Link Layer: WiFi and 5G

CS204: Advanced Computer Networks
Nov 8, 2023
Agenda

• Introduction to wireless
  • Architecture Options
  • Wireless Link Characteristics

• WiFi
  • Challenges to design wireless link layers
  • WiFi’s Approach

• Cellular
  • Basic Architecture
  • Critical Functions
  • Mobility
802.11 (Wi-Fi) MAC

• Basic Access Mechanism for Data Traffic
  • CSMA/CA
  • Binary exponential back-off

• Timing Intervals: SIFS, Slot Time, PIFS, DIFS, EIFS

• Distributed coordination function (DCF) Operation
DCF MAC

• Carrier sense multiple access with collision avoidance (CSMA/CA)
  • based on carrier sense function in PHY called Clear Channel Assessment (CCA)
  • CSMA/CA+ACK for unicast frames, with MAC level recovery
  • parameterized use of RTS/CTS to protect against hidden terminals
  • frame formats to support both infrastructure and ad-hoc networks
IEEE 802.11 with Omni Antenna

RTS = Request To Send

CTS = Clear To Send
IEEE 802.11 with Omni Antenna
Illustration for DCF Operation

Station 1
- NAV
- DIFS
- random backoff (7 slots)
- SIFS
- CTS
- SIFS
- DATA
- SIFS
- ACK
- new random backoff (10 slots)
- DIFS
- Station defers
- NAV

Station 2
- NAV
- DIFS
- RTS
- SIFS
- DATA
- SIFS
- ACK
- remaining backoff (2 slots)
- NAV

Station 3
- NAV
- DIFS
- random backoff (9 slots)
- SIFS
- Station defers, but keeps backoff counter (=2)
- SIFS
- Station sets NAV upon receiving RTS
- DIFS
- Station defers
- SIFS
- ACK

Station 4
- NAV
- DIFS
- Station sets NAV upon receiving RTS
- SIFS
- DATA
- SIFS
- Station sets NAV upon receiving CTS, this station is hidden to station 1

Station 5
- NAV
- DIFS
- ACK
- SIFS

Station 6
- NAV
- DIFS
- DATA
- SIFS

time
Does it solve hidden receivers?

- Assuming carrier sensing zone = communication zone
- Case: C sends RTS to D, D replies CTS to C

E does not receive CTS successfully, nor RTS from C → Can later initiate transmission to D. Hidden receiver problem @ E remains.
Increase carrier sense range?

- E knows C is sending, but cannot hear what C sends
- E will defer on sensing carrier $\rightarrow$ no collision!
Barriers/obstructions?

- E doesn’t hear C (during DATA transmission) → Carrier sensing does not help
WiFi Mobility Approach

*Client-initiated* solution

- Client decides that link to its current AP is poor
- Client uses scanning function to find another AP
- Client sends Re-association Request to new AP
- If Re-association Response is successful
  - then client has roamed to the new AP
  - else client scans for another AP
- If AP accepts Re-association Request
  - AP indicates Re-association to the Distribution System
  - Old AP may be notified thru distribution system
WiFi Scanning

• Scanning required for many functions
  • finding and joining a network
  • finding a new AP while roaming
  • initializing an ad hoc network

• 802.11 MAC uses a common mechanism
  • passive or active scanning

• Passive scanning
  • by listening for Beacons

• Action Scanning
  • probe + response
Agenda

• Introduction to wireless
  • Architecture Options
  • Wireless Link Characteristics

• WiFi
  • Challenges to design wireless link layers
  • WiFi’s Approach

• Cellular
  • Basic Architecture
  • Critical Functions
  • Mobility
Mobile Internet

~ 3.5 billion Smartphone users

~ 31 billion Interconnected devices in 2020

114.9 billion Mobile app download in 2019
Mobile Network Architecture Evolution

- **2G**
  - Circuit-switching for voice

- **3G**
  - Circuit-switching for voice
  - Packet-switching for data

- **4G/5G**
  - Packet-switching for everything
  - IP-based

Telecomm Infrastructure → IP-based Internet
3G vs. 4G

3G (PS + CS)

