Indoor WLAN Design

Part I: Using IEEE 802.11b Standard Devices

Kjell Jørgen Hole and **Trond Davidsen**
NTNU, UiB

Last updated 15.11.02

Outline

- IEEE 802.11b wireless communication standard
- How to position base stations to
  - obtain **full radio coverage** of target area, and
  - **avoid interference** problems
- How to connect base stations to a wireline network such that mobile stations may **roam** the network
- Access control

Wireless Network Devices

MS *Mobile Station*—Mobile communication device containing a radio transceiver

BS *Base Station*—Fixed radio transceiver acting as an interface between the wireless network and the wireline (core) network. The BS is also called an *access point*

Bridge A bridge joins two networks at the hardware level. Other protocols see the two networks as the same. A BS is set up as a (layer 2) bridge between the wireless network and the wireline network

IEEE 802.11b MS

Figure 1 A laptop computer can become an MS by installing a PCMCIA card implementing the IEEE 802.11b standard. The above card is made by Apple

IEEE 802.11b BS

Figure 2 This an AirPort BS made by Apple. AirPort implements the IEEE 802.11b standard

IEEE 802.11b Communication Standard

- Direct Sequence Spread Spectrum (DSSS) in 2.4 GHz Industrial, Scientific, and Medical (ISM) band
- DSSS spreads the signal over a bandwidth of about 22 MHz, allowing transmissions to be robust against interference
- European regulators cap maximum radiated power at 100 mW
- 1 Mb/s, 2 Mb/s, 5.5 Mb/s, or 11 Mb/s gross data rate depending on wireless link quality

IEEE 802.11b Standard (cont.)

- A BS and MS has a range from 20 m to more than 300 m, depending on the specific implementation and operating environment
- Carrier Sense Multiple Access (CSMA) with Collision Avoidance (CA) medium access scheme is discussed in Part III

IEEE 802.11b—Channels

- BSs and MSs transmit on different radio frequencies, called **channels**
- Standard defines 14 channels
- Only 11 channels are used in the U.S.
- Can use 13 channels in Europe. Have BSs that support all channels

More on Channels

- Since many 802.11b PCMCIA cards cannot access channel 12 and 13, most wireless networks use channels 1 through 11
- A channel is selected for a BS when it is set up
- An MS automatically tunes to the channel used by the BS

Remark: Note that there is only 5 MHz separation between the channel center frequencies, and that an 802.11b signal occupies approximately 22 MHz of the frequency spectrum

IEEE 802.11b—Nominal Throughput

Nominal peak throughput offered to the IP layer for a Maximum Transmission Unit (MTU) of 1500 bytes.

Bit rate (Mb/s)	Nominal throughput (Mb/s)
11	6.2
5.5	3.9
2	1.7
1	0.9

IEEE 802.11b—Error Control

- Lucent WaveLAN IEEE 802.11b networking card* utilizes an Automatic Repeat Request (ARQ) scheme with maximum four retransmissions

- No Forward Error Correction (FEC) is used

*This card is also denoted the Orinoco Silver Card. It is embedded in Apple's first generation AirPort base stations. The "marketing friendly" name Wi-FI is used to refer to 802.11b-compliant networking cards

UDP Performance over IEEE 802.11b links

The User Datagram Protocol (UDP) is a connectionless transport protocol for real-time traffic. Retransmissions are not used (Lucent WaveLAN IEEE802.11b may cause up to four retransmissions)

Measured UDP throughput over 10.000 packets

Bit rate (Mb/s)	Payload (bytes)	Good channel throughput (Mb/s)	Bad channel throughput (Mb/s)
	1500	6.071	1.259
	1024	5.001	1.2
11	768	4.206	1.293
	512	3.172	1.548
	256	1.763	0.999

TCP Performance over IEEE 802.11b links

The Transport Control Protocol (TCP) provides reliable connection-oriented service between two hosts with support for flow and congestion control as well as error recovery

Measured TCP throughput

Bit rate (Mb/s)	Test	Throughput (Mb/s)
	1	2.906
	2	0.707
11	3	4.488
	4	0.501
	5	4.586

