, fewer connections than a local area network; short duration of the network; and, lower enabling and equipment costs.[2] In 1998, Ericsson combined forces with IBM, Intel, Nokia and Toshiba to form the Bluetooth special interest group that has wide support amongst a range of equipment, software and service providers.[3] The first version of Bluetooth was published in 1999 with an amended version of 1.0b with minimal changes. The IEEE 802.15 Standard is based upon version 1.0b and approved 15 April, 2002.[4]

Technology

WPAN communications using the IEEE 802.15 standard operate in the 2.4 to 2.4835GHz ISM and have a fast frequency hop of 1600 hops per second across 79 1MHz channels. The hopping reduces interference and the fading of the signal and uses a fast time division duplex scheme (See Box 6.2) with each hop having a duration of 625 ms. Information is passed to each device through packets with each packet transmitted on different frequencies. For data communications a unidirectional signal is used with a theoretical maximum data rate of 723.2 kbs (57.6 kbs downstream) and symmetric data transfer with a theoretical maximum of 433.9 kps. However for voice communications, a bi-directional 64 kbs channel is used and jitter is reduced in the voice traffic through the small packet sizes.

There is the possibility for interference to occur as the 2.4GHz spectrum is also used by other wireless technologies including the IEEE 802.11 standard (see Chapter 7 – Wireless Local Area Networks), cordless telephones. Microwave ovens also emit radio waves in this frequency. The data packet arrangement is shown in Figure 6.1 – Bluetooth Data Packet.

Figure 6.1 – Bluetooth Data Packet.



Format of an over-the-air payload bearing Bluetooth WPAN packet Adapted from IEEE Std 802.15.1-2002 Figure 3.

BOX 6.2 – WHAT IS TIME DIVISION DUPLEX?

Time Division Duplex is a transmission method that uses only one channel for transmitting and receiving, separating them by different time slots. No guard band is used. By contrast, Frequency Division Duplex (FDD) is a transmission method that separates the transmitting and receiving channels with a guard band (some amount of spectrum that acts as a buffer or insulator).

As the WPAN is meant for mobile devices, it is important that the power usage be kept low. The IEEE 802.15 specifications allow for three classes of transmit power; have differing transmit distances; and, data rates. Table 6.1 – Class Characteristics for 802.15 Devices shows the variability. Most of the plug-in hardware devices such as a PCMCIA or Flash cards will be Class 3 devices. In Chapter 9 – Comparison of Wireless Technologies, the IEEE 802.15 devices will be shown to use the least power of all.[5]

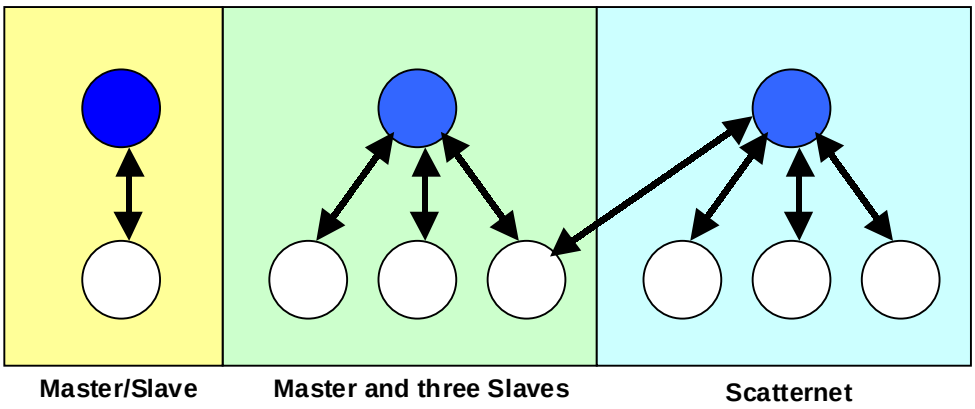
Table 6.1 – Class Characteristics for 802.15 Devices[6]

Type	Power	Range
Class 3	0 dBm / 1 mW	~ 10 centimetres
Class 2	4 dBm / 2.3 mW	~ 10 metres
Class 1	20 dBm / 100 mW	~ 100 metres

Piconets

Piconets are the *ad hoc* networks established through this technology with each piconet having a master and one to seven active slaves (See Figure 6.2 – Piconets). As the enabled devices come within range, a master is elected by establishing the connection with the other device(s) setting the frequency hopping sequence and the system clock to determine the phase. The connection is managed using a Link Manager Protocol that controls the physical radio frequency (RF) link and negotiates the packet size during transmission; manages power modes and consumption; and, encryption.[7]

