IEEE 802.11b WLAN versus Bluetooth

A paper describing the two technologies and evaluating their coexistence and future

2G1305 Internetworking

Authors

Fredrik Jacobson 770727-0372
Benjamin Özmen 780406-5956

Submitted: 11\textsuperscript{th} March 2002
Abstract

This paper is part of a home assignment in the course 2G1319 Internetworking, at the Royal Institute of Stockholm. It investigates the wireless technologies Bluetooth and IEEE 802.11b. The technologies are described and compared to each other. The main reason for writing this report was to evaluate the coexistence of the two technologies in the same network or if they were competitive technologies in the same market.

The conclusion in this paper is that the two technologies in fact have different end-user groups and that they both could add something to the wireless market.
**Introduction**

In the last few years, there have been many discussions about the two technologies IEEE 801.11b Wireless Local Area Network (WLAN) and Bluetooth. They are both operating by transmitting wirelessly and are both operating at the same frequency, 2.4 GHz. Therefore, many say they are competing technologies in both technological and business areas and one of them is not going to survive. This paper first examines the IEEE 801.11b WLAN and Bluetooth technologies apart and then evaluates their similarities, their differences and the possible coexistence of them in the future.

**WLAN**

A wireless local area network (WLAN) is a flexible data communication system implemented as an extension to, or as an alternative for, a wired LAN. Using radio frequency (RF) technology, WLANs transmit and receive data over the air, minimizing the need for wired connections. Thus, WLANs combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs.

There are several different standards used in WLANs. At the 2.4 GHz frequency band, the IEEE 802.11 b is dominating the market. At the 5 GHz frequency band there are two main technologies, these are IEEE 802.11a and HiperLAN-2. Both will have data bandwidths up to 54 Mbps, but these have not yet fully reached the markets.

This paper is investigating in the similarities and differences between IEEE 802.11b and Bluetooth, therefore, a more thoroughly discussion about the IEEE 802.11b is stated below.

**IEEE 802.11b**

The IEEE 802.11b standard is limited in scope to the physical (PHY) and Medium Access Control (MAC) network layers. The PHY layer corresponds directly to the lowest layer defined by the ISO in the OSI Reference Model. The MAC layer corresponds to the lower half of the Data Link layer. The Logical Link Control (LLC) represents the upper part of the Data Link layer. See figure 1 below.

![OSI Reference Model](http://alpha.fdu.edu/~kanoksri/IEEE80211b.html)

*Picture 1. The ISO Reference Model (source: http://alpha.fdu.edu/~kanoksri/IEEE80211b.html)*
The IEEE 802.11b standard specifies a choice of three different PHY layers, any of which can underlie a single MAC layer. The idea of allowing a choice of PHY implementations was necessary so that IEEE 802.11b systems designers and integrators have a choice in the technology that matches the price, performance, and operations profile of a specific wireless product or application. The standard allows an optical-based PHY layer that uses infrared (IR) light to transmit data, and two RF-based PHY layers that use different types of spread-spectrum radio techniques.

The IR PHY will typically be limited in range and is most practically used within a single room. The IR technique is not common today. The two RF-based technologies are Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS), and they will be described below.

Physical Layer techniques

The ISM bands
In the United States, the Federal Communications Commission (FCC) governs radio transmissions. Other nations have corresponding regulatory agencies. Most WLANs operate over one of the ISM (Industrial, Scientific and Medical) bands. These include 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35 GHz and 5.725-5.875 GHz. For WLANs to be sold in a particularly country, the manufacturers must ensure in certification by the corresponding FCC agency in that country. In the United States and most other countries, the ISM bands are unlicensed i.e. free to use for everybody including companies, households, schools etc.

In order to manage interference without requiring special site licenses, regulatory agencies require that products developed for unlicensed use employ one of the two prevailing Spread Spectrum (SS) technologies; DSSS or FHSS. A third alternative is to use very low output power, this is possible but impractical for most applications.