3G Gateways

Packet Switching (PS)

3G Base stations

4G (PS only)

Mobility Management Entity (Control Node)

Circuit Switching (CS)

Mobile Switching Center

Telephony Network

Internet

3G vs. 4G

3G (PS + CS)

3G Gateways

Packet Switching (PS)

4G (PS only)

Mobility Management Entity (Control Node)

Circuit Switching (CS)

Mobile Switching Center

Telephony Network

Internet
From 5G NSA (Non-Standalone) to SA

• 5G NSA: 4G architecture and protocol with 5G radio (current 5G)
  • Recall – PHY Innovation drives network design
  • That said, the following description will focus on 4G LTE
    • Even 5G SA shares similar design philosophy
4G LTE Network Architecture

Main components:
• MME (mobility management entity): mobility support
• PS gateway: IP routers
• BS (base station): radio access
• User device: clients requesting for 4G access
Operations on Network Planes

Two main planes in operation in parallel:

- **Data plane**: data content delivery
- **Control plane**: signaling functions for control

There is an additional plane that works with the above two planes:

- **Management plane**: configurations, monitoring
Control Plane Features

• Control plane regulates:
  • Radio resource allocation
  • Mobility management
  • Connectivity
  • Security management, ...

• Control-plane signaling message is free of charge

• Control-plane is always offered highest serving priority

• Layered protocol stack

Connectivity Management (CM)
Mobility Management (MM)
Radio Resource Control (RRC)

4G
Internet
Data-Plane Protocols: IP + Lower layers

- **Packet Data Convergence Protocol (PDCP)** – header compression, radio encryption
- **Radio Link Control (RLC)** – Readies packets to be transferred over the air interface
- **Medium Access Control (MAC)** – Medium access
Putting These Together

<table>
<thead>
<tr>
<th>Device</th>
<th>eNB</th>
<th>EPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS, ...</td>
<td>RRC</td>
<td>MME</td>
</tr>
<tr>
<td>Non-access Stratum (NAS)</td>
<td>TCP/UDP</td>
<td>NAS(CM/MM)</td>
</tr>
<tr>
<td>Radio Res Ctrl (RRC)</td>
<td>IP</td>
<td>SPGW</td>
</tr>
<tr>
<td>Packet Data Convergence (PDCP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radio Link Control (RLC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium Access Control (MAC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Layer (PHY)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Control

Data
Procedures Upon Device Power-On

System Initialization

Connectivity Control

Network Selection PLMN
Cell selection

Contestion based random access
RRC connection setup
RRC-CONNECTED
Attch (registration) procedure

MM-REGISTERED CM-CONNECTED

MM-DEREGISTERED CM-IDLE
RRC-CONNECTED

RRC-IDLE

MM-DEREGISTERED CM-IDLE

MM-DEREGISTERED CM-IDLE

MM-DEREGISTERED CM-IDLE

System Initialization

Connectivity Control
Control Plane State Transitions

- **Power On**
  - Registration (Attach)
  - Allocate device IP address
  - Authentication
  - Release due to device Inactivity
  - Release RRC connection
  - Configure DRX for paging

- **MM_Deregistered CM_Idle**
  - Deregistration (Detach)
  - Change PLMN
  - New traffic

- **MM_Registered CM_Connected**
  - New traffic
  - Establish RRC Connection
  - Release device IP address

- **MM_Registered CM_Idle**
  - Timeout of Periodic Tracking area Update
  - Release device IP address
Power Management via RRC in LTE

• Device RRC finite state machine
• 2 states: IDLE, CONNECTED
• Discontinuous reception (DRX): monitor a subframe per DRX cycle; receiver sleeps in other sub-frames
Data Delivery Path

• Simple IP based forwarding

• Data packets do not traverse control-plane elements (like MME)
  • Control plane packets also need to go through data plane protocols as well
  • However, much higher priority for control plane packets
Data Delivery

• Recall in WiFi: random access-based plus RTS-CTS
  • Would that be a good idea for cellular?
  • No, considering the number of users, and the licensed band

• Mobile Network: Access control through **scheduling**
  • Every node notifies the base station for resource (Resource block)
Step-by-Step Operation: Uplink data delivery

- DATA Packet arrives
- DRX OFF
- DRX ON

Mobile Device

- Scheduling related
  - SR (scheduling request)
  - Grant (allocated slot)
  - DATA (& BSR (buffer status report) if grant not enough)
  - Grant (for BSR request)
  - DATA
  - NACK (negative ACK) & Grant
  - DATA

4G BS
Step-by-Step Operation: Downlink data delivery

- **Mobile Device**
  - **DATA Packet arrives**
  - **DRX related**
    - **DRX OFF**
    - **DRX ON**
  - **Scheduling related**
  - **Retransmission related**

- **4G BS**
  - **Grant (allocated slot)**
  - **DATA**
  - **Grant (allocated slot)**
  - **DATA**
  - **NACK (negative ACK)**
  - **DATA (retransmission)**
Voice Services in LTE

• How to provide “carrier grade” voice over IP-based 4G LTE?
  • Recall, we no longer have circuit switch in 4G

• Two solutions:
  • #1. VoLTE (Voice over LTE): deliver voice directly in packets (over IP),
    • but with higher delivery quality
  • #2. CSFB (Circuit-Switched Fallback): leverage CS in legacy 3G network to deliver voice
Mobility in Mobile Networks

• **Mobility support**: a fundamental service to the evolving Internet
  • Seamless network service to mobile users *everywhere*

• Cellular network is the *only* deployed infrastructure with working solution to *wide-area* mobility support

• We will see
  • Which mobility functions are standardized, which are not?
  • Challenges and guidelines for mobility management
Mobility in Cellular Network since 2G

• **Low-level base station (BS):** connect mobile device
  • A BS can have multiple cells (sectors), each covering geographical area

• **High-level controller:** MME for each **location area**
  • Track user location, allocate IP, configure data forwarding path
Mobility Support in 4G LTE

- Span on multiple network nodes
- Involve multiple control procedures
2-Tier Mobility Support

• Low-level: Device associates to a BS
  • Association to BS ≠ active connectivity to BS
    • **Idle-state**: the device disconnects from the BS
    • **Active-state**: the device connects to the BS (e.g., for data transfer)

• High-level: the device registers to the controller
  • The network knows **where** the user is

---

[Diagram showing network topology with BSs and MMEs, indicating location areas and location update process]
Low Level Handoff (Handover)

• **Handoff**: mobile device changes its association from the old BS to the new BS
  - One of the basic functions for cellular mobility support
  - Not equivalent to mobility
    - Handoff can happen without mobility (e.g., radio link downgrade)

• Two categories of handoff
  - **Idle-state handoff**: initiated by mobile device
  - **Active-state handoff**: initiated by the old BS
    - Seamless voice/data delivery should be guaranteed
Idle-State Handoff

1. Old BS broadcasts handoff parameters to device
   • Measurement threshold, preference, speed-dependent scaling factors, etc.

2. Mobile device measures the signal strengths of neighboring BSes
   • Signal strengths are averaged to tolerate transient radio variation

3. With the measurement results, mobile device decides the new BS to associate with
1. Old BS informs MME of impending handoff, provides list of 1+ new BSSs
2. MME sets up path (allocates resources) to new BS
3. new BS allocates radio channel for mobile
4. new BS signals MME, old BS: ready
5. old BS tells mobile: perform handoff to new BS
6. mobile, new BS signal to activate new channel
7. mobile signals via new BS to MME: handoff complete. MME reroutes data/call
8 MME-old-BS resources released
Details on Active-State Handoff

- Initiated by old BS, assisted by the mobile device