WLAN Requirements and Design

- The Wireless Local Area Network (WLAN) must have
  - complete radio coverage of target area
  - network capacity to carry the expected load
- The requirements can be met by using a proper combination of
  - **BS locations**
  - **channel (frequency) assignments**

Transmission Barriers

- Wood, plaster, and glass are not serious barriers to radio transmissions, but brick and concrete walls can be significant ones
- Metal, such as in desks, filing cabinets, reinforced concrete, and elevator shafts are great obstacles to radio transmissions
- Typical transmission ranges up to 300 m in an open environment, but this range may be reduced to 20–60 m through walls and other partitions

Measurements are Needed

- The BS layout must be based on measurements, not just on "rule of thumb" calculations
- Extensive testing and careful consideration of radio propagation issues are needed when the intended coverage area is large
- *Indoor measurements can be particularly challenging because a building constitutes a three-dimensional space*
- A BS located on one floor provides signal coverage to adjacent floors

Channel Interference

Co-channel interference is caused by devices transmitting on the same channel

Interchannel interference is caused by devices transmitting on adjacent channels

Both co-channel and interchannel interference may severely limit the transfer rates of a wireless network

Design Approach

- Space the BSs as far apart as possible while ensuring complete radio coverage. This approach will help reduce the co-channel interference and the cost of equipment and installation
- *Single-floor network:* Use only channels 1, 6, and 11 to avoid nearly all interchannel interference
- *Multi-floor network:* Use channels 1, 4, 7, and 11 to limit interchannel interference

Design Approach (cont.)

- Single-floor network:
  - Assign channels 1, 6, and 11 such that no two adjacent BSs use the same channel (see Figure 3)
- Multi-floor network:
  - Assign channels 1, 4, 7, and 11 such that no two adjacent BSs use the same channel
  - Make sure that closely spaced BSs do not use adjacent channels, i.e., do not use channels 1 and 4

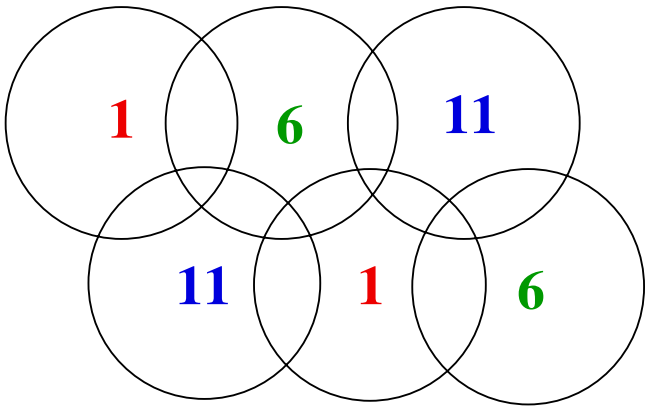

Figure 3 Channel assignment causing no interference

High-Density User Areas

- The design must also consider service to areas with high and low densities of users
- Most areas will be low-density (user) areas. However, classrooms and lecture halls will be high-density areas with high concentrations of students
- A good design approach is to use up to three BSs with different channel frequencies to cover the same high-density area

Design Procedure

1. Initial selection of BS locations
2. Adjust the BS locations based on signal strength measurements
3. Create coverage map
4. Assign channel frequencies to BSs using the coverage map

Simplified Design Example

- The coverage volume of a single BS may be represented by three coaxial cylinders, as depicted in Figure 4

- The radius of each cylinder is such that nearly all MSs may communicate with the BS

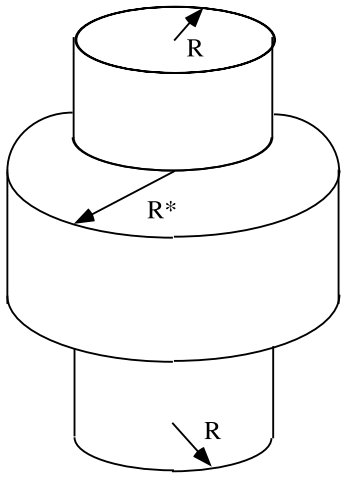

Figure 4 Idealized BS coverage. The middle cylinder, representing the coverage on the floor on which the BS is located, has radius R^*. The upper and lower cylinder, representing the adjacent floors, have radius $R < R^*$

Simplified Design Example (cont.)

- The object consisting of the three cylinders moves about as the location of the BS is changed

- The placement of the BSs within a building can be viewed as the problem of locating the cylindrical shapes such that the building space is filled and such that the shapes overlap as little as possible

Network Communication Techniques

Roaming Multiple BSs can be set up to create a single wireless network. An MS is able to **roam** the network when it can move from BS to BS with no interruption in service

DHCP Dynamic Host Configuration Protocol—Method of automatically assigning network parameters including

- MS's own IP address
- IP address of default Internet gateway (for outgoing packets)
- IP address of local DNS (Domain Name Server)

Setting up a Wireless Network for Roaming

1. Connect all BSs to the same physical subnet on Ethernet network (i.e., all BSs connect to the same router)

2. Give the same "network name"

3. Set up the BSs as bridges

4. To optimize performance, set the BS density to *High*, *Medium*, or *Low* depending on how far apart the BSs are from each other

Why Roaming is Possible

- DHCP server on Ethernet subnet provides IP addresses to MSs

- An MS retains its IP address when it moves from one BS to another BS

- Tables in BS bridges defining active MSs are updated when MSs move between BSs ("hand off")

The roaming protocol is not defined in the 802.11b spec, so each manufacturer has implemented their own method. This means that hand-offs between BSs of different manufacturers aren't possible

Setting BS Density

- The wireless network performance can be improved by setting BS density

- The setting tells MSs that are in motion to look for and switch to a new BS's signal when the signal strength of the BS it is connected to goes below a certain level

Example: In a high-density (user) area where the BSs are close together, setting BS density to High achieves higher transfer rates by forcing an MS to look for a new BS when the signal of the BS it is connected to goes below 11 Mb/s

Setting BS Density (cont.)

The following "rule of thumb" assignments indicate how to set the BS density:

Max distance between BSs	30m	60m	120m
BS density setting	High	Medium	Low

802.11b Access Control

The BS controls access to the wireless network using

MAC address filtering —An MS attempting to access a wireless network must have its MAC (Medium Access Control) address listed in tables contained in the BSs

Closed network —The MS must specify the "name" of the wireless network to associate with a BS

These techniques are only useful for small private networks with few BSs and a MSs

WEP—802.11b Encryption

WEP *Wired Equivalency Privacy*—A form of encryption that encrypts packets at the MAC layer. Only MSs with the "secret key" can associate with a BS

- any MS without the key may be able to see network traffic, but every packet is encrypted
- since the encryption takes place at the data link layer, only the wireless link is protected
- all MSs use the same key and can therefore decrypt each others packets

What is VPN?

- A **Virtual Private Network** (VPN) uses authentication and/or encryption to connect users to a private network over a public network, usually the Internet (see **www.vpnc.org** for more info)

- VPN is often based one the Point to Point Tunneling Protocol (PPTP) made by Microsoft

Wireless VPN

- When an MS first connects to a BS:

  1. the MS receives a "private" IP address from DHCP server

  2. the MS connects to a VPN server using the private IP address and transmits the user's login name and password

  3. the VPN server verifies the login name and password and returns a "real" routable IP address

Wireless VPN (cont.)

- All outgoing traffic from the MS passes through a PPTP tunnel to the VPN server which transmits the traffic to its final destination. The return traffic is first received by the VPN server and then transmitted through the PPTP tunnel to the MS

- A VPN client must be installed on the MS. There exist VPN clients for many different operating systems

Conclusions

- It may be difficult to set up an indoor wireless network with multiple BSs. Extensive measurements and testing are needed when the desired coverage area is large

- Access control must be implemented

- The information rate per user is no more than 4–5 Mb/s