Wireless Security Protocol Analysis and Design
Wireless Networks

1. WIRELESS NETWORKS
1. WIRELESS NETWORKS

- 1.1 WiFi 802.11
OSI Structure

Upper layers

Data link layer

Physical layer

802.2 Logical Link Control (LLC)

802.2 MAC

802.11 MAC

802.11 PHY

802.11a PHY

802.11b PHY

802.11g PHY

802.2 PHY

802.5 PHY

802.2 PHYS

802.5 PHYS

802.11 PHY (DSSS)

802.11 PHY (OFDM1)

802.11 PHY (HR/DSSS)

802.11 PHY (HR/OFDM2)
Infrastructure Networks

- BSS: Basic Set Service
- ESS: Extended Set Service
Ad Hoc Networks

• IBSS: Independant Basic Set Service
• Peer-to-peer connections between stations
• The distribution services are:
  – **Association**: when a station enters a new BSS, it establishes an association with the AP of this BSS, and if it is authenticated, can send and receive data via this AP
  – **Dissociation**: can be used by either a station or an AP
  – **Reassociation**: it enables a station which already has an association with an AP to move from this AP to another one.
  – **Distribution**: determines how frames have to be routed to an AP. If the destination is local, we can send the frames directly. If not, they have to be transmitted via the wire network.
  – **Integration**: if a frame has to be routed through a network not using 802.11, this service does the translation
• The Intracell services are:
  - *Authentication*: used to establish the identity of others stations
  - *Authentication cancelling*: when a station wants to leave its network, its authentication is cancelled.
  - *Privacy*: it prevents the content of messages from being read by anyone other than the intended recipient.
  - *Data delivery*
### WiFi standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>Wi-Fi 5</td>
<td>High Bandwith (54 Mbit/s théoriques, 30 Mbit/s réels)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Frequency band :5 GHz.</td>
</tr>
<tr>
<td>802.11b</td>
<td>Wi-Fi</td>
<td>The most common</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Theorical bandwith 11 Mbit/s (6 Mbit/s real)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Up to 300 meters if no barriers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Band : 2,4 GHz with</td>
</tr>
<tr>
<td>802.11f</td>
<td>Roaming</td>
<td>Enable the user to change his or her AP when moving, thanks to the Inter-Access point roaming protocol.</td>
</tr>
<tr>
<td>802.11g</td>
<td></td>
<td>High Bandwith (54 Mbit/s,26 Mbit/s real) on the band of des 2,4 GHz.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Devices using 802.11g can still work existing networks (most commonly 802.11b devices)</td>
</tr>
<tr>
<td>802.11i</td>
<td></td>
<td>This standard aims at improving security on wireless transmissions, thanks to the Advanced Encryption Standard (see §2 for more information about security)</td>
</tr>
<tr>
<td>802.11n</td>
<td>WWiSE (World-Wide Spectrum Efficiency)</td>
<td>This is a new technology (april 2007), which should provide 540 Mbit/s (the real bandwith is 100 Mbit/s within a 90 meters area)</td>
</tr>
</tbody>
</table>
CSMA/CA

Radio networks:

=> hidden station
=> exposed station problem
CSMA/CA

- Sender transmits short RTS (request to send) Packet

- Receiver replies with short CTS (clear to send) packet

- Hidden nodes will not transmit for specified duration: NAV
802.11 supports three types of frames: management frames (00), control frames (01) and data frames (10).
Management frames are used for station association, disassociation, timing and synchronization, authentication and desauthentication.
Control frames are used for handshaking and positive acknowledgments during the data exchange.
Data frames are used to exchange data.
Current Issues and Challenges

- Security
- Interference
- Quality of Service
- Mobility
1. WIRELESS NETWORKS

• 1.2 WiMax - Worldwide Interoperability for Microwave Access
Why?

- Different environments:
  ⇒ 802.11 has to deal with mobility
  ⇒ 802.16 mostly connects buildings

- 802.16 covers bigger areas ⇒ the strength of the radio signal can be very different, more complex problem of modulation
Wireless Networks

- 802.16 has to connect more users per cell, and has to have a larger bandwidth
  - =>WiFi connections transmit up to 54 megabits per second
  =>WiMAX should be able to handle up to **70 megabits per second**
  ⇒ WiFi’s range is about 100 feet (30 m). WiMAX range will be about **30 miles** (50 km) with wireless access.

- The waves are different => adapt the physical layer.
  Waves can be absorbed by the rain, snow, or clouds, so we have to be careful about the errors.

- 802.16 can perfectly handle real-time applications (such as voice or videos).
A **WiMAX tower**, ~ cell-phone tower And a **WiMAX receiver**

2 forms of wireless service:

- **non-line-of-sight**, WiFi sort of service, where a small antenna on your computer connects to the tower.

**lower frequency range**

- **line-of-sight** service, where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole 

**higher frequencies.**
OSI Structure
Frame structure

- The EC field indicates whether the data are encrypted or not.
- The IC field tells us whether a final checksum is used or not.
- The EK fields indicate the keys used for the encryption, if there is one.
- The length field gives the length of the whole frame, including the header.
- The Header CRC is a header checksum (calculated with a polynomial).
2. WiFi 802.11 Security
Existing Protocols:

- SSID
- MAC Address Filtering
- WEP
SSID

→ For Service Set IDentifier

→ The first step in user’s authentification

→ Configurable identification that allows clients to communicate to the AP
Wireless Security

SSID

SSID = ELz5bd
SSID = LAz5bd
SSID (and why it is quite inutile)

- AP have default SSID: “tsunami” for Cisco devices
- Devices unfortunately use to broadcast their SSID during beacon frames
- An attacker can discover your SSID by using a brute-force dictionary attack
MAC Address Filtering

• Permit only a few MAC addresses to connect to the network

• Two ways:
  – The AP has the list of authorized MAC addresses
  – A RADIUS server is used to centralize the correct MAC addresses
MAC Address Filtering
MAC Address Filtering

First possibility : Locally

→ You have to administrate locally the authorization MAC addresses and it becomes a problem when the numbers of clients and APs grows.
MAC Address Filtering

Second Possibility: RADIUS Server

→ The entire list of authorized addresses can be found, not encrypted in the configuration file of the server…
MAC Address Filtering

The main problem is that the MAC address of the client is sent in clear: any intruder can sniff authorized MAC addresses and, then, changes his own address with proper tools...
WEP

Wired Equivalent Privacy
WEP

SSID and MAC Addresses are transmitted in the clear text…

→ Encoding the data : SSID, MAC Address, data sent after the connection between the user and the server.
WEP

- It is an optional encryption standard implemented in the MAC Layer. So it is used at the 2 lowest layers, the data link and the physical layer.
- It is using a static key, a 64-bit one or a 128-bit one.
WEP in Action

• The NIC (Network Interface Card) encrypts the payload (frame body and CRC) of each 802.11 frame before transmission using an RC4 stream cipher provided by RSA Security.

• So 802.11 WEP only encrypts data between 802.11 stations. Once the frame enters the wired side of the network, such as between access points, WEP no longer applies.
Wireless Security

WEP

Wired Network

Encoding only on the wireless network

The same secret

Authentication Mechanism
First Step

A requesting station sends an Authentication frame to the intend responder announcing that it intends to use shared key authentication.
The responder replies with the second Authentication frame having 128 bytes of random challenge text generated by the WEP engine in a standard form.
Authentication Mechanism
Third Step

The requester copies the challenge in the third Authentication frame, encrypts the frame with its secret key and sends it back to the responder.
The responder then checks the ICV and if correct, it decrypts the contents of the challenge text field and compares them to that sent in frame 2. If the contents match, it sends a final frame announcing success. If the contents don't match or the ICV check fails, the final frame announces failure.
The secret key used in WEP algorithm is 40-bit long (or 104) with a 24-bit Initialization Vector (IV) that is concatenated to it for acting as the encryption/decryption key.
WEP Algorithm – Encryption
Wireless Security

WEP Algorithm – Decryption
What’s wrong with WEP?

• Relatively short IVs: for a large busy network, reoccurrence of IV can happen within an hour or so → Sniffing…

• Static key: it is the same key for all the APs and the users of the network → rarely changed
However WEP is better than nothing

- Most of the time, WEP is turned off
- 90% less intrusions
- Protecting many home and business networks from the general public