Wireless 802.11b Networks

Introduction to Network Design and Security

Kjell Jørgen Hole

Outline

- Part I—802.11b wireless networks:
  - the IEEE 802.11b communication standard
  - introduction to network design
- Part II—Security in 802.11 networks:
  - possible attacks
  - some common security techniques
  - introduction to the new security standard, WPA

Part I—802.11b wireless networks

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

Figure 1 A laptop computer can become an MS by installing a PCM-CIA 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

DHCP

- All BSs and MSs get IP addresses from a DHCP (Dynamic Host Configuration Protocol) server on the wired network when BSs are set up as bridges

- Note that a BS may also contain a DHCP server. This server can deliver IP addresses to the MSs, as well as other devices on the wired network

!!! Remember to turn off the DHCP server on all BSs if there is a DHCP server on the wired network

802.11b 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 Mbps, 2 Mbps, 5.5 Mbps, or 11 Mbps gross data rate depending on wireless link quality

Nominal Throughput

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

Bit rate (Mbps)	Nominal throughput (Mbps)
11	6.2
5.5	3.9
2	1.7
1	0.9

UDP Performance over 802.11b links

The *User Datagram Protocol* (UDP) is a connectionless transport protocol for real-time traffic

Measured UDP throughput over 10.000 packets

Bit rate (Mbps)	Payload (bytes)	Good channel throughput (Mbps)	Bad channel throughput (Mbps)
	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

More on the 802.11b Standard

!!! Note that the throughput of 1–6 Mbps is the total available data rate for *all* MSs connected to the same BS

- A BS, or an MS, has a range from 20m to more than 300m, depending on the specific implementation and operating environment

- Utilizes the *Carrier Sense Multiple Access* (CSMA) with *Collision Avoidance* (CA) medium access scheme

  – similar technique used on wired Ethernet

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

!!! 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

Requirements and Design

- The 802.11b wireless network 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 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 300m in an open environment, but this range may be reduced to 20–60m 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

Remark: Both co-channel and interchannel interference may severely limit the throughput of a wireless network

Common 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*: What can we do when there are only three channels without interchannel interference?

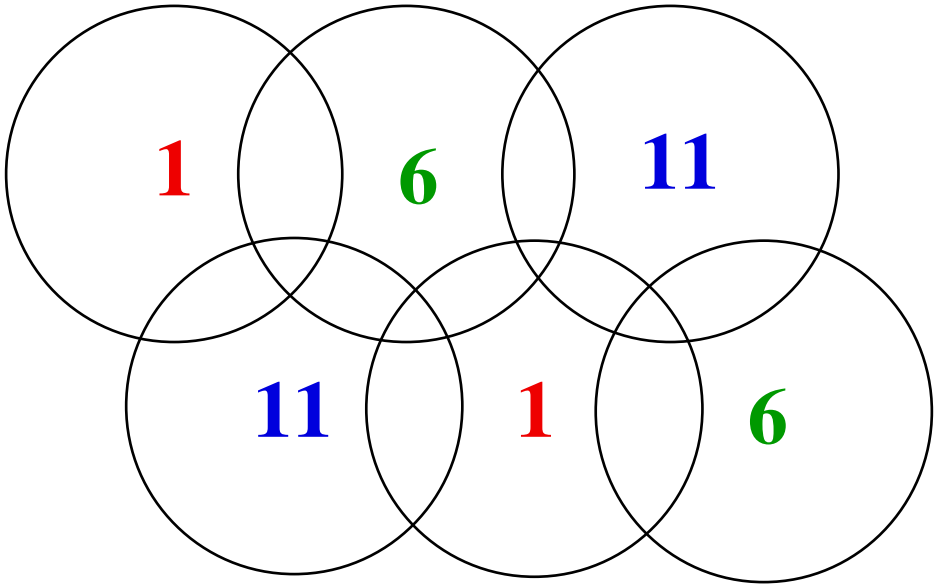

Figure 3 Channel assignment causing no interference in *single-floor* networks

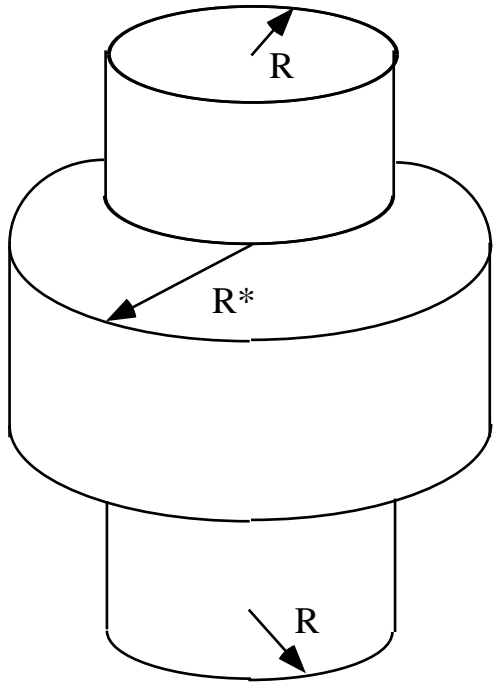

Figure 4 Idealized BS coverage. The middle cylinder, representing the coverage on the floor on which the BS is located, has radius R^*. The upper and lower cylinder, representing the adjacent floors, have radius $R < R^*$

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

Part II—Security in 802.11 networks

Denial-of-Service Attacks

Denial-of-Service (**DoS**) attacks aim to prevent access to network resources by flooding the network with traffic choking the transmission lines. DoS attacks can target different layers of the network

- *Application layer*: Large amounts of requests are transmitted to a network-aware application, e.g. a web server, swamping the server process. The goal is to prevent other users from accessing the service

Another DoS Attack

- *Transport layer*: Many connection requests are sent to a host. The attack is targeted against the operating system of the victim's computer. A typical attack involves sending an excessive number of TCP connection requests

- **Remark**: At the application and transport layers, there is nothing fundamentally different between DoS attacks on wireless and wired networks. The same is not true for the *network*, *data-link*, and *physical layers*

802.11 Physical DoS Attacks

- Attacker can be outside building containing 802.11 network
- Possible to create device that saturates the 802.11 frequency bands with noise and reduce the *signal-to-noise ratio* to an unusable level
- The attacker may also use common commercial devices:
  - 2.4GHz cordless phones
  - large scale Bluetooth deployments

802.11 Data-Link DoS Attack

- MSs are programmed to connect to the BS with the strongest signal
- It may be possible for an attacker to install a "malicious" BS with the correct SSID (network name)
- If the "malicious" BS has the strongest signal, then an MS will connect to this BS
- A signal amplifier or directional antenna may be used to create a very strong signal

802.11 Network DoS Attack

- Since an 802.11 network is a *shared medium*, a malicious user can flood the network with traffic, denying access to users associated to the affected BS

- As an example, an attacker can generate a ping (ICMP) flood to saturate the BS

- Given the relatively slow speed of 802.11 networks, a network DoS may happen due to large file transfers or bandwidth-intense applications

Eavesdropping

Eavesdropping Occurs when a nearby attacker can receive the radio waves from a nearby network and reconstruct the frames. All frames can then be examined in real time or stored for later examination

!!! Because the original 802.11 WEP encryption has several flaws, it can be cracked. A user who accesses his mail using the POP or IMAP protocols is then at risk because these protocols often pass the mail over the wireless network without any form of extra encryption

Manipulation

Manipulation Occurs on a wireless link when an attacker

1. is able to receive the victim's encrypted data, manipulate it, and retransmit the changed data to the victim. The attacker may change emails, instant messages, or database transactions

2. intercepts packets with encrypted data and is able to change the destination address to forwarded the packets across the Internet. While the data is encrypted on the wireless link, the received data over the Internet is decrypted

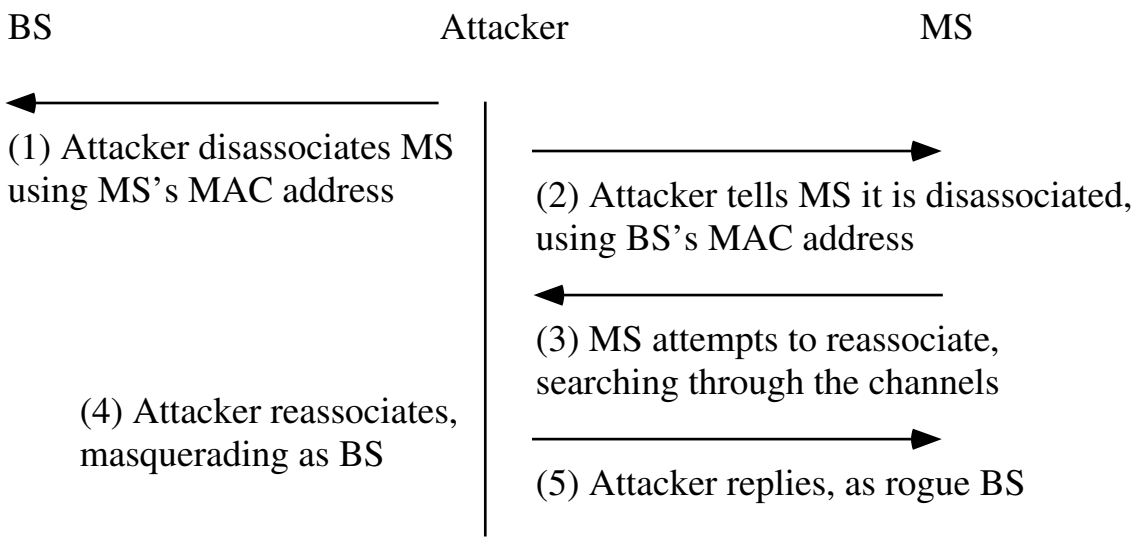

Figure 5 Rogue BS

MS Access Control

- **Prevent access to MS** through the use of a *firewall* on the MS
  - monitors all data going in or out of your computer
  - blocks any suspicious attempts to access your computer
  - provides software switches that block network sharing
- Firewall software is available from a number of companies and is built into some operating systems

Upper Layer Tunnels: SSL and SSH

- *Secure Socket Layer* (**SSL**) is a public-key, cryptography-based confidentiality mechanism
  - used in HTTPS to enable secure access to web pages
  - used by some mail clients (POP3 or IMAP over SSL)
- *Secure Shell* (**SSH**) is a secure replacement for *rlogin*. SSH utilizes public-key cryptography like SSL, but does not rely on a trusted authority to issue the public/private key pairs

BS Access Control

The BS controls access to the wireless network using:

Closed network —BSs do not broadcast SSID in the Beacon frames. Hence, an MS must specify the "name" of the wireless network to associate with a BS

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

Closed network and MAC address filtering are not part of the 802.11 standard. However, these techniques are implemented by vendors

Do Not Trust Closed Networks

- The SSID is broadcast in the clear by MSs wanting to join the network

- An attacker only has to sniff packets waiting for a probe request containing the SSID

Do Not Trust MAC Filtering

- The MAC address is broadcast in the clear with each frame, even when WEP is enabled
- Many wireless cards allow the MAC address to be changed by the user
- The change can be made via the driver GUI in Windows or *ifconfig* in Linux/BSD

Alternative: Captive Portal

- A captive portal is a router or gateway host that will not allow traffic to pass until *authentication conditions* are met. The operation of a portal is:

  1. Assign a new MS on the network an IP address through DHCP
  2. Block traffic, except to the captive portal server
  3. Redirect any web traffic to the captive portal
  4. Display terms of use and/or login screen
  5. Allow access after user has accepted terms and/or logged in

Closed and Open Portals

Closed Portal Used to limit the access to a known set of users with user names and passwords

Open Portal Requires acceptance of terms before access is granted

- The *NoCat* portal (`http://nocat.net`) supports both closed and open modes. When running in closed mode *NoCat* uses encrypted communications with a central authentication server to validate passwords

- The *NoCat* server at The Department of Informatics, UiB runs in closed mode

Disadvantages of Portals

- Each time a laptop is turned on, the web browser must be loaded before a new connection can be established
- The web browser must run in the background at all times
- It is difficult to keep the connection alive on some platforms

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 `http://www.vpnc.org`)

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

- PPTP may be used to set up an encrypted connection over TCP/IP links, typically between a person and his home office

  – PPTP also supports several authentication protocols

Disadvantages of VPN

- A VPN client must be installed on the MS
- Because interoperability between vendor's VPN products is not assured, you must buy server and client software from the same company
- VPN clients can sometimes be intrusive, slowing down communication
- If you have many VPN users, then you need a high-capacity VPN server

Security Needs

- Needed security mechanisms:
  - **Authentication** Who are you?
  - **Access control** Should you be allowed to access the network?
  - **Key management** Distribution and protection of secret keys
  - **Message privacy** Protecting the data
  - **Integrity** Preventing modification and insertion

!!! The initial 802.11 security, called WEP, fails to provide any of the above security mechanisms

WPA Overview

WPA *Wi-Fi** *Protected Access*. Specification of security enhancements that provide *authentication*, *access control*, *message integrity*, *message privacy*, and *key management* for existing 802.11b systems

- applicable for both home and enterprise users
- designed to run on existing hardware as a software upgrade
- forward-compatible with the upcoming 802.11i standard

*Another name for 802.11b compliant devices

Improved Authentication and Access Control

- To improve user authentication and access control, WPA implements the IEEE **802.1x** standard for port-based access control and the *Extensible Authentication Protocol* (**EAP**)

- This framework utilizes a central authentication server, such as RADIUS (Remote Authentication Dial-In User Service), to authenticate each user on the network before they join it

- *Mutual authentication* is employed so that the wireless user does not accidentally join a rogue network

WPA Layers

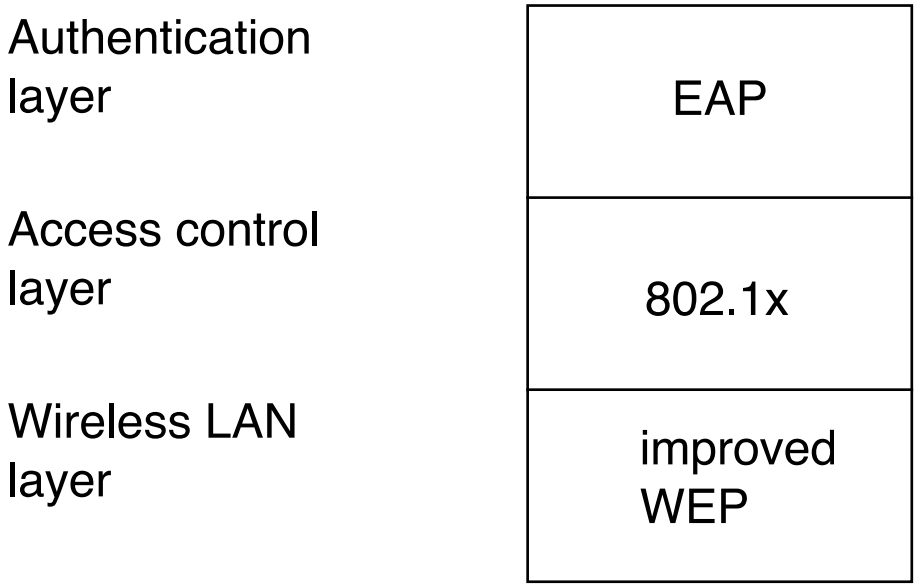

Figure 6 WPA security layers

What is Missing from WPA?

- WPA is a subset of the current IEEE 802.11i draft standard
- The main pieces of the 802.11i draft not included in WPA are
  - secure IBSS (Independent Basic Service Set)
  - secure fast handoff
  - secure de-authentication and disassociation
  - enhanced encryption protocols

Initial Analysis of WPA

- V. Moen, H. Raddum, and K. J. Hole, Weaknesses in the Temporal Key Hash of WPA, submitted to Mobile Computing and Communications Review, Aug. 2003

!!! Have shown that given two packet keys it is possible to find the temporal (session) key. The attacker can then do anything the legitimate user can do for the duration of the temporal key

Conclusions

- It is difficult to set up indoor multi-floor networks with many BSs. *More efficient design techniques are needed*

- *A thorough analysis of the new WPA security standard is badly needed*

  – do not rely on WEP encryption, there exist programs to crack keys

Talk available at

Wi-Fi short course at www.kjhole.com