Today, two very different spread spectrum RF technologies for the 2.4 GHz WLANs are used. SS is a technique for spreading the signal over a wide range of the spectrum. By doing this, concentrating power in a single narrow frequency is avoided. Originally developed by the military, SS was used for reliable and secure transmissions. The technique is a trade off between bandwidth efficiency and reliability, integrity and security. If a receiver or an eavesdropper doesn’t know the parameters of the SS broadcast, the signal will look like background noise.

The IEEE 802.11b WLAN used DSSS. FHSS is not longer a common technology for WLAN but it is used by the Bluetooth standard. Since this paper is investigating in IEEE 802.11b and Bluetooth, the two corresponding Spread Spectrum technologies are explained in more detail below.

Direct Sequence Spread Spectrum (DSSS)
DSSS avoids excessive power concentration by spreading the signal over a wide frequency band. The transmitter maps each bit of data into a pattern of chips. The signal propagates at different frequencies in these chips to the receiver. At the receiver the chips are mapped back into a bit and recreated to the original data. For this technique to work, the transmitter and receiver must be synchronized. The ratio of chips per bit is called the spreading ratio. More
chips per bit, and thus a higher chip ratio will increase the resistance of interference. A low chip ratio increases the net bandwidth for the transmission. Virtually all manufacturers of 2.4 GHz products offer a spreading ratio less than 20. The proposed ratio in the IEEE 802.11b standard is 11.

Most IEEE.802.11b products in the market allow three DSSS channels in the same area. This is accomplished by separating the 2.4 GHz ISM bands into several non-overlapping sub-bands. Each of these bands contains an independent DSSS network.

**Frequency Hopping Spread Spectrum (FHSS)**

FHSS spreads the signal by transmitting a short burst on one frequency, “hopping” to another frequency for another short burst and so on. Like in DSSS, the transmitter and receiver must be synchronized, otherwise the signal will look like background noise. The *hopping pattern* describes which frequencies used and in which order they occur. The *dwell time* gives the time at each frequency. Both the hopping pattern and dwell time are restricted by most regulatory agencies. For example, the FCC, requires that 75 or more frequencies are used and a maximum dwell time of 400 ms.

FHSS allow much more channels in the same area than DSSS. This is accomplished by implementing separate channels on different, orthogonal, hopping sequences. There are a large number of possible hopping sequences in the 2.4 GHZ band which introduces the large number of non-overlapping channels.

**IEEE 802.11b Topologies**

The IEEE 802.11b standard defines two pieces of equipment, a wireless station, which is usually a PC or a Laptop with a wireless Network Interface Card (NIC), and an Access Point (AP), which acts as a bridge between the wireless stations and the Distributed Systems (DS).

Three basic topologies are supported in 802.11b WLANs; the independent basic service set (IBSS) or often called the Ad Hoc Mode, the basic service set (BSS), and the extended service set (ESS). The BSS and ESS are often called Infrastructure Mode. The MAC layer implements the support for all three configurations. See blow for more details of the different topologies and figure 2, which explains them.

![Figure 2. Different IEEE 802.11b WLAN topologies.](source: http://alpha.fdu.edu/~kanoksri/IEEE80211b.html)
**Independent Basic Service Set (IBSS) or Ad Hoc Mode**
IBSS (Ad Hoc) configurations are also referred to as an independent network. Logically, an IBSS configuration is analogous to a peer-to-peer office network in which no single node is required to function as a server. In IBSS, wireless stations can communicate directly with one another and generally cover a limited area. Every station may not be able to communicate with every other station due to the range limitations.

**Basic Service Set (BSS)**
BSS configurations rely on an AP that acts as the logical server for a single WLAN channel. While it may seem that the AP adds an unnecessary layer of complexity, it is actually necessary to perform the wired-to-wireless bridging function and connect multiple WLAN channels as it does in the ESS. All wireless stations communicate with the AP and all frames are relayed between wireless stations by the AP. See below for more about APs.

**Extended Service Set (ESS)**
ESS configurations consist of multiple BSS cells that can be linked by either wired or wireless backbones. The APs communicate among themselves to forward traffic from one BSS to another. This facilitates movement of wireless stations between different BSS, often called *roaming*, see below for more about roaming.