Figure 6.2 – Piconets



Various piconet fomations. Adapted from IEEE Std 802.15.1-2002 Figure 4

Connection Modes

There are four methods of connecting these devices. The first is the active mode where the device actively seeks other devices and is assigned an active member network address (AM_ADDR). The second connection mode is termed as 'hold' and operates in a reduced power mode while still retaining its active member network address. The hold mode can receive synchronous data packets only. The third mode is the 'sniff' mode which not only operates in a reduced power mode with an active member address but is able to receive synchronous and asynchronous packets. The sniff mode allows a device to be involved in another piconet simultaneously (this involvement forms a scatternet). The fourth connection mode is 'park' and allows a unit to listen for broadcast messages from the master but not to actively participate in the piconet. Consequently the device is given a parked member address (PM_ADDR). In any one piconet there can be a maximum of 255 parked devices.[8]

Every device in this technology is in a standby mode by default and periodically scans for other enabled devices. The first type of scan is a page scan where the device listens for its own device access code which is used to convey the device's name when setting up connections between devices. This scan occurs every 11 ms. A potential master device scans the available frequency hops looking for another device every 1.28 seconds through two sets of frequencies.[9]

Physical Links

This technology has two types of physical links. One is the Synchronous Connection-Oriented (SCO) and provides for up to three 64 kbs circuit-switched connections for voice and audio and does not allow for re-transmission of the data packets. The other is the Asynchronous Connectionless (ACL) which is a packet-switched link with up to 721 kps downstream (57.6 kps upstream) and 432.6 kps symmetrical data transfer with no error correction employed.[10] The proposed enhancements to the Bluetooth 2.0 specification will see higher data rates of between 2 to 12 Mbps.[11] It is important to note that with interference and other limiting factors, it is wise to assume that the advertised data rates are theoretical maximums and are not actually able to be achieved. By reducing the advertised rates by half provides a more realistic value.

Protocol Stack

The main purpose of this technology is to ensure that devices will be able to communicate with each other and this requires the use of compatible communication stacks. Figure 6.3 – Protocol Stack describes the arrangement of the protocol stack and is mapped to the Open Systems Interconnection (OSI – See Box 7.1). The protocol stack includes a set of routines to perform a range of tasks for communication between devices. Communication between the layers in the stack move from lowest to highest for incoming data and highest to lowest for outgoing data. Current devices have a silicon chip that manages the Link Manager and the baseband with the radio frequency managed by another protocol.[12]

Bluetooth protocols

Baseband - This refers to the synchronous or asynchronous arrangements described above in Physical Links.

Link Manager - controls the data packets from the master to the slave as described above in Piconets

Host Controller Interface - this provides a uniform interface method for accessing the Bluetooth hardware capabilities. It contains a command interface to the baseband controller and the Link Manager on one side and the protocol stack on the other.

Logical Link Control and Adaptation Protocol - Links to the Host Controller Interface and allows multiple channels to share a single link. TCP/IP connections and Object Exchange Protocol (OBEX) file transfer (see below) can be used simultaneously. Additionally this protocol segments and reassembles the outgoing data packets that exceed the maximum size (no more than 2745 bits); maintains quality of service; and, maps piconets.[13]

Service Discovery Protocol - this provides a method to discover services available without the user determining if the service is available or not.

Telephony Control - this is a bit-oriented protocol which defines the call control signalling for the establishment and release of speech and data calls between devices.

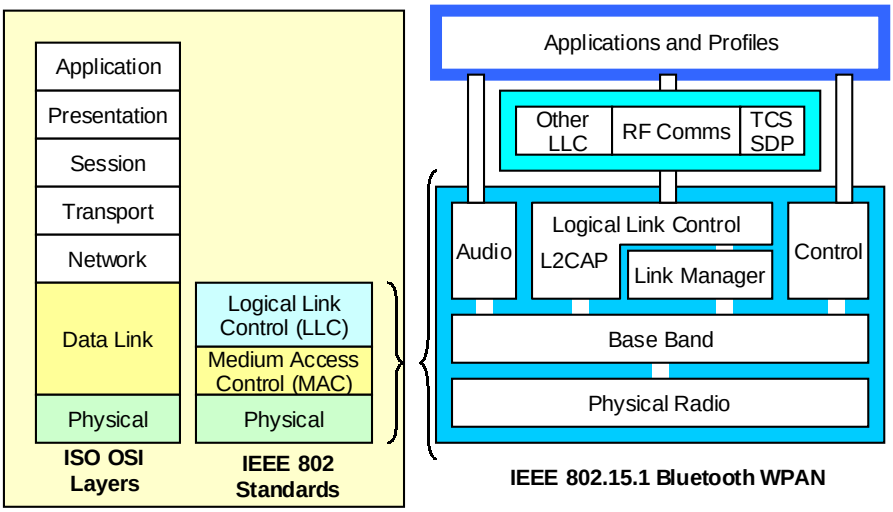
Non-Bluetooth protocols

Radio Frequency Communication (RFCOMM) - This protocol acts as a serial port for the device and emulates an RS-232 port that is widely used for serial data transfers.

Object Exchange Protocol (OBEX) - This provides a simple mechanism for moving objects like files, electronic business cards and messages. This layer is optional and uses infrared.

PPP, TCP/IP, UDP - Transmission Control Protocol over Internet Protocol (TCP) and User Datagram Protocol (UDP) are the two transport protocols in TCP/IP. TCP ensures that a message is sent accurately and in its entirety. However, for real-time voice and video, there is really no time or reason to correct errors, and UDP is used instead. This corresponds to the Asynchronous Connectionless and Synchronous Connection-Oriented (respectively) as described above in Physical Links.

Figure 6.3 – Protocol Stack



Mapping of ISO OSI to scope of IEEE 802.15.1 WPAN Standards Adapted from IEEE 802.15.1-2002 Figure 2

Profiles

As this technology has a broad range of possible applications, there needs to be a defined set of rules that govern how the Protocol Stack is to be used. These are called profiles and thirteen have been developed by the Bluetooth Special Interest Group. WPAN devices will be processing one set of data at a time and therefore not all of the protocol stack will be used. For example, the serial port profile requires the Logical Link Control and Adaptation Protocol, Service Discovery Protocol, and the RFCOMM protocol but not the others. [14]

Generic Access Profile - This defines how two devices find each other and establish a connection. It also handles the discovery and connection of other units including the types of services and applications that each will support. This profile is important to suppliers of devices to insure compatibility.

Service Discovery Application Profile - This defines how the application software on a device is able to find services on other devices. This profile is particularly important to ensure that new services and applications are able to be recognised. This is similar to the plug-n-play connectivity that many users will expect to see.
Serial Port Profile - This defines how the RS-232 serial port emulation is established between devices.
Generic Object Exchange Profile - This defines the protocols and procedures that are to be used for defining the lower layer protocols that use the Object Exchange Protocol.

Other profiles that are optional in devices are:

- Cordless Telephony (allowing for telephone calls to be made through a wireline system)
- Intercom (allows for a 'walkie-talkie' function between devices)
- Headset
- Dial-up Network
- Fax
- LAN
- Object Exchange (for the transfer of business cards, appointment lists)
- File Transfer (allows for file sharing between devices as well as deleting files on other devices)
- Synchronisation (for transferring data from a user's PC to Personal Digital Assistant)

Security

Security is an issue of concern for wireless communications as these transmissions in an *ad hoc* network can be captured by other devices. Therefore it is important for users to understand the security issues involved in all wireless technologies. The WPAN technology is able to be made secure but is primarily intended to have high levels of compatibility with other enabled devices.

The frequency hopping of IEEE 802.15 devices goes someway to preventing eavesdropping by other devices as only those devices in the piconet know the hopping sequence. However, when a new device is added to the piconet, the users of the other devices are able to manage the security levels for those newcomers. There are three modes of security available to this technology. [15]

Mode 1 - this is a non-secure mode to be used to seek out other devices. In this mode, the device transmits its Device Access Code but does not start a security, authorisation or encryption procedure.
Mode 2 - Using a private user key for authentication, this mode will allow flexible polices for access to applications and services and is used for applications running in parallel but have differing security requirements.
Mode 3 - This mode requires the device to have authentication and encryption before any connection is able to be established.

When devices join in a piconet, settings from previous sessions can be re-established. This will allow trusted devices to begin the session without re-establishment of the security settings. New devices will need to go through the security preferences with these trusted devices. A device can be set so that unknown devices are not aware of the physical presence of the device or are not able to connect to the device without authorisation. Before the creation of the first session, the users of the two devices need to enter a PIN of up to 16 digits. This then creates a key that can be used for future sessions.

Current forecasts

Bluetooth enabled devices are likely to become the most popular wireless connectivity technology as many manufacturers of mobile telephones and personal digital assistants are including this technology within the product. Estimates vary on the number of products with this technology with total installed base of 125 million units in 2003[16], rising to 1.6 billion by 2006.[17] This growth is not surprising especially when the cost of the chipsets are believed to be heading towards US$10 in 2003.[18]

ZigBee

ZigBee is a WPAN technology and has as the standard the IEEE 802.15.4. This technology is a competing technology to Bluetooth and is a low-cost and lower-power wireless technology. The technology works in the 2.4GHz spectrum with a theoretical maximum data throughput of 220 Kpbs. The maximum distance for transmission is 75 m. The initial application target is for in-home device connectivity including light control, fire protection, climate control and security systems.[19] At the time of preparing this report few products were available but with participating companies such as Mitsubishi, Motorola and Philips. More developments are likely.[20]

IMPLICATIONS FOR THE SHARED TECHNOLOGY INDUSTRIES

Automotive

The use of a WPAN is ideally suited to a motor vehicle as the distances between devices within the cab will be limited to an acceptable range and the use of cables to connect devices are cumbersome. For this reason the IEEE 802.15 will be the technology used. Major motor vehicle manufacturers including BMW, General Motors, and Daimler Chrysler are planning to include this technology in 2003[21] and it is estimated that by 2007 between 20 to 42 percent of all vehicles worldwide will be fitted with this technology.[22] It is important to note that the sales of enabled devices was .6 million in 2000 and is expected to be 1600 million in 2006. The anticipated estimated working life of the equipment is much shorter than the life of a motor vehicle and compounded with enhancements of software. It is likely that there will be an increase in the number of vehicles that are retro-fitted with IEEE 802.15 enabled "hands-free" systems, and this will begin to occur very soon.[23]

An important note here is that "telematics" is a general term for communications intra- and inter-vehicle in the automotive industry and this may include not only IEEE 802.15 enabled devices but also devices that record and store engine performance for capture by service centres. It will be important to distinguish between IEEE 802.15 systems (for user's voice and data) and vehicle performance monitoring by service managers.

One area termed telematics by US and European manufacturers is a high value service for subscribers that allows for emergency attendance or assistance for the user. General Motors' OnStar service for Cadillac and 35 other models includes features such as voice-activated dialing, navigation, roadside assistance and remote diagnostics.[24] The OnStar system is an integrated cellular telephone within the vehicle which is separate to a mobile handset. The demand for these services is yet to be realised in Australia as many individuals hold memberships in automotive clubs that provide road-side assistance and navigation may not be necessary in familiar areas. Voice activated dialing is already a capability of mobile handsets.

Building and Construction

The review of the literature for this report did not uncover any discussion of WPAN technology. This is not unreasonable as WPAN devices are primarily for mobile applications. There are some emerging applications for a wireless local area network (See Chapter 7 – Wireless Local Area Networks) to be used but commercial applications will tend to stay with a cable-based solution for greater reliability and security.

Engineering

In process control, manufacturing and other structure-based locations, IEEE 802.15 will not be a likely solution. There is the possibility that remote and non-networked devices may be enabled with this technology for intermittent readings.

Electrical

IEEE 802.15 is unlikely to have many applications in this industry as it is primarily a mobile technology.

Electronics

Consumer electronics will benefit enormously from this WPAN enabled device. The interconnectivity within the home with an increase in digitally based devices will see data transfer much more prominent. Currently using infra-red communications, owners of personal digital assistants can download software to use the device as a remote control. The possibilities of using the personal digital assistant to download a television schedule and click on a program for digital recording is a highly likely scenario. At present, the impact of this technology on consumer electronics has not been identified to the extent that is possible.[25]

Information Technology

The use of IEEE 802.15 devices has been developed for workplace use with file sharing, printing, and voice communications. The technology is incumbent in this industry and is therefore not emerging. New applications and problem solving will continue during implementation.

Telecommunications

The IEEE 802.15 is likely to have a significant impact on the adoption of higher data-rate mobile handsets such as General Packet Radio Service (GPRS) or Code Division Multiplex Access (CDMA1x) wireless connections. Each of these will allow for faster data access and with mobile devices and computing devices enabled.[26] The ability to dial-up the Internet becomes a much more realistic possibility with these higher speed connections and with a compatible phone and notebook computer with a larger screen, a user is able to more easily view the content.

---

[1] LXE Inc. (2002). *Bluetooth Basics*. Available: http://www.lxe.com/whitepapers/whitepaper_bluetooth.htm Accessed 4 February, 2003.

[2] PricewaterhouseCoopers. (2002). *Technology Forecast: 2002-2004*. Menlo Park, CA: Author.

[3] Gartner. (2002). *Gartner's Glossary of Wireless and Mobile Terms: 2002 Update*. Reference Number: R-17-0193.

[4] IEEE Computer Society. (2002). *Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)*. New York: Author.

[5] Pico Communications. (2001). *Cats and Dogs Living Together: A Comparison of Bluetooth and Wi-Fi (802.11b)*. Cupertino, CA: Author. Available: http://www.picocommunications.com/white_papers.html Accessed: 4 February, 2003.

[6] Pico Communications. (2000) *Bluetooth and Bluetooth Internet Access Points*. Cupertino, CA: Author. Available: http://www.picocommunications.com/white_papers.html Accessed: 4 February, 2003.

[7] Atmel Corporation. (2000). *The Bluetooth Wireless Technology White Paper*. San Jose, CA: Author. Available: http://www.atmel.com/dyn/products/other_docs.asp?family_id=610 Accessed: 5 February 2003.

[8] DevX. (2000). *Bluetooth Wireless Technology Overview*. Available: http://archive.devx.com/wireless/articles/Bluetooth/BtoothIntro.asp Accessed: 4 February, 2003.

[9] DevX. (2000). *Bluetooth Wireless Technology Overview*. Available: http://archive.devx.com/wireless/articles/Bluetooth/BtoothIntro.asp Accessed: 4 February, 2003.

[10] Atmel Corporation. (2000). *The Bluetooth Wireless Technology White Paper*. San Jose, CA: Author. Available: http://www.atmel.com/dyn/products/other_docs.asp?family_id=610 Accessed: 5 February 2003.

[11] Infocom Development Authority of Singapore. (2002). *The Connected Home*. Singapore: Author. Available: http://www.ida.gov.sg (>Technology Development >Infocomm Technology Roadmap) Accessed: 5 February 2003.

[12] Troy XCD. (2000). *Bluetooth Protocol Stack*. Irvine, CA: Author. Available: www.troygroup.com/wireless/products/wireless/docs/bt_stack_white_paper.pdf Accessed: 5 February 2003.

[13] Atmel Corporation. (2000). *The Bluetooth Wireless Technology White Paper*. San Jose, CA: Author. Available: http://www.atmel.com/dyn/products/other_docs.asp?family_id=610 Accessed: 5 February 2003.

[14] Atmel Corporation. (2000). *The Bluetooth Wireless Technology White Paper*. San Jose, CA: Author. Available: http://www.atmel.com/dyn/products/other_docs.asp?family_id=610 Accessed: 5 February 2003.

[15] Pico Communications. (2001). *Cats and Dogs Living Together: A Comparison of Bluetooth and Wi-Fi (802.11b)*. Cupertino, CA: Author. Available: http://www.picocommunications.com/white_papers.html Accessed: 4 February, 2003.

[16] Infocom Development Authority of Singapore. (2002). *The Connected Home*. Singapore: Author. Available: http://www.ida.gov.sg (>Technology Development >Infocomm Technology Roadmap) Accessed: 5 February 2003.

[17] Hunn, N. (2002). *Bluetooth and Wi-Fi - The Market Status*. London: TDK. Available: http://www.tdksystems.com/support/whitepapers Accessed: 6 February 2003.

[18] Simpson, R., Milanesi, C., & Keene, I. (2002). *WLAN and Bluetooth Predictions, 2003*. Gartner Reference Number: SPA-18-7261.

[19] Hiller, K. (2002). *Wireless Networking With HomeRF: An Introduction*. Gartner Research. Reference Number: DPRO-93769.

[20] Continental Automated Buildings Association. (2002). *Four Major Companies Join Forces to Forge ZigBee Alliance*. Ottowa, ON: Author. Available: www.caba.org/standard/zigbee.html Accessed: 14 February 2003.

[21] Stackpole, B. (2003). *Look Ma, no hands!* Electronic Business, 1 February, 2003. Available: http://www.e-insite.net Accessed 4 February, 2003.

[22] Juliussen, E., & Magney, P. (2002). *Technologies for Telematics Systems: Trends, Outlook and Opportunities*. Minnetonka, MN: Telematics Research Group. Available: http://www.telematicsresearch.com Accessed:7 February, 2003.

[23] Gartner Dataquest. (2002). *Bluetooth and Telematics: At the Heart of the Wireless Car*. Reference No.: SEMC-WW-DP-0157

[24] Chatterjee, A, Kaas, H., Kumaresh, T. V., & Wojcik, P. J. (2002). A Road Map for Telematics. *The McKinsy Quarterly, Spring 2002,* pp. 100-110.

[25] Consumer Electronics Assocation. (2002). *5 Technologies to Watch.* Arlington, VA: Author. Available: http://www.ce.org/publications/default.asp Accessed: 7 February, 2003.

[26] Hunn, N. (2002). *Bluetooth - Saviour of GPRS.* London: TDK Systems. Available: http://www.tdksystems.com/support/whitepapers Accessed: 7 February 2003.