Medium Access and standards for Wireless Networks

Graduate course in Electrical Communications

Dr. Luca De Nardis
Outline

• Classification of wireless MAC protocols

• Random Access protocols
  – The Aloha protocol
  – The Carrier Sensing Multiple Access (CSMA) protocol

• Standards for wireless LAN
Classification of wireless MAC protocols

- The above classification is based on how DATA traffic is transferred.
- Most scheduled protocols, in fact, foresee a random access phase in which control packets are subject to collision.
Random Access Protocols

• In random access protocols each packet is subject to collision, since no resource reservation is adopted
• The main advantage of this family of protocols is simplicity:
  – Each terminal can transmit with no (or limited) information regarding other terminals
  – Random access protocols provide low delays, since packets are transmitted (almost) immediately
• The main drawback is the low scalability with traffic load:
  – When the offered traffic increases, the probability of collision increases as well, and the number of lost packets increases
  – This reduces the throughput (roughly: the amount of data successfully transferred) and increases the delay, since lost packets must be eventually retransmitted
• In order to reduce the negative effect of collisions, Collision Avoidance mechanisms are often adopted
Scheduled Access Protocols

- Scheduled access protocols adopt mechanisms that avoid more than one terminal to transmit at a given time.
- Data packets are never subject to collision, since at any time all terminals in the network are made aware of which terminal in the network is allowed to transmit.
- These protocols are particularly suited for centralized network architectures, where a controller (Base Station, Access Point) manages the access, but are suitable as well for distributed network architectures in which the resource control and management is centralized (centralized network organization). Schemes include:
  - **Polling**: the controller “calls” one terminal at the time (see Bluetooth).
  - **Demand Assignment**: the controller grants the channel to terminals following a request, typically submitted in a random access phase.
  - **Static**: A resource (e.g. time slot, carrier) is statically assigned to a terminal when it joins the network.
- In distributed architectures, scheduled protocols can be adopted either by selecting a terminal which acts as a controller (see above) or by adopting a distributed scheduling strategy (token).
Hybrid Protocols

• Hybrid Protocols combine the contention-based approach of random access protocols with the contention-less approach of scheduled access protocols.
• When a terminal has packets to transmit, it transmits the first packet using random access.
• The first packet piggybacks a reservation request (e.g. for time slots in a scheduled TDMA protocol).
• If the first packet is received correctly, the reservation request guarantees that the remaining packets are transmitted without any risk of collision.
• Often proposed for voice streams.
• Examples:
  - Packet Reservation Multiple Access (PRMA) (reserves slots in a TDMA frame).
  - Random Reservation Access – Independent Station Algorithm (RRA-ISA) (reserves slots in a polling sequence).
Random Access Protocols

- Three main classes of Random Access Protocols will be analyzed:
  - Aloha and Slotted Aloha
  - Carrier Sensing Multiple Access
  - Carrier Sensing Multiple Access with Collision Avoidance
ALOHA

• The simplest random access protocol is ALOHA.
• Developed in 1970 at University of Hawaii.

• ALOHA does not require any action by terminals before they transmit a packet.
• A checksum is added at the end of each packet.
• The receiving terminal uses the checksum to evaluate if the packet was received correctly or was corrupted by collision.
• In case of collision the packet is discarded.
• Retransmission of discarded packets is accomplished based on an Automatic Repeat on ReQuest (ARQ) protocol, that re-schedules packets after a random delay.
Carrier Sensing Multiple Access

- In networks with high traffic load ALOHA is not effective due to collisions
- Performance can be increased by introducing Carrier Sensing, leading to Carrier Sensing Multiple Access (CSMA)
  - When a terminal A has packets to transmit, it senses the channel before starting transmission
  - If another terminal B is already transmitting, terminal A will detect its transmission
  - In this case A will postpone its own transmission
  - When A senses the channel as idle for a predefined amount of time, it assumes the channel as available and starts transmission.
Throughput of Random Access protocols

Throughput $S$ vs. Offered Traffic $G$

- ALOHA
- Slotted ALOHA
- CSMA
- Ideal MAC

Key points:
- $G = 0.5, S = 1/2e$
- $G = 1, S = 1/e$
- $a = 0$
- $a = 0.25$
- $a = 0.50$
- $a = 0.75$
- $a = 1$
• The performance of CSMA heavily depends on the network scenario

• Wireless networks are in fact characterized by:
  1. Varying network topology
  2. Partial connectivity
     • This can lead to errors in protocols that work perfectly fine in wired networks

• In the case of CSMA, the wireless medium causes two phenomena that significantly reduce the protocol performance:
  – Hidden terminal
  – Exposed terminal
CSMA Issues (2/4)

- Hidden terminal (1)

- Node $S$ is sending a packet to $D$, which is acting only as receiver
- Node $H$, willing to transmit, starts the Carrier Sensing procedure, sensing the channel for the time period $w$ defined in the protocol
- After a time $w$, $H$, which cannot detect the transmission by node $S$ (due to limited radio coverage), assumes the medium is available
• Hidden terminal (2)

• H starts its transmission, causing a collision in D, and potentially the loss of both packets

• N.B.: Since wireless medium is inherently broadcast, this issue arises even if H is not willing to transmit to D, but to another terminal D2 in its range!
- Exposed terminal

- In $t = 0$, terminal $S_1$ starts a packet transmission to $D_1$
- In $t = t_0$, $S_2$ is willing to transmit a packet to $D_2$
- $S_2$ starts the Carrier Sensing procedure
- $S_2$ detects a transmission already active, and assumes the channel is busy, postponing thus the transmission to $D_2$
- Since $D_2$ is not reached by $S_1$, however, the transmission $S_2 \rightarrow D_2$ could be activated without causing any collision
Collision Avoidance

• Collision Avoidance mechanisms can be divided in:

<table>
<thead>
<tr>
<th>In-Band Collision Avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The Collision Avoidance procedure uses the same channel used for data transmission</td>
</tr>
<tr>
<td>• Typically based on a sequence of control packets exchanged between transmitter and</td>
</tr>
<tr>
<td>receiver (hand-shaking)</td>
</tr>
<tr>
<td>• Examples:</td>
</tr>
<tr>
<td>– MACA (Medium Access with Collision Avoidance)</td>
</tr>
<tr>
<td>– 802.11 DFWMAC (Distributed Foundation Wireless MAC)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Out-of-Band Collision Avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The Collision Avoidance procedure uses a dedicated channel</td>
</tr>
<tr>
<td>• Typically based the assertion of sinusoidal tones (since the channel is dedicated, there</td>
</tr>
<tr>
<td>is no need for organizing control information into packets)</td>
</tr>
<tr>
<td>• Example:</td>
</tr>
<tr>
<td>– BTMA (Busy Tone Multiple Access)</td>
</tr>
<tr>
<td>– DBTMA (Dual Busy Tone Multiple Access)</td>
</tr>
</tbody>
</table>
In-band CA: Medium Access with Collision Avoidance (MACA)

- MACA does not use Carrier Sensing, in the sense that terminals start transmitting a packet without spending any time sensing the channel.
- In MACA when a terminal has a data packet to send, it does not transmit directly the data packet, but instead starts a Collision Avoidance procedure with the intended destination, based on three steps:
  1. Transmission of a Request-To-Send (RTS) packet from source to destination
  2. Transmission of a Clear-To-Send (CTS) packet from destination to source, in response to the CTS
  3. Transmission of the DATA packet from source to destination, after reception of the CTS
- The procedure is called handshaking.
CSMA with Collision Avoidance (CSMA-CA)

- Although MACA was proposed as an alternative to CSMA protocols, CSMA and In-band Collision Avoidance can be combined in order to get the advantages provided by MACA and reduce the probability of having collisions on the RTS packets (CSMA-CA).

- The CSMA-CA approach is adopted in the Distributed Foundation Wireless MAC (DFWMAC) adopted in the IEEE 802.11 standard (WiFi).

- In DFWMAC the handshaking is formed of four steps. The four steps are:

  1. RTS (Direction: S -> D)
  2. CTS (D -> S)
  3. Data (S -> D)
  4. Acknowledge (Ack) (D -> S)

- CSMA is adopted before transmitting the RTS packet.
1985: the entity responsible for radio emissions in USA, the FCC (Federal Commission for Communications) makes three frequency bands available for wireless communications:

- 902 – 928 MHz
- 2400 – 2483.5 MHz
- 5725 – 5850 MHz

These are the already mentioned Industrial, Scientific and Medical (ISM) bands. They are license-free and can be used without any concession fee.

In order to reduce interference generated between different devices using the ISM band, the FCC imposes 2 constraints:

- Use of transmitted power < 1 W
- Use of Spread Spectrum techniques to limit the Average Power Spectral Density
Wireless LAN - Origins (2/2) -

• **1990**: The first wireless LAN system is launched on the USA marked by NCR Corporation: WaveLan (now sold by Lucent/Orinoco)

• In the next few years other companies enter the wireless LAN market: Proxim, IBM, DEC...

• **1992**: The 2.4 GHZ is finally made available in Europe too for license free wireless communications

• Proposed solutions both in Europe and in USA were proprietary, posing two serious issues to wireless LAN:
  - No interoperability between products of different brands
  - Limited market

• **1997**: the first standard for wireless LAN is released:

  IEEE 802.11
Wireless LAN
- Bands of Operation-

- Devices in the 902-928 MHz ISM band:
  - Proprietary wireless LANs (SS)
  - Cordless Phones (mainly NB)
  - Cordless Headphones (NB)
  - Surveillance systems (NB)

- Devices in the 2.4-2.4835 GHz ISM band:
  - IEEE LAN standards (SS)
  - Audio/video signal repeaters (NB)
  - Remote Garage openers (NB)

- Devices in the 5.725-5.85 GHz ISM band:
  - Reserved for high bit rate networking devices (no cordless phones)
  - IEEE/ETSI LAN standards (SS)
Interference in the ISM bands

- Since the ISM bands are open to any device compliant to the FCC emission rules both intra-system and inter-system interference are a serious issue.
- Most of the standards foresee the organization of devices in independent subnetworks (e.g. Base Service Sets in 802.11, Piconets in Bluetooth) and do not provide means for managing interference between different subnetworks (intra-system interference).
- Obviously, no interoperability is guaranteed between different standards using the same frequencies and provoking thus mutual interference (inter-system interference).
Original definition of IEEE 802.11:

<table>
<thead>
<tr>
<th>Frequency</th>
<th>IEEE 802.11 Wireless LAN Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz</td>
<td>Infra-red (950mm−950mm)</td>
</tr>
<tr>
<td>Spread Spectrum</td>
<td>DSSS</td>
</tr>
<tr>
<td>Baseband Modulation</td>
<td>DQPSK</td>
</tr>
<tr>
<td>Max bandwidth</td>
<td>1Mbps</td>
</tr>
<tr>
<td>Access Control</td>
<td>CSMA/CA, RTS/CTS</td>
</tr>
<tr>
<td>Area(open air/office)</td>
<td>100−300m/20−100m</td>
</tr>
</tbody>
</table>
Wireless LAN
- IEEE Standards and task groups (2/3) -

- **802.11b:**
  - Introduced in 1999, with the definition of Wi-Fi:
    - RF in 2.4 GHz ISM band
    - 5.5 – 11 Mb/s (now up to 22 Mb/s)
    - Complementary Code Keying Modulation

- **802.11a:**
  - Higher Bit rate: from 6 up to 54 Mb/s
  - RF in 5 GHz ISM band
  - OFDM (Orthogonal Frequency Division Modulation)
• **802.11e:**
  - Deals with the MAC level of the standard
  - Its goal is to increase the 802.11 capability of dealing with real-time applications:
    - Audio streams
    - Video streams
  - So far, this task group defined statistic e deterministic methods for traffic differentiation

• **802.11g:**
  - Released in 2005
  - Same bit rate of the 802.11a standard (54 Mb/s)
  - Same band of the 802.11b standard

• **802.11n:**
  - Almost released - draft-based products available
  - Higher speeds (>100 Mb/s)
Wireless LAN
- ETSI standards-

• **Hiperlan (High PErformance Radio Local Area Network) I:**
  - Standard released in 1998
  - Bit rate: 20 Mb/s
  - RF in the ISM 5 GHz band
  - Quality of Service (QoS) support at MAC layer
  - Modulations: FSK (Frequency Shift Key) – GMSK (Gaussian Minimum Shift Key)

• **Hiperlan II (around 2000)**
  - Bit rate: 54 Mb/s
  - RF in the ISM 5 GHz band
  - Quality of Service (QoS) support at MAC layer
    - Capability of managing real-time and multimedia streams
  - Capability of interface with GSM cellular networks
  - At the moment, it is being harmonized with (i.e. absorbed by) 802.11a
Other WLAN standards
- Bluetooth (IEEE 802.15.1) -

- Based on Frequency Hopping
- Works in the ISM 2.4 GHz band, as 802.11b/g
- Compared to 802.11:
  - Lower bit rate (1 Mb/s)
  - Lower range:
    - 100 m for Class 1 devices ($P_{out} = 20$ dBm)
    - 10 m for Class 2 devices ($P_{out} = 4$ dBm)
    - 10 cm for Class 3 devices ($P_{out} = 0$ dBm)
  - Limited scalability (a piconet can be formed of up to 8 active devices)
  - Typically designed for ad-hoc topologies
  - Lower flexibility

Bluetooth is not a competitor for 802.11, but it covers a different market segment
Bluetooth - Mitigating interference -

- Each device working in an ISM band MUST adopt a Spread Spectrum technique to mitigate interference (FCC rule)
- Bluetooth uses Frequency Hopping to achieve spectrum spreading
- In FH-SS, the transmitter spreads the spectrum by continuously jumping from one frequency channel to another
The sequence of frequency hops is defined by a FH code.

Time occupation of frequency for a FH-SS signal looks as follows:
Bluetooth
- Frequency Hopping (2/3)-

- A FH-SS guarantees a good resilience to a single frequency interferer.
- The higher the number of hops and the shorter the dwell time, the higher the robustness.

Interference suffered in just one dwell time
Coexistence of different FH-SS signals

- If the FH codes are properly selected (orthogonal) → No interference!!
- Otherwise, collisions in one or more dwell time generate interference
Bluetooth
- Medium Access -

- Bluetooth adopts a Contention Free access, based on the Master-Slave approach:
HomeRF is an industrial standard that was designed for interconnecting several home devices equipped with a radio interface:

Examples: PCs and cordless phones, Printer sharing among PCs, wireless connection to the web...
Other WLAN standards
- Home RF (2/2) -

- **Physical Layer** - based on the 802.11PHY, in the FH-SS flavor (bit rate ≤ 1 Mbit/s): for modern standards (10 – 100 Mbit/s) at lower limit within wireless LAN devices

- **MAC Layer** – combination of 802.11 MAC (used for data), and of the MAC layer of DECT (Digital Enhanced Cordless Telecommunications) for voice traffic:
IEEE WLAN/ WPAN Standards

<table>
<thead>
<tr>
<th>Data Rate (Mb/s)</th>
<th>Range (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b/g</td>
<td>0.1 - 10</td>
</tr>
<tr>
<td>802.15.1</td>
<td>1 - 100</td>
</tr>
<tr>
<td>802.15.3</td>
<td>10 - 1000</td>
</tr>
<tr>
<td>802.15.3a</td>
<td>100 - 1000</td>
</tr>
</tbody>
</table>

Location & Tracking

UWB

IEEE WLAN/WPAN Standards
802.15.3/802.15.3a Overview

• 802.15.3
  – Personal Area Network: 10 Meters range
  – QoS requirements
  – High Data Rate transfers (video, digital still images, large file transfers): 20 – 55 Mb/s
  – Extension to 802.15.1 (Bluetooth)

• 802.15.3a
  – Personal Area Network: 10 Meters range
  – QoS requirements
  – Very High Data Rate transfers (video, cable replacement, home entertainment, large file transfers): 28.5 – 480 Mb/s UWB
802.15.3/802.15.3a MAC Architecture

• Clustered MAC Architecture
  • During start-up, devices organize themselves in PicoNets (PNs)
  • Each PN is controlled by a PicoNet Coordinator (PNC)
  • When a new device appears, it searches for existing PicoNets (by listening to broadcast messages sent by PNCs) and selects one of them
  • The standard completely defines procedures for intra-PicoNet operations
  • Procedures for inter-PicoNet operations are only preliminary in the standard
IEEE 802.15.3/802.15.3a Intra-PicoNet resource sharing

- TDMA is adopted within the PicoNet
- Time axis is organized in Superframes
- Each Superframe is subdivided in three periods:
  - Beacon Period — Used by the PNC to broadcast information to all terminals in the piconet
  - Contention Access Period (CAP) — Used by terminals to send small amounts of data to other terminals, or to ask the PNC for reserved Channel Time Allocations (CTAs) (that is, time slots) (Optional field)
  - Contention-Free Period (CFP) — Dedicated to transmissions during the CTAs announced in the beacon period and to control traffic during Management CTAs (MCTAs)

- The PNC schedules the access to the medium by granting CTAs
802.15.4/802.15.4a Overview

• 802.15.4
  – Ultra-low complexity, ultra-low power, ultra-low cost
  – Low Data Rate transfers (sensors, automation, interactive toys): 20 – 250 Kb/s
  – Personal and Local Area Network: at least 10 meters range

• 802.15.4a
  – Ultra-low complexity, ultra-low power, ultra-low cost
  – Low Data Rate transfers (sensors, automation, interactive toys): 10 – 250 Kb/s
  – Local Area Network: 30 meters range (extended to 100s of meters by relaying)
  – Location and tracking capability
IEEE 802.15.4 MAC

- Devices organize themselves in Personal Area Networks (PANs), similar to the PicoNets of 802.15.3
- Each PAN is managed by a Coordinator, which must be a FFD
- Two different topologies are allowed within a PAN:
  - Star topology
  - Peer-to-peer topology

```
+-------------------+-------------------+
| RFD              | FFD               |
+-------------------+-------------------+
| PAN Coordinator (FFD) | PAN Coordinator (FFD) |
```

- In the peer-to-peer topology, coverage extension is achievable by introducing the concept of multiple clusters within a PAN
IEEE 802.15.4 PAN resource sharing

- TDMA is possible (**but not mandatory**) within the PicoNet
- If TDMA is adopted, the PAN Coordinator defines a Superframe by emitting periodic beacons, divided in:
  - Beacon Period — Used by the PAN Coordinator to broadcast information to all devices in the PAN
  - Contention Access Period (CAP) — Divided in Time Slots (TS), it is used by terminals to send data to other devices or to the coordinator in a slotted CSMA-CA fashion
  - Contention-Free Period (CFP) — Divided in Guaranteed Time Slots (GTS), it is used for low-latency devices (e.g. PC peripherals) (optional field)
## Application scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Link distance</th>
<th>Data rate</th>
<th>Environment</th>
<th>Mobility</th>
<th>Power</th>
<th>Cost</th>
<th>Number of devices</th>
<th>Location accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding equipment</td>
<td>100-250m</td>
<td>10Kbps</td>
<td>Indoor</td>
<td>Walking speed</td>
<td>Low</td>
<td>Medium</td>
<td>100’s</td>
<td>1m</td>
</tr>
<tr>
<td>Finding a patient</td>
<td>20-30m</td>
<td>1 0 - 1 0 0 Kbps</td>
<td>Indoor</td>
<td>Walking speed</td>
<td>Low</td>
<td>Medium</td>
<td>20-30</td>
<td>1m</td>
</tr>
<tr>
<td>Position monitored for training purposes</td>
<td>75-100m</td>
<td>1 0 - 1 0 0 Kbps</td>
<td>Indoor</td>
<td>Walking speed</td>
<td>Low</td>
<td>Medium</td>
<td>100’s</td>
<td>1m</td>
</tr>
<tr>
<td>Warehouse tracking</td>
<td>1-500 m</td>
<td>1 kbps</td>
<td>In-door</td>
<td>Walking speed</td>
<td>Low</td>
<td>Low</td>
<td>100s</td>
<td>10 cm</td>
</tr>
<tr>
<td>Industrial monitoring</td>
<td>1-500 m</td>
<td>10 kbps</td>
<td>In-door / Out-door</td>
<td>Walking speed</td>
<td>Low</td>
<td>Low</td>
<td>100s</td>
<td>10 cm</td>
</tr>
<tr>
<td>Smart distributed networks</td>
<td>10 – 2000 m</td>
<td>1 kbps</td>
<td>Out-door</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>10s</td>
<td>1 m</td>
</tr>
<tr>
<td>Avalanche victims location finding</td>
<td>100 m</td>
<td>&lt; 100 kb/s</td>
<td>Out-door</td>
<td>Walking speed</td>
<td>Low</td>
<td>Low</td>
<td>&lt; 10</td>
<td>10 cm.</td>
</tr>
</tbody>
</table>
802.15.4a: a potential application (1/2)

Track Firefighter Status

- When Firefighters are trapped or lost, there is no effective way to rescue them
- Trapped or lost firefighters, if conscious, often don’t know their own location
- Unlike the Movies, structural fires are characterized by heavy smoke and darkness
- Sounds are diffused by smoke and difficult to localize
- Seconds count...
- If they are known to be on the scene (sometimes they are not), it may take a long time before a firefighter is missed
- Commanders don’t know status of their firefighters (oxygen level, health, etc.)
Indoor accurate positioning (10 cm accuracy) is the key requirement