**Access Points (APs) and Roaming**
The main function of an AP is to form a bridge between wireless and wired LANs. It can also be used as a hub to connect wireless clients to a network. The AP bridge wired and wireless protocols and they control traffic as they buffer, transmit and receive data. An APs transmission radius is called a *microcell*. Today’s IEEE 802.11b APs can transmit data up to 500 feet (164 m) in an open environment (www.compaq.com). The range decreases in more build up areas with more obstacles. The best way to extend the range is to install more APs that operate in the same channel, this will also increase the capacity. Overlapping microcells create seamless access as the wireless stations roam from one microcell to another. Adding more APs in the same location will increase the number of simultaneously users in that area. Up to three overlapping channels can be used concurrently without interference.

In a setting with overlapping microcells (ESS), with different channels, wireless stations and APs frequently check the strength and quality of transmission. To accommodate roaming from one microcell to another the WLAN system hands off roaming users to the AP with the strongest and highest quality signal. In an ESS, wireless Network Interface Cards (NIC) and APs follow a series of steps to determine which AP should accept a hand-off between cell sites. This exchange is based on available bandwidth, traffic, signal strength and quality. When an adapter detects a signal getting weaker and another getting stronger it requests a switch and the new AP accepts a hand-off from the previous AP. The roaming procedure differs slightly in hardware from different manufacturers but the previous described technique is the most common one.

Wireless Network Interface Cards (NIC) acts as the interface between the client network operating system and the data arriving from an AP. With NIC, data coming from the WLAN is “transparent” to the client network operating system- this means the network operating system recognizes wireless data as it would recognize Ethernet data.
IEEE 802.11b Medium Access Control (MAC) Features

The MAC layer is a set of protocols that is responsible for maintaining order in use of a shared medium. The IEEE 802.11b MAC layer was developed to work seamlessly with standard LAN Ethernet to ensure that wireless and wired nodes are the same logically. Standard LAN Ethernet networks use Carrier Sense Multiple Access with Collision Detection (CSMA/CD). This technique doesn’t make any control of the medium before transmission, which is preferred when transmitting data over a well-trafficked medium like the air as in IEEE 802.11b.

IEEE 802.11b defines both a frame format and MAC scheme that differs from standard Ethernet. This frame format enables number of features such as fast acknowledge, handling hidden stations, power management, and data security.

Physical Carrier Sense Mechanism

The IEEE 802.11b standard uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). In this technique, each station listens to the medium before transmitting. If the medium is idle the station transmits, but if it is busy, each station must wait until transmission stops. When the medium gets idle from busy the receiver station of the previous communication session sends an acknowledgement (ACK) to all stations. After received the ACK, the sender have to wait a preset time plus a random number of time slots before trying to send again. This is done to avoid collisions over the medium.

Virtual Carrier Sense Mechanism

An assumption in the previous discussion is that every station can “hear” all other stations. However, this is not always true. In the Hidden-Node Problem, wireless stations A, B and C all can see, hear, and communicate with AP P. A and B can hear each other, and B and C can hear each other, but A and C can not hear each other. See figure 3 below.

![Figure 3. The Hidden-Node Problem and the 4-way RTS/CTS handshake protocol](http://alpha.fdu.edu/~kanoksri/IEEE80211b.html)

To handle the Hidden-Node Problem, the IEEE 802.11b standard specifies an optional Request To Send (RTS)/Clear To Send (CTS) four-way handshake protocol, see figure 3 above. This protocol reduces the probability of a collision at the AP. A wireless station that wants to transmit on the medium first sends a RTS message to the AP. The RTS message
should include the source, the destination, and the amount of time the desired transaction will take. If the medium is free (idle) the AP sends a CTS message to the wireless client. The CTS message includes the same information as the RTS message.

All stations, both receivers and transmitters, use both the Physical Carrier Sense Mechanism and the Virtual Carrier Sense Mechanism together to avoid collisions. The two techniques will together reduce the probability that that a “hidden” wireless station causes interference at the AP when the AP is communication with another wireless station that can’t see the hidden one. If the hidden station don’t hear the others station’s RTS message it will still hear the CTS message from the AP. The CTS message will inform the hidden station about the current situation, and it can continue in the Physical Carrier Sense Mechanism instead of sending a RTS that is going to be denied.

The MAC layer in IEEE 802.11b also supports a concept called fragmentation. The fragmentation concept gives the manufacturers some flexibility when designing APs and wireless stations, and can be useful in environments with dense RF interference. The 802.11b standard requires that all APs support fragmentation but leaves such support optional for wireless stations.

**IEEE 802.11b Security Aspects**

Because wireless is a shared medium, everything that is transmitted or received over a wireless network can be intercepted. Encryption and authentication are always considered when developing a wireless network system. The goal of adding these security features is to make wireless traffic as secure as wired traffic. The IEEE 802.11b standard provides a mechanism to do this by encrypting the traffic and authenticating nodes via the Wired Equivalent Privacy (WEP) protocol. The main goals of WEP are to protect from access to the wireless network by intruders using similar WLAN equipment and to protect from capture of WLAN traffic through eavesdropping.

The Shared Key Authentication, which is an authentication mechanism where a wireless station has to prove its knowledge of a certain key, solves protection against unauthorized access to the network. The authentication process is as follows:

1. A requesting wireless station sends an Authentication frame to the AP.
2. When the AP receives an initial Authentication frame, the AP will reply with an Authentication frame containing 128 bytes of random challenge text generated by the WEP algorithm.
3. The requesting wireless station will then copy the challenge text into an Authentication frame, encrypt it with a shared key, and then send the frame to the responding AP.
4. The receiving AP will decrypt the value of the challenge text using the same shared key, and compare it to the challenge text sent earlier. If a match occurs, the responding station will reply with an authentication indicating a successful authentication. If not, the responding AP will send a negative authentication.

The eavesdropping is blocked by using the WEP algorithm, which generates random numbers initialized by a shared secret key. The WEP algorithm releases a sequence of keys of random bits. These sequences are combined with the outgoing or incoming packets to produce an encrypted or decrypted version of the packets.
However, in August 2001 a group of experts announced they had succeeded in defeating the WEP security scheme. Since that publication, various hacker tools that exploit the vulnerabilities and weaknesses in WEP have appeared on public web sites. These softwares include tools for capturing encrypted packages over the wireless medium and tools to do a cryptanalysis and to decrypt the packages as well.

WECA has announced that a revision to Wi-Fi, named 802.11i, is under development, and may be ready for certification testing in 2002. WECA stands for Wireless Ethernet Compability Alliance. Its mission is to certify interoperability between Wi-Fi (IEEE 802.11b High Rate) products and to promote Wi-Fi as the standard. The Wi-Fi logo assures that the product has been tested to operate with products of different brands that are certified. It also guarantees that the product is working according to the standard (IEEE 802.11b).

In the meantime, WECA has published the WEP Security Statement as a list of best practices for corporate and individual users. The Statement may be found at http://www.Wi-Fi.com/pdf/20011015_WEP_Security.pdf and includes advice for users in both small and large environments. For smaller organizations, including home users, and for lesser-valued data, WECA recommends one or more of the following:

- Turn WEP on and manage your WEP key by changing the default key and, subsequently, changing the WEP key, daily to weekly.
- Password protects drives and folders.
- Change the default SSID (Wireless Network Name).
- Use session keys if available in your product.
- Use MAC address filtering if available in your product.
- Use a VPN system. Though it would require a VPN server, the VPN client is already included in many operating systems such as Windows 98 Second Edition, Windows 2000 and Windows XP.

For larger organizations, or where high security is required, the WECA statement provides examples of additional security methods.

**Power, Range and throughput in IEEE 802.11b**

The distance that Radio waves can propagate is a function of several different factors, for example; product design including the power of transmitter and receiver antennas, propagation path, interactions with obstacles along the propagation path which can change the energy of the signal etc.

WLAN typically reach distances from 150 to 150 meters, depending on the factors mentioned above. Wireless Wide Area Networks (WWAN) reach distances between hundreds to thousands of meters. However, the data rates are lower in WWAN than in WLAN and to reach the same distances like WWAN, the WLAN transmitter powers and receiver sensitivities have to be great, thus setting high demands on power supply from batteries or power cabling. They wireless stations used in WLAN cannot facilitate the amount of power needed for sending data at rates of 11 Mbps these distances, thus covering a smaller area.

The IEEE 802.11b standard provides speeds up to 11 Mbps with fallback levels on 5.5 Mbps, 2 Mbps and 1 Mbps. The standard defines dynamic rate shifting, which allows data rates to be
automatically adjusted to the fallback levels for noisy conditions. This means IEEE 802.11b devices will transmit at lower speeds, 5.5 Mbps, 2 Mbps, and 1 Mbps under noisy conditions. When the devices move back within the range of a higher-speed transmission, the connection will automatically speed up again.

In figure 4 below, differences in range and power consuming for WWAN, WLAN and Wireless Personal Area Networks (WPAN), which includes Bluetooth, are illustrated.

![Picture 4. Ranges and power consumption for WWAN, WLAN, and WPAN](http://www-106.ibm.com/developerworks/library/wi-phone/?dwzone=wireless)

### Bluetooth

Bluetooth is the name of a technology that uses short-range radio links. It was originally intended to replace the cable connecting portable and/or fixed electronic devices. The name Bluetooth originally is named after a Danish Viking and King, Harald Blåtand (Bluetooth in English), who lived in the latter part of the 10th century. Harald Blåtand united and controlled Denmark and Norway (hence the inspiration on the name: uniting many devices from different manufactures through Bluetooth).

L.M. Ericsson of Sweden invented Bluetooth in 1994. In February 1998 Ericsson founded a Special Interest Group (SIG) together with IBM, Nokia and Toshiba. The purpose of this SIG was to develop an open specification for short-range wireless connectivity. Since 1998 many other companies have joined the group. Currently there are over 2500 members in this group. By signing a zero cost agreement, companies can join the SIG and qualify for a royalty-free license to build products based on the Bluetooth technology.
Bluetooth is as mentioned a WPAN protocol designed to replace cables. Low cost, modest speed and short range (<10) are hallmarks for this technology. Bluetooth can support connection with up to seven devices at one piconet. A piconet is a small network of Bluetooth-enabled devices. Piconet topology consists of a single master and up to seven slaves. In a single piconet only one Bluetooth-device can transmit at a time. Therefore the master controls the piconet through a series of transmissions. When the master has something to transmit to the slaves it does so. When the master isn’t transmitting any information it constantly polls the slaves and listens to their answers. If a slave wants to transmit data it have to wait for the master to ask if the slave wants to transmit any data. The slave’s responses on the question can either be NULL for no information to transmit or they can begin transmission if they have anything to send.

Bluetooth operate in the unlicensed, 2.4 GHz radio spectrum ensuring communication compatibility worldwide. The physical layer uses frequency-hopping spread spectrum (FHSS) technique. Frequency hopping means the Bluetooth chip transmits and receives on 79 different hop frequencies that are 1 MHz wide, from 2402 to 2480 MHz. Switching between one hop frequency to another in a pseudo-random sequence, 1600 times a second. Thus, eventually, Bluetooth devices occupy 79MHz, but at any specific moment only 1 MHz is occupied. Each of these hops goes to a slot that is 625us long, (packets can last 1,3 or 5 slots, but the hop frequency remains the same for each packet). The hopping sequences allow multiple Bluetooth piconets (networks) to co-exist simultaneously.

**Power and range**

Bluetooth (BT) is basically a point-to-point service that is used to transmit very short distances. Bluetooth has become famous because for its small size and low cost (the price is now under 5$ a piece, which is a very important limit to get under in the industry if a technique shall be big) A very big asset of Bluetooth is that whenever another device comes into range the devices will automatically start to communicate with each other without the users acknowledge. Some people think that Bluetooth is a radio-frequented (RF) alternative to Infrared technology. The major difference is that Bluetooth don’t need any line-of-sight (LOS) and the RF can traverse through walls.

BT uses very small power for transmission in the network. The power range is expected to be 1-100mW and at that transmission power the maximum distance that devices can communicate is 100 m. This is what is planned for in the future with Bluetooth 2.0, which hopefully also will have a data rate up to 10 Mbps. Today Bluetooth transmitters only have a power at 1 mW and a range in the 10 m area.

**Network topology**

As mentioned earlier Bluetooth devices form overlapping networks called piconets. In each piconet there can be up to eight devices. Each unit can belong to several different piconets simultaneously, which allows many different users access to the device. A good example is a printer in an office.

By definition, the device that establishes and controls the piconets is called a master. Any other device in that piconet is called the slave (maximum 7 slaves in one piconet). Each piconet uses a slow hopping frequency with a pattern decided by the master.
Packets in the Bluetooth protocol (figure 5) contain three major fields. It’s the Access Code, Header and Payload.

- **Access Code**: Here does the master take care of synchronizing the network. Each device on the piconet is also identified here. The access code is unique to each piconet, so packets in the same piconet will have the same access code.

- **Payload**: Contains the data to be transmitted.

- **Header**: The header is used for link control and consists of six different fields that are mostly used for error control and data typing. Main fields in this header are the **AM_ADRR** and the **ARQN**
  
  o **AM_ADRR**: This field is used to identify the participating members of the piconet. Each device in the piconet is assigned a temporary 3 bit address by the master (the master has 000 and the resulting seven addresses are for the slaves). This address is used by the master to verify if a device is supposed to be on the specific network. Devices that leave the piconet gives up their address. This makes it possible for other devices to connect to the piconet.

  o **ARQN** is used to inform the source of successful transmission. This field is only used for a payload with data that has a CRC in it. Otherwise there would be no chance for the destination to decide if the data is correct or not. 1 in this field responds to successful transmission and 0 for error and retransmission request. Data is resent on the next available open timeslot.

![Figure 5](image)

Bluetooth is a full duplex protocol. The timeslot that Bluetooth uses for sending is 625 µs. The master transmits on even timeslots and the slaves are able to reply on odd timeslots. A single device can transmit a packet over a maximum of five timeslots. Each packet is transmitted on one of the hopped frequencies and stays constant in that frequency during transmission.

Data packets in Bluetooth are broken into two types.

- **Synchronous Connection Oriented (SCO)**
  SCO is used for synchronous data, such as voice. The connection is established by the master sending a SCO setup message. Once the slave responds, the connection is a point-to-point link. A master can only handle 3 SCO links to one slave (or three different slaves). Also slaves can handle only three SCO links. This allows different users to share the same synchronous data at the same time.
  In SCO packets are never resent.

- **Asynchronous Connection Less (ACL)**
The ACL link is a packet switched connection sent between the slots allocated for SCO data. There can only be one ACL connection between the master and the slave. The packets can be resent via ARQ just like in ordinary wired LANs.

Examples of different packets are NULL, POLL, DM1, DM2, DM3, HV1, HV2 and DV. The NULL and POLL packets are used to get link and network information. The DV packet is a combined Data and Voice packet, which automatically makes it to a SCO packet.

The data rate for SCO is at the moment 432 kbps and for the ACL 721 kbps.

**Security Aspects in Bluetooth**

The security aspect of wireless communication is a very important question. Bluetooth implements what is called the E1 algorithm. This algorithm is based on a Challenge/Response the master will challenge the new device. The device responds with another challenge in relation to the first challenge. The Challenge/Response is done in the BD_ADDR bits of the header. The BD_ADDR bits are used in Bluetooth to determine who or what is on this link and is also the IEEE802.11b standard address of each Bluetooth device. There are also authentication bits and 8-128 bits of encryption algorithm. Finally there is the random key of 128 bits. The encryption bits are regenerated whenever encryption changes. The authentication bis are set up at setup of two devices and will only change when a device gives up its AM_ADDR address. All this is used to authenticate a device. Once a device is authenticated, the master will send information about the piconet.

There are two security levels used by a device. Trusted Device (a device that is paired with another device and has unrestricted access to all the services) and the Untrusted device (a device with no pairing with another device that has limited access to services, or a temporary connection used for ‘passing by’).

The data sent between two devices is also encrypted. The header and Access code are never encrypted. This would make it impossible for devices to communicate. The encryption algorithm is E0 and consists of three parts. One part for initialization and one part for encryption and decryption.

**Bluetooth versus IEEE 802.11b WLAN**

There have long been speculations about, not just technical interference, also whether Bluetooth and IEEE 802.11b are in competition with each other or not. During 2000 and the initial part of 2001 Bluetooth was seen as a leading wireless technology capable of replacing wired networks. This made people think that Bluetooth was trying to become a WLAN contender.

Lately people have started to realize that IEEE 802.11b and Bluetooth are designed for different roles. There is no point trying to force one technique to do what the other is better suited to do. Bluetooth is designed for quick, seamless short range networks and features better power consumption, small protocol stack, robust data and voice transfer. These features make Bluetooth well suited for WPAN. IEEE 802.11b is designed for infrequent mobility, IP-based data transmission, medium range and high data rate. All these features make IEEE 802.11b idealistic for WLAN. IEEE 802.11b would be a very clumsy, expensive and power hungry
alternative for WPAN. When we have decided that Bluetooth shall be used to WLAN and 802.11b shall be used to WLAN, a question arises. Can they work together?

**Differences**

The major difference between the two technologies is the data rate. Bluetooth has a maximum rate of 1 Mbps (721 kbps) compared to IEEE 802.11, that runs at up to 11 Mbps. The difference in the rates lies in the Physical and Data Layers. The output power of Bluetooth is 1 mW compared to WLAN with 1 W. Also the range differs a lot. Bluetooth devices have a maximum range of 10 meters compared to IEEE 802.11b:s 300 meters. Also the modulation technique differs. Bluetooth uses GFSK (Gaussian Frequency Shift Keying) as opposed to CCK (Complementary Code Keying) in IEEE 802.11b. This leads to different transmission types. Bluetooth uses frequency hopping while IEEE 802.11b uses DSSS. Frequency hoping could cause delays in the transmission and the only way to prevent this is to slow down the information exchange. Therefore the hop frequency is constant during transmission of a packet. But, when larger packets are transmitted it could be spread out over a maximum of five timeslots. In the DSSS (Direct Sequence Spread Spectrum) case, the CDMA allows the signal to be spread out over a large frequency and make all other users look like noise to the destination. The number of devices that can be connected with IEEE 802.11b does not have any hard limit like Bluetooth (1 master and 7 slaves).

Another difference is the usage of the techniques. Bluetooth is being used device to device data transfer, which allows devices as PDAs, cellular phones, printers etc. to talk to each other on the fly. IEEE 802.11b has become more of an access point for a computer to get on wired backbone. The security aspect of the techniques is different. Bluetooth uses a combination of 4 LFSR’s (Linear Feedback Shift Registers) to encrypt data at the Physical layer. Also the very high frequency hoping rate aids in keeping data secure. In IEEE 802.11b the access points act as a hub in a wired network, and thus don’t have much security on the Physical layer. The problem is that the hubs send all packets to every user in the network and if data isn’t meant for that computer, it simply discards the packet. This is a big security issue. It’s easy to listen to the traffic in a wireless network. There is an optional encryption capability that implements RC4 security algorithm in the Data layer.

**Similarities**

Both techniques are wireless network topologies. Similarities at the Physical layer are that they both operate in the 2.4 GHz ISM band. They are both able to create ad-hoc networks. The second similarity is that they both connect electronic devices without wires, but Bluetooth mainly connects devices as PDAs, cell phones etc and 802.11b are used to connect networks. There are not that many similarities, which mean that the techniques are more complementary than adversary to each other.

**Bluetooth and IEEE 802.11b Co-existence factors**

Both Bluetooth and IEEE 802.11b transmit as mentioned earlier in the 2.4 GHz ISM range. The question is if they cause interference with each other?
Yes they DO cause interference, which increases as they approach on another, but both technologies are designed to handle interference. The Bluetooth uses the FHS, hoping between 79 frequencies (all 1 MHz each) at a rate of 1600 hops/s. The timeslots are 625 µs. IEEE 802.11 defines 11 possible channels that may be used. Channel hops also occur but 600 times slower than Bluetooth. Each channel has a center frequency. The center frequencies are 5 MHz from each other. Occasionally devices from the two techniques hop to the same frequency. This results in reduced throughput and that packets get lost. This interference isn’t as bad as first feared. In extreme conditions where a Bluetooth and IEEE 802.11b device interfere is positioned right beside to a receiver of the opposite technology, throughput is significantly reduced. When the distance is increased, such as 10 meters between the devices, throughput is only minimally reduced.

One interesting thing to note is that Bluetooth will cause more interference with IEEE 802.11b than the other way around. The explanation is that while a IEEE 802.11b device is transmitting on a particular frequency, a Bluetooth device will probably hop to this frequency several times before IEEE 802.11 hops to the next frequency. Another thing is that the size of the packets is bigger in IEEE 802.11 than Bluetooth, which means that IEEE 802.11b looses more data when a packet is lost compared to Bluetooth.

A basic technique behind enabling Bluetooth and IEEE 802.11b to Co-exist is to ensure Bluetooth and IEEE 802.11 devices located near each other never use the same frequency at the same time. Additionally a more complex method of adaptive reservation could be used to maximize throughput by resolving conflicting reservations to ensure both devices avoid long traffic delays and to take into account the fact that one device may be busier than the other. This would ensure that a Bluetooth/802.11 chipset would be able to function almost seamlessly side by side and thus maximize the potential of the wireless device using the joint chipset. IEEE has formed The IEEE 802.15 Coexistence Task Group. This group is developing recommended practices for coexistence of wireless PANs (Personal Area Networks) that operate in the 2.4 GHz frequency spectrum, and they've done preliminary analysis of the interference potential between 802.11 and Bluetooth. In addition, the group has made preliminary recommendations on how to solve the problem with interference.

**Conclusion**

Many people think that Bluetooth and IEEE 802.11b are competitive technologies. As we have seen in the paper the two technologies have in fact really different end-user scenarios and could both add something to the wireless market. Bluetooth and IEEE 802.11b have distinct applications. If you are a laptop computer user with a need to access corporate networks or if you have a need for high performance, IEEE 802.11b is the way to go. But if you need the lowest cost with less range and less speed solution for a wide range of devices, then Bluetooth is the clear choice.

Co-existence and simultaneous operation between the two techniques is a highly desirable goal. Both techniques are expected to grow rapidly over the next few years, offering users completely wireless communication. The main question for us was to investigate in whether Bluetooth and IEEE 802.11b can physically live with each other. As mentioned in the report interference occurs, which leads to decreased throughput. However, actions are although being made to reduce interference to negligible effects.
We are sure that this problem will be solved in the future and IEEE 802.11b and Bluetooth will be able to co-exist without any interference at all. We have also found out the difference in the usage of the two techniques and we that Bluetooth and IEEE802.11b are complements, not competitors.

**Sources**

http://www.barcode.co.th/select.html
http://www.wlana.com
http://www.80211-planet.com
http://www.proxim.com
http://www.nipc.gov/publications/nipcpub/bestpract.html
http://developer.intel.com/technology/itj/q22000/articles/art_5.htm
http://www.wi-fi.net/downloads/weca80211boverview.pdf
http://www.palowireless.com/bluearticles/cc4_bluetooth80211b_part1.asp
http://www.palowireless.com/bluearticles/intro.asp
http://www.ausystem.com/servlet/PSPDownloadServlet?iPublicationId=69
http://www.howstuffworks.com/bluetooth.htm
http://www.hut.fi/~joraskur/BT2.pdf
www.wlan-forum.com