MAC; Mobile and Wireless Networks

Outline

MW.1  Wireless and mobile networking concepts
MW.2  MAC functions and services
MW.3  MAC algorithms
MW.4  Wireless networks
MW.5  Mobile networks
MAC; Mobile and Wireless Networks

MW.1  Wireless & Mobile Networking Concepts

MW.1  Wireless and mobile networking concepts
MW.2  MAC functions and services
MW.3  MAC algorithms
MW.4  Wireless networks
MW.5  Mobile networks
Wireless Networks
Classification of Types

- Geographic scope
  - distance over which links operate
  - area of layer 2 subnetwork
- Mobility
  - mobility of wireless nodes
- Coördination
  - centralised vs. distributed control
Wireless Networks
Classification of Types: Scope

- Geographic scope
  - WBAN: wireless body area network
  - WPAN: wireless personal area network
  - WLAN: wireless local area network
  - WMAN: wireless metropolitan network
  - WRAN: wireless regional area network
  - WWAN: wireless wide area network

- Mobility
- Coördination
Wireless Networks
Classification of Types: Mobility

- **Geographic scope**
  - WBAN, WPAN, WLAN, WMAN, WRAN, WWAN

- **Mobility**
  - fixed: nodes are stationary
  - mobile: nodes are mobile
    - some nodes may be fixed (e.g. base stations)
  - nomadic: nodes are highly and routinely mobile
    - may be frequently out of range of one-another

- **Coordination**
Wireless Networks
Classification of Types: Mobility

- Geographic scope
  - WBAN, WPAN, WLAN, WMAN, WRAN, WWAN
- Mobility
  - fixed, mobile, nomadic
- Coördination
  - infrastructure: base station controls and transit traffic
  - ad hoc or peer-to-peer: mobile nodes directly communicate
Wireless Networks

Characteristics

- Wireless LANs very different from wired
  why?
Wireless Networks

Characteristics

- Wireless LANs very different from wired
  - always use shared medium
  - MAC is required
- Wireless characteristics
  - significant attenuation $1/r^2$
  - noise and interference
    - from one-another
    - from other devices
    - from environment
  - multipath reflections
    - reflections interfere with main signal
    - increases attenuation to $1/r^4$
Wireless Networks

Network Elements: Base Station

- **Base station** (BS)
  - fixed wireless node
    - one or more antennæ
    - may be small (e.g. home hub)
    - may have huge tower
  - range is frequently called a *cell*
  - typically connected to Internet via wired link
Wireless Networks
Network Elements: Base Station

- **Base station** (BS)
  - fixed wireless node
    - one or more antennae
    - may be small (e.g. home hub)
    - may have huge tower
  - range is frequently called a *cell*
  - typically connected to Internet via wired link
    - possibly wireless multipath through other BSs
Wireless Networks

Network Elements: Wireless Node

- **Base station** (BS)
- **Wireless node** (WN)
  - also called *untethered* node
  - no *wired* network connection
  - fixed or stationary node doesn’t move
  - wireless does *not* imply mobility
  - typical example: laptop personal computer
Wireless Networks
Network Elements: Wireless Link

- **Base station** (BS)
- **Wireless node** (WN)
- **Wireless link**
  - formed when 2 nodes in range *associate*
Network Elements: Wireless Link

- **Base station** (BS)
- **Wireless node** (WN)
- **Wireless link**
  - nodes associate
  - interconnects BSs
Wireless Networks

Network Elements: Wireless Link

- **Base station** (BS)
- **Wireless node** (WN)
- **Wireless link**
  - nodes associate
  - interconnects BSs
  - interconnects WNs to BSs
Wireless Networks

Network Elements: Wireless Link

- **Base station** (BS)
- **Wireless node** (WN)
- **Wireless link**
  - nodes associate
  - interconnects BSs
  - interconnects WNs to BSs
  - interconnects WNs peer-to-peer
MAC; Mobile and Wireless Networks

MW.2  MAC Functions and Services

MW.1  Wireless and mobile networking concepts
MW.2  MAC functions and services
MW.3  MAC algorithms
MW.4  Wireless networks
MW.5  Mobile networks
Medium Access Layer

Hybrid Layer/Plane Cube

MAC layer: arbitration to shared medium in control plane
Medium Access Layer

MAC Definition

- Medium access control (MAC) arbitrates a channel in shared medium (free space, guided wire, or fiber) among stations
• MAC protocol (or algorithm)
  – responsible for determining *when* node can transmit *frame*
  – may fully distributed or coördinated
MAC Layer
Service and Interfaces

- MAC is in between physical layer 1 and link layer 2
  - lower link sublayer in IEEE 802 model
- MAC layer is mostly in control plane
  - control over when to transmit a L2 frame
  - but may have its own encapsulation (e.g. IEEE 802 legacy)
    - layer 2 addresses needed for shared medium
- MAC layer service to link layer (L2)
  - MAC layer encapsulate/decapsulate if appropriate
  - initiate transfer of frame into the medium
MAC Layer
Service and Interfaces

- MAC layer *frame* may encapsulate link layer *frame*
  - done for link layer / MAC protocol independence
    - IEEE 802: 802.2 LLC (logical link control) over 802.N MAC
MAC; Mobile and Wireless Networks

MW.3  MAC Algorithms

MW.1  Wireless and mobile networking concepts
MW.2  MAC functions and services
MW.3  MAC algorithms
  MW.3.1  Channel partitioning
  MW.3.2  Coördinated access
  MW.3.3  Random access
  MW.3.4  Spread spectrum
MW.4  Wireless networks
MW.5  Mobile networks
Link Sharing
Multiplexing vs. Multiple Access

- Multiplexing vs. multiple access
- Link multiplexing
  - single transmitter
  - dedicated point-to-point link
- Multiple access:
  - multiple transmitters
  - shared medium
  - essentially physical layer multiplexing
  - MAC algorithm needed to arbitrate
MAC Algorithms

MW.3.1 Channel Partitioning

MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
  MW.3.1 Channel partitioning
  MW.3.2 Coördinated access
  MW.3.3 Random access
  MW.3.4 Spread spectrum
MW.4 Wireless networks
MW.5 Mobile networks
Channel Partitioning MAC

Introduction and Assumptions

- Channel has sufficient capacity
  - individual inter-station date rates less than channel capacity
- Multiple stations share a channel
Channel Partitioning MAC

Introduction and Assumptions

• Channel has sufficient capacity
  – individual inter-station date rates less than channel capacity
• Multiple stations share a channel
• Channel *partitioned* into pieces
  – pieces assigned to individual inter-station communication
  – MAC arbitrates
Channel Partitioning MAC

Introduction and Assumptions

- Channel has sufficient capacity
  - individual inter-station data rates less than channel capacity
- Multiple stations share a channel
- Channel *partitioned* into pieces
  - pieces assigned to individual inter-station communication
  - MAC arbitrates
- Contention-free MAC
  - partitioning ensures no contention *in* medium
    - subject to engineering and design, e.g. sufficient guard bands
Channel Partitioning MAC
Alternatives

- **TDMA**: time division multiple access
- **FDMA**: frequency division multiple access
  - typically refers to RF
  - **WDMA**: wavelength division multiple access (light)
- **CDMA**: code division multiple access
  - spread spectrum (later)
- **Note similarity to multiplexing schemes**
  - TDMA ~ TDM, FDMA ~ FDM, WDMA ~ WDM
  - essentially *distributed physical layer* versions of link muxing
Channel Partitioning MAC
Introduction and Assumptions

- Channel has sufficient capacity
  - individual inter-node date rates less than channel capacity
- Multiple nodes share a channel
- Channel *partitioned* into pieces
  - pieces assigned to individual inter-node communication
  - MAC arbitrates
Channel Partitioning MAC

TDMA

- TDMA: time division multiple access
- Channel divided into \( n \) time slots
  - served cyclically
  - generally equal size
  - within a frequency band
Channel Partitioning MAC

TDMA

• TDMA: time division multiple access
• Channel divided into $n$ time slots
  – served cyclically
  – generally equal size
  – within a frequency band
• MAC arbitrates how nodes assigned to slots
  – static TDMA: slots reserved for particular links
  – dynamic TDMA: slots scheduled based on traffic demand
Channel Partitioning MAC

FDMA

- FDMA: frequency division multiple access
- Channel divided into *n* frequency bands
  - generally of equal bandwidth
  - over period of time
Channel Partitioning MAC

FDMA

• FDMA: frequency division multiple access
• Channel divided into $n$ frequency bands
  – generally of equal bandwidth
  – over period of time
• MAC arbitrates how nodes assigned to frequencies
  – static
  – dynamic
Channel Partitioning MAC

WDMA

• Medium: fiber optic cable
• Channel divided into wavelengths
• MAC arbitrates how stations assigned to wavelengths
  – example: multiple transmitters attached to *star coupler*
• Distinction from WDM
  – WDM multiplexing determined by higher layers
    • e.g. network layer assignment of flows to wavelengths
  – distinction between WDM and WDMA subtle
Channel Partitioning MAC

**OFDMA**

- **OFDMA**: orthogonal freq. div. multiple access
  - based on OFDM using multiple carriers
- **Channel consists of frequency band**
  - divided into closely spaced carriers
  - adjacent carriers non-interfering: *orthogonal*
- Each link assigned *subset* of carriers
- MAC arbitrates how stations carrier subset
Channel Partitioning MAC

Link Duplexing

- **Link types**
  - half duplex: unidirectional hop-by-hop transfer
  - full duplex: bidirectional hop-by-hop transfer

- **Most communication requires full duplex link**
  - even unidirectional data transfer

*why?*
Channel Partitioning MAC
Link Duplexing

- **Link types**
  - half duplex: unidirectional hop-by-hop transfer
  - full duplex: bidirectional hop-by-hop transfer

- **Most communication requires full duplex link**
  - even unidirectional data transfer
  - control messages such as ACKs for ARQ
    - may be highly asymmetric
Channel Partitioning MAC

Link Duplexing

- Link types
  - half duplex: unidirectional hop-by-hop transfer
  - full duplex: bidirectional hop-by-hop transfer

- Most communication requires full duplex link
  - even unidirectional data transfer
  - control messages such as ACKs for ARQ
    - may be highly asymmetric
  - Alternative strategies for full duplex
    - separate end-to-end paths

problem?
Channel Partitioning MAC

Link Duplexing

- **Link types**
  - half duplex: unidirectional hop-by-hop transfer
  - full duplex: bidirectional hop-by-hop transfer

- **Most communication requires full duplex link**
  - even unidirectional data transfer
  - control messages such as ACKs for ARQ
    - may be highly asymmetric
  - Alternative strategies for full duplex
    - separate distinct end-to-end paths through network
      - may have different loss & delay properties
      - may be necessary in some cases (e.g. satellite)
Channel Partitioning MAC

Link Duplexing

- **Link types**
  - half duplex: unidirectional hop-by-hop transfer
  - full duplex: bidirectional hop-by-hop transfer

- **Most communication requires full duplex link**
  - even unidirectional data transfer
  - control messages such as ACKs for ARQ
    - may be highly asymmetric
  - **Alternative strategies for full duplex**
    - separate distinct end-to-end paths through network
    - paired unidirectional links in same guided media
      - e.g. 2×twisted-pair, 2×fiber
Channel Partitioning MAC
Link Duplexing

- Link types
  - half duplex: unidirectional hop-by-hop transfer
  - full duplex: bidirectional hop-by-hop transfer

- Most communication requires full duplex link
  - even unidirectional data transfer
  - control messages such as ACKs for ARQ
    - may be highly asymmetric

- Alternative strategies for full duplex
  - separate distinct end-to-end paths through network
  - paired unidirectional links in same guided media
  - sharing same media (e.g. fiber or free space)
Channel Partitioning MAC
Frequency Division Duplexing

- **Duplexing**: bidirectional transmission sharing media
- **FDD**: *frequency division duplexing*
  - forward and reverse traffic assigned to *different* freq. bands

*advantages and disadvantages?*
Channel Partitioning MAC
Frequency Division Duplexing

- Duplexing: bidirectional transmission sharing media
- FDD: frequency division duplexing
  - forward and reverse traffic assigned to different freq. bands
  - simple scheme
  - no collisions between forward and reverse packets
  - less efficient use of spectrum under light load
Channel Partitioning MAC

Time Division Duplexing

- Multiplexing in time and space for full duplex
  - bidirectional data transmission
- FDD: frequency division duplexing
- TDD: time division duplexing
  - forward and reverse traffic assigned to same freq. bands

Advantages and disadvantages?
Channel Partitioning MAC

Time Division Duplexing

- Multiplexing in time and space for full duplex
  - bidirectional data transmission
- FDD: frequency division duplexing
- TDD: time division duplexing
  - forward and reverse traffic assigned to *same* freq. bands
  - slots divided between upstream and downstream traffic
  - asymmetric traffic needs dynamic bandwidth adjustment
  - operates in conjunction with various channel multiplexing
    - eg. TDD within FDMA
Channel Partitioning MAC

Advantages and Disadvantages

- Channel partitioning

advantages and disadvantages?
Channel Partitioning MAC
Advantages and Disadvantages

- Channel partitioning advantages
  - simple mechanism
  - inherently fair with respect to station sharing
  - best under high uniform and deterministic load
Channel Partitioning MAC
Advantages and Disadvantages

• Channel partitioning advantages
  – simple mechanism
  – inherently fair with respect to station sharing
  – best under high uniform and deterministic load

• Channel partitioning disadvantages
  – per flow fairness more difficult
  – inefficient under low load
    • $1/n$ of channel bandwidth unless multiple partitions/station
  – inefficient under high-nondeterministic load
    • distributed partition assignment difficult
    • multiple or variable partition sizes difficult to manage
Channel Partitioning MAC
SDMA and Directional Antennæ

• Assumption so far
  – omnidirectional antennæ radiate in all directions

*problem?
Channel Partitioning MAC
SDMA and Directional Antennae

• Assumption so far
  – omnidirectional antennæ radiate in all directions
  – radiate even where not needed
  – reduce channel capacity

• Directional antennæ
  – radiate focused beam toward receiver
  – reduce power use
  – reduce interference: spatial reuse

• SDMA: space division multiple access MAC
  – complexity of beam steering and station tracking
## Channel Partitioning MAC Characteristics

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Channel Partitioning</th>
<th>Coordinated Access</th>
<th>Random Access</th>
<th>Spread Spectrum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types</td>
<td>TDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td>low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Tolerance</td>
<td>high deterministic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence of Contention</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resilience</td>
<td>poor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examples</td>
<td>802.16 mesh</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MAC Algorithms
MW.3.2 Coördinated Access MAC

MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
  MW.3.1 Channel partitioning
  MW.3.2 Coördinated access
  MW.3.3 Random access
  MW.3.4 Spread spectrum
MW.4 Wireless networks
MW.5 Mobile networks
Coordinated Access MAC
Introduction and Assumptions

- Channel has sufficient capacity
  - individual inter-station data rates less than channel capacity
- Multiple stations share a channel
Coordinated Access MAC

Introduction and Assumptions

• Channel has sufficient capacity
  – individual inter-station data rates less than channel capacity

• Multiple stations share a channel

• Stations use channel for a period of time
  – in a fully highly coordinated manner
    • central controller (e.g. polling)
    • algorithmic turn taking (e.g. token passing)
  – MAC arbitrates

[Kurose & Ross] call this *taking turns* MAC
Coordinated Access MAC
Polling

- Controller grants channel access to station
  - each station *pollled* to determine if it needs to transmit
Coordinated Access MAC

Token Passing

- Token grants channel access to station
  - token passed between stations
  - generally round robin

- Topologies
  - bus
    - IEEE 802.4 never successful
  - natural ring interconnection
    - IEEE 802.5
Coordinated Access MAC
Token Passing Resilience

- Token ring interface
  - inserted in the ring

*what happens when station turned off?*
Coordinated Access MAC

Token Passing Resilience

- Token ring interface
  - inserted in the ring
  - relay required to close circuit
Coordinated Access MAC
Token Passing Resilience

- Token ring interface
  - inserted in the ring
  - relay required to close circuit
- Resilience to ring cuts
  *problems?*
Coordinated Access MAC
Token Passing Resilience

- Token ring interface
  - inserted in the ring
  - relay required to close circuit

- Resilience to ring cuts
  - user unplugging station cuts ring
Coordinated Access MAC
Token Passing Resilience

- Token ring interface
  - inserted in the ring
  - relay required to close circuit
- Resilience to ring cuts
  - user unplugging station cuts ring
  - dual ring resilient to single cut
    - stations wrap to second ring
Coördinated Access MAC
Advantages and Disadvantages

- Channel partitioning
  - simple mechanism, best for high uniform load
- Coördinated access

*advantages and disadvantages?*
Coördinated Access MAC
Advantages and Disadvantages

• Channel partitioning
  – simple mechanism, best for high uniform load

• Coördinated access advantages
  – nondeterministic algorithm good for nonuniform loads
  – balances benefits of partitioning and random access
  – good for relatively high load
Coördinated Access MAC
Advantages and Disadvantages

• Channel partitioning
  – simple mechanism, best for high uniform load

• Coördinated access advantages
  – nondeterministic algorithm good for nonuniform loads
  – balances benefits of partitioning and random access
  – good for relatively high load

• Coördinated access disadvantages
  – relatively complex network interface
### Coördinated Access MAC Characteristics

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Channel Partitioning</th>
<th>Coördinated Access</th>
<th>Random Access</th>
<th>Spread Spectrum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types</td>
<td>TDMA</td>
<td>token ring polling</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td>low</td>
<td>high</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Tolerance</td>
<td>high deterministic</td>
<td>higher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence of Contention</td>
<td>–</td>
<td>degradation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resilience</td>
<td>poor</td>
<td>wired: moderate</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>wireless: poor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examples</td>
<td>802.16 mesh</td>
<td>802.5 TR</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MAC Algorithms
MW.3.3 Random Access MAC

MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
  MW.3.1 Channel partitioning
  MW.3.2 Coördinated access
  MW.3.3 Random access
  MW.3.4 Spread spectrum
MW.4 Wireless networks
MW.5 Mobile networks
Random Access MAC
Introduction and Assumptions

• Channel has sufficient capacity
  – individual inter-station data rates less than channel capacity
• Multiple stations share a channel
• Stations use channel for a period of time
  – generally entire channel (baseband access)
  – in a fully distributed (random) manner
    • similar to statistical TDM
  – MAC arbitrates

*What is simplest possible random access MAC?*
Random Access MAC

ALOHA

- **ALOHA**: 1970s radio network among Hawaiian islands
- Senders transmit whenever they have data (no MAC)

- **Performance metrics**
  - channel efficiency
    - what fraction of transmission attempts are successful
  - channel throughput
    - what is the maximum *carried load* of the channel?
Random Access MAC

ALOHA

- ALOHA: 1970s radio network among Hawaiian islands
- Senders transmit whenever they have data (no MAC)

- Problem
  - collisions: transmissions interfere with one another
Random Access MAC

ALOHA

- ALOHA: 1970s radio network among Hawaiian islands
- Senders transmit whenever they have data (no MAC)

Problem
  - collisions: transmissions interfere with one another
  - even if only very small overlap
Random Access MAC

ALOHA

- ALOHA: 1970s radio network among Hawaiian islands
- Senders transmit whenever they have data (no MAC)

Problem
  - *collisions*: transmissions interfere with one another
  - even if only very small overlap

*can we do better?*
Random Access MAC
Slotted ALOHA

- ALOHA: 1970s radio network among Hawaiian islands
- Senders transmit whenever they have data in slot

- Problem
  - *collisions*: transmissions interfere with one another
  - improvement: divide time into *slots*
Random Access MAC
Slotted ALOHA

- ALOHA: 1970s radio network among Hawaiian islands
- Senders transmit whenever they have data in slot

- Problem
  - collisions: transmissions interfere with one another
  - improvement: divide time into slots
  - delay transmissions to next slot time
Random Access MAC

Slotted ALOHA

- ALOHA: 1970s radio network among Hawaiian islands
- Senders transmit whenever they have data in slot

- Problem
  - collisions: transmissions interfere with one another
  - improvement: divide time into slots
  - delay transmissions to next slot time
  - slotted time reduces probability of collisions
Random Access MAC
Unslotted vs. Slotted Performance

- Slotting approximately doubles performance
  - slotted: Throughput = $Ge^{-G}$
  - unslotted: Throughput = $Ge^{-2G}$
Random Access MAC

Challenges

• Multiple nodes must be able to share channel
• When 2 or more nodes *simultaneously* transmit
  – signals garbled in a *collision*: none of them are successful
• How to arbitrate among them?
  – MAC algorithm

*How can we do better than random transmission?*
Random Access MAC

Contestation

- *Contention-based* or *random-access* MAC
  - nodes transmit when they have data
  - subject to MAC
    - per frame decision
    - analogue to connectionless service
  - *collisions* possible
  - efficient channel utilisation
    - in the absence of collisions
Random Access MAC
Contention and Collisions

What is the simplest way to reduce collisions?
Random Access MAC

CSMA (1-persistant)

• CSMA – *carrier sense* multiple access
  – nodes can sense if channel is in use by another station
  – wait to transmit to avoid collision
  – human analogy: don’t interrupt others already speaking

• 1-persistant CSMA
  – wait until channel free, then transmit
    (transmit with probability 1)

*Problem? How can we do better?*
Random Access MAC
CSMA (non- and $p$-persistent)

- Problem: synchronisation of collisions
  - waiting nodes will *all* transmit as soon as channel free
- Two options:
- Non-persistent CSMA
  - if carrier sensed wait random period before trying again
    (rather than continuously sensing until channel free)
  - better utilisation, but delayed even when unnecessary
- $p$-persistent CSMA (for slotted time)
  - continuously sense carrier until channel is available
  - but with only with probability $p$ transmit on next slot
CSMA
Collisions

- Collisions occur even with carrier sense
  - due to propagation delay
  - sender may not know channel already in use
CSMA

Collisions

- Collisions still occur
  - due to propagation delay
  - sender may not know channel already in use
- Pr[collision] incr. w/ length
  - B & D don’t know other xmit
CSMA Collisions

- Collisions still occur
  - due to propagation delay
  - sender may not know channel already in use
- Pr[collision] incr. w/ length
  - B & D don’t know other xmit
  - until signals meet near C
  - and return
- Inefficient
  - channel used by garbage

Can we do better?
CSMA/CD
Collision Detection

- CSMA/CD: CSMA with *collision detection*
  - station detecting a collision immediately ceases transmission
  - human analogy: polite conservationist
- Worst case CD takes *twice* media propagation delay
  - A transmits packet
CSMA/CD
Collision Detection

- **CSMA/CD**: CSMA with *collision detection*
  - station detecting a collision immediately ceases transmission
  - human analogy: polite conservationist
- **Worst case CD takes** *twice* media propagation delay
  - A transmits packet
CSMA/CD
Collision Detection

- CSMA/CD: CSMA with collision detection
  - station detecting a collision immediately ceases transmission
  - human analogy: polite conservationist
- Worst case CD takes twice media propagation delay
  - A transmits packet
  - B transmits packet just before A reaches B
CSMA/CD
Collision Detection

- CSMA/CD: CSMA with *collision detection*
  - station detecting a collision immediately ceases transmission
  - human analogy: polite conservationist
- Worst case CD takes *twice* media propagation delay
  - A transmits packet
  - B transmits packet just before A reaches B
  - A+B interference travels back to A
CSMA/CD
Collision Detection Efficiency

- CD frees channel earlier
  \[ \frac{1}{1 + 5 \frac{t_{\text{prop}}}{t_{\text{trans}}}} \]
  \( t_{\text{prop}} \) max prop between nodes
  \( t_{\text{trans}} \) time to transmit max frame

- Efficiency
  \( \rightarrow 1 \) as \( t_{\text{prop}} \rightarrow 0 \)
  \( \rightarrow 1 \) as \( t_{\text{trans}} \rightarrow \infty \)
CSMA/CD
Collision Detection Efficiency

- CD frees channel earlier
  \[ \frac{1}{1 + 5 \frac{t_{prop}}{t_{trans}}} \]
  \( t_{prop} \) max prop between nodes
  \( t_{trans} \) time to transmit max frame

- Efficiency
  \[ \rightarrow 1 \text{ as } t_{prop} \rightarrow 0 \]
  \[ \rightarrow 1 \text{ as } t_{trans} \rightarrow \infty \]

- Much better than CSMA
  - still decentralized, simple, and cheap
  \( problem? \)
CSMA/CD

Backoff

• If stations *all* transmit after backoff, same problem
  – need some way of un-synchronising retransmissions

*How?*
CSMA/CD
Exponential Backoff

• If stations *all* transmit after backoff, same problem
  – need some way of un-synchronising transmissions

• Exponential backoff:
  – stations wait a *random* number of slot times before retrying
  – binary exponential distribution:
    $n$th collision wait randomly among $\{0...2^{n-1}\}$ slots
    1st collision: wait 0 or 1 slots
    2nd collision: wait 0, 1, 2, or 3 slots
    ...
  – low load: minimise delay
    moderate load: spread retries
CSMA/CD Problems

Problems?
CSMA/CD

Problems: Collision Detection and Carrier Sense

Problem with collision detection?
CSMA/CD
Problem with Collision Detection

- Problems with collision detection
  - station must be able to simultaneously transmit and receive
    - requires full duplex
  - not possible for single wireless tranceiver at given frequency
- *CSMA/CD not appropriate for wireless networks*
  - Ethernet evolution eliminated vast majority of CSMA/CD
CSMA
Problem with Carrier Sense

- CSMA/CD not appropriate for wireless networks

*Problem with carrier sense?*
CSMA
Problem with Carrier Sense

- CSMA/CD not appropriate for wireless networks
- Problem with carrier sense
  - only appropriate when all nodes within range
  - typically not the case for wireless networks
  problem?
CSMA
Problem with Carrier Sense

• CSMA/CD not appropriate for wireless networks
• Problem with carrier sense
  – only appropriate when \textit{all} nodes within range
  – typically \textit{not} the case for wireless networks
  – problem: hidden nodes
CSMA
Hidden Nodes

- *Hidden nodes* (terminals)
  - some nodes are hidden from one another
  - out of transmission range
  - unaware that they are causing collisions with hidden node
CSMA
Hidden Nodes

- Hidden node problem
CSMA
Hidden Nodes

- Hidden node problem
  - A can communicate with B
CSMA
Hidden Nodes

- Hidden node problem
  - A can communicate with B
  - C can communicate with B
CSMA
Hidden Nodes

- Hidden node problem
  - A can communicate with B
  - C can communicate with B
  - A can not communicate with C
CSMA
Hidden Nodes

• Hidden node problem
  – A can communicate with B
  – C can communicate with B
  – A can not communicate with C
    • unaware of interference at B
CSMA

Hidden Nodes

• Hidden node problem
  – A can communicate with B
  – C can communicate with B
  – A cannot communicate with C
    • unaware of interference at B

• Causes of hidden nodes
  – line-of-sight obstructions
CSMA

Hidden Nodes

- Hidden node problem
  - A can communicate with B
  - C can communicate with B
  - A cannot communicate with C
    - unaware of interference at B

- Causes of hidden nodes
  - line-of-sight obstructions
  - signal attenuation
    - limited transmission range
CSMA
Exposed Nodes

- *Exposed nodes* (terminals)
  
  *problem?*
CSMA
Exposed Nodes

- *Exposed nodes* (terminals)
  - some nodes are in range of one another
  - prevent transmission because collision assumed
CSMA

Exposed Nodes

- *Exposed nodes* (terminals)
  - some nodes are in range of one another
  - prevent transmission because collision assumed

- Example:
  - B transmitting to C
CSMA
Exposed Nodes

- **Exposed nodes** (terminals)
  - some nodes are in range of one another
  - prevent transmission because collision assumed

- **Example:**
  - B transmitting to C
  - but A hears B: won’t transmit due to CA
**CSMA**

Exposed Nodes

- *Exposed nodes* (terminals)
  - some nodes are in range of one another
  - prevent transmission because collision assumed

- **Example:**
  - B transmitting to C
  - but A hears B: won’t transmit due to CA
  - even though it could to D without jamming B→C
CSMA
Exposed Nodes

- *Exposed nodes* (terminals)
  - some nodes are in range of one another
  - prevent transmission because collision assumed

*Solution?*
CSMA
Exposed Nodes

- *Exposed nodes* (terminals)
  - some nodes are in range of one another
  - prevent transmission because collision assumed
- Spatial reuse necessary
  - *directional antennae* one strategy

---

EECS 882
CSMA
Alternative Improvement to CD

- CSMA/CD not practical for wireless networks
  - full duplex problem
  - hidden terminal problem

*Alternatives that are still better than (pure) CSMA?*
CSMA
Collision Avoidance

• *Collision avoidance* (CA)
  – attempt to avoid collision (but don’t detect once occurs)
CSMA
Collision Avoidance: Floor Acquisition

- Floor acquisition (FAMA: floor access multiple access)
  - efficient negation to determine which node transmits
  - may be in-band or out-of band (e.g. signalling frequency)
  - similar to audio conference floor acquisition protocols
MACA: multiple access with collision avoidance
  – in-band floor acquisition

How?
CSMA/CA

MACA

- MACA: multiple access with collision avoidance
  - in-band floor acquisition
- MACA operation (analogy: teleconference “may I”)
  - sender transmits RTS (request to send) if no carrier sense
CSMA/CA

MACA

- MACA: multiple access with collision avoidance
  - in-band floor acquisition
- MACA operation
  - sender transmits RTS (request to send)
  - intended receiver replies with CTS (clear to send)
  - all nodes in range of both will detect at least 1 of RTS/CTS
MACA: multiple access with collision avoidance
- in-band floor acquisition

MACA operation
- sender transmits RTS (request to send)
- intended receiver replies with CTS (clear to send)
- all nodes in range of both will detect at least 1 of RTS/CTS
- if sender receives clear CTS it can transmit
MACAW: MACA for wireless

- CSMA/CA
- data frames acknowledged
- exponential backoff per send/receive pair
- modified backoff algorithm
## Random Access MAC Characteristics

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Channel Partitioning</th>
<th>Coordinated Access</th>
<th>Random Access</th>
<th>Spread Spectrum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types</td>
<td>TDMA</td>
<td>token ring polling</td>
<td>ALOHA, slot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FDMA</td>
<td></td>
<td>CSMA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WDMA</td>
<td></td>
<td>CD, CA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td>low</td>
<td>high</td>
<td>low</td>
<td></td>
</tr>
<tr>
<td>Load Tolerance</td>
<td>high deterministic</td>
<td>higher</td>
<td>lower</td>
<td></td>
</tr>
<tr>
<td>Consequence of Contention</td>
<td>–</td>
<td>degradation</td>
<td>collisions</td>
<td></td>
</tr>
<tr>
<td>Resilience</td>
<td>poor</td>
<td>wired: moderate</td>
<td>poor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>wireless: poor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examples</td>
<td>802.11</td>
<td>802.5 TR</td>
<td>Ethernet 802.11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>802.16 mesh</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MAC Algorithms

MW.3.4 Spread Spectrum MAC

MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
  MW.3.1 Channel partitioning
  MW.3.2 Coördinated access
  MW.3.3 Random access
  MW.3.4 Spread spectrum

MW.4 Wireless networks
MW.5 Mobile networks
Spread Spectrum MAC

Introduction and Assumptions

- Channel has sufficient capacity
  - individual inter-station data rates less than channel capacity
- Multiple stations share a channel
- Stations use channel for a period of time
Spread Spectrum MAC
Introduction and Assumptions

- Channel has sufficient capacity
  - individual inter-station data rates less than channel capacity
- Multiple stations share a channel
- Stations use channel for a period of time
- Transmission *spread* in frequency spectrum
  - coding techniques avoid interference
- CDMA: code division multiple access
Spread Spectrum MