The IEEE 802.11 standard

Imad Aad

INRIA, Planete team
WLANs vs. Wired LANs

- History
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security
WLANs vs. Wired LANs

- No wires → Mobility
- Scarse bandwidth (?)
- Multipath, pathloss, interference / noise → BER

Diagram:

- Tx
- s
- Obstacle 1
- s1
- Rx
- s0
- Obstacle 2
- s2
- s0 + s1 + s2
**WLANs vs. Wired LANs**

- No wires → Mobility
- Scarse bandwidth (?)
- Multipath, pathloss, interference / noise → BER

LOS

\[ \alpha = 2 \]

No LOS

\[ \alpha = 4 \]

15–25 dB drop

\[ \alpha = 4–6 \]
WLANs vs. Wired LANs
WLANs vs. Wired LANs

- No wires → Mobility
- The hidden node problem
- Scarse bandwidth (?)
- Multipath, pathloss, interference / noise → BER
- Protection / Privacy
WLANs vs. Wired LANs
WLANs vs. Wired LANs

Application layer

Network layer

LLC sub-layer

MAC sub-layer

PHY layer

IEEE 802.2

IEEE 802.11 – IEEE 802.3
Outline

- WLANs vs. Wired LANs
- History
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security
1970s: ALOHA

1972: Slotted ALOHA

Slotted ALOHA: $S = Ge^{-G}$

Pure ALOHA: $S = Ge^{-2G}$
1970s: ALOHA
1972: Slotted ALOHA
1975: Carrier Sense Multiple Access (CSMA)
   △ non persistent
   △ p-persistent
History

- 1970s: ALOHA
- 1972: Slotted ALOHA
- 1975: Carrier Sense Multiple Access (CSMA)
  - non persistent
  - p-persistent
- CSMA with collision detections (CD): Ethernet (1976)
- CSMA w/ coll. avoidance (CA): IEEE 802.11 (1997)
Outline

- WLANs vs. Wired LANs
- History
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security
Working modes

- Ad-hoc mode vs. Infrastructure mode (IS)
- Independent BSS (IBSS), Basic Service Set (BSS), Extended Service Set (ESS)
Working modes

- Ad-hoc mode vs. Infrastructure mode (IS)
- Independent BSS (IBSS), Basic Service Set (BSS), Extended Service Set (ESS)
Working modes

- Ad-hoc mode vs. Infrastructure mode (IS)
- Independent BSS (IBSS), Basic Service Set (BSS), Extended Service Set (ESS)

Handoff on the MAC sub-layer
Outline

- WLANs vs. Wired LANs
- History
- Working modes
  - **MAC sub-layer**
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security
MAC sub-layer

DCF: Distributed Coordination Function (ad-hoc, IS modes)
PCF: Polling Coordination Function (in IS mode, optional)
DCF: Distributed Coordination Function (ad-hoc, IS modes) - Basic mechanism ($\text{pktsize} < \text{RTSthreshold}$)
DCF: Distributed Coordination Function (ad-hoc, IS modes)
- The hidden node problem
DCF: Distributed Coordination Function (ad-hoc, IS modes)
- RTS/CTS mechanism \( \text{pktsize} \geq RTSThreshold \)
DCF: Distributed Coordination Function (ad-hoc, IS modes)
- Fairness ? ... depends on scenario
- QoS ? ... not yet ... wait for 802.11e
**MAC sub-layer**

**DCF: Distributed Coordination Function (ad-hoc, IS modes)**

**PCF: Polling Coordination Function (in IS mode, optional)**
Packet fragmentation

- Source (Tx) sends Fragment 0, ACK0
- Destination (Tx) sends Fragment 1
- Time for ACK1
- Destination (Tx) sends Fragment 2
- Source (Tx) sends ACK2

Channels:
- NAV (CTS)
- NAV (fragment 0)
- NAV (fragment 1)
- NAV (fragment 2)
- NAV (ACK0)
- NAV (ACK1)
Outline

- WLANs vs. Wired LANs
- History
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security
The PHY layer (1997)

Application layer

Network layer

LLC sub-layer

MAC sub-layer

PHY layer

3 PHY types:
- DSSS (most products)
- FHSS (less products)
- IR (unknown products)
The PHY layer (1997)

the EM spectrum allocation

Freq.:
1 KHz 1 MHz 1 GHz 1 THz 1 PHz 1 EHz

Freq.:
30 KHz 300 KHz 3 MHz 30 MHz 300 MHz 3 GHz 30 GHz

Freq.:
902 MHz 928 MHz 2.4 GHz 2.4835 GHz 5.725 GHz 5.785 GHz

Infrared
Visible
UV
X rays
Gamma rays

(AM radio) (SW radio) (FM radio − TV) (TV − Cell.)

HF VHF UHF SHF

3 GHz 30 GHz

902 MHz 928 MHz

ISM U − NII

Cordless phones
Baby monitors
(old) Wireless LANs

IEEE 802.11(b)
Bluetooth
Microwave ovens

IEEE 802.11a
Hiperlan II
The PHY layer (1997)

- DSSS (Direct Sequence Spread Spectrum)
- FHSS (Freq. Hopping Spread Spectrum)
- IR (Infra Red)
DSSS: principle

**Note:**
- single code (11-chips)
- multiple access? ... no
- security? ... no

IEEE 802.11 – p.13
DSSS: principle

Transmitter baseband signal before spreading

1 bit period

1 0

11 chips

1 0 1 1 0 1 1 1 0 0 0

1 0 1 1 0 1 1 1 0 0 0

Scrambled Data

Periodic 11 Bit Barker code

mod−2 adder

Carrier modulator

Transmitter baseband signal after spreading

IEEE 802.11 – p.13
DSSS: principle

@ Transmitter

before spreading  after spreading

@ Receiver

before despreading  after despreading

narrowband interference
PSK (Phase Shift Keying)

\[ S(t) = A \sin \left( 2\pi \omega t + \varphi(t) \right) \]

\[ \varphi = 0 \]
DPSK (Differential PSK): no reference signal needed

\[ S(t) = A \sin \left( 2\pi \omega t + \varphi(t) \right) \]
The PHY layer (1997)

DSSS: modulation

DBPSK

(0)
0
180

(1)

0 Mbps

DQPSK

(0)
0
180

(01)
270

(11)

1 Mbps

2 Mbps

IEEE 802.11 – p.13
DSSS: Spectrum at modulator output

The PHY Layer (1997)
in France (few months ago): allowed channels
The PHY layer (1997)

in France (few months ago): maximum channel separation
The PHY layer (1997)

in Europe

(Ch. 1) 2.412 MHz
(Ch. 3) 2.472 MHz
Transmission power

<table>
<thead>
<tr>
<th></th>
<th>GSM</th>
<th>$\mu$ wave oven</th>
<th>IEEE 802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical</td>
<td>100 mW - 600 mW</td>
<td>0.2mW/cm$^2$</td>
<td>6.3 mW</td>
</tr>
<tr>
<td>Regulations</td>
<td></td>
<td>1-5 mW/cm$^2$ @ 5cm</td>
<td>100 mW (Eur.)</td>
</tr>
</tbody>
</table>
The PHY layer (1997)

- DSSS (Direct Sequence Spread Spectrum)
- FHSS (Frequency Hopping Spread Spectrum)
- IR (Infra Red)
The PHY layer (1997)

FHSS

- Modulation: GFSK
  binary 0/1: \( F_c \pm f_d \) (for 1 Mbps)
  00, 01, 10, 11: \( F_c \pm 2f_d \) (for 2 Mbps)

- \( F_c \) sequence = \( F_x(i) = [b(i) + x] \text{mod}(35) + 48 \) (France)
  \( b(i) \): tables
  \( x \): 3 sets

- Fast-FH vs. Slow-FH: min 2.5 hops/s

- Bluetooth interference ?... YES
The PHY layer (1997)

- DSSS (Direct Sequence Spread Spectrum)
- FHSS (Freq. Hopping Spread Spectrum)
- IR (Infra Red)
Infra Red (IR)
Pulse Position Modulation (PPM)

- 1 Mbps: 4 data bits → 16-PPM symbol
- 2 Mbps: 2 data bits → 4-PPM symbol
Outline

- WLANs vs. Wired LANs
- History
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security
IEEE 802.11b: 2.4 GHz. 1Mbps, 2Mbps, 5.5Mbps 11 Mbps.

- High Rate DSSS
- Modulation: (backward compatible) DBPSK, DQPSK Complementary Code Keying (CCK) + DQPSK, (opt.) Packet Binary Convolutional Coding (PBCC) + (BPSK,QPSK)
- Currently the most widely used one
IEEE 802.11a: 5.7 GHz, 6 Mbps → 54 Mbps!!

- OFDM (Orthogonal Frequency Division Multiplexing)
  - Principle:
    High-rate data is divided into several lower rate binary signals.
    Each low-rate signal modulates a different sub-carrier (48)
    Sub-carrier sets are orthogonal.
  - Modulation: BPSK, QPSK, 16QAM and 64QAM
- FEC: Convolutional encoding needed (Viterbi)
- Close to Hiperlan 2 specs.
- “coming soon”
PHY Extensions (1999)
Outline

- WLANs vs. Wired LANs
- History
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security
WEP (Wired Equivalent Privacy)
WEP (Wired Equivalent Privacy)

- Initialization Vector (IV)
- Secret Key
- Plaintext
- Integrity Algo.
- WEP PRNG
- Key Sequence
- XOR
- Integrity Check Value (ICV)
- Ciphertext
- Message
- IV
WEP (Wired Equivalent Privacy)

- default keys / established keys
- 40-128 bit key
- Algorithm: RC4 (symmetric stream cipher)
- Cracking tools: WEPcrack, AirSnort:
  if “100MB-1GB of data can be gathered” then one “can guess the encryption password in less than a second”!!

Access control table ? ... inefficient
Network ID ? ... inefficient
it works!
looks just like ethernet to higher layers
no QoS support... yet.
limited security management.

Planete team: http://www.inrialpes.fr/planete
Imad AAD: imad.aad@inrialpes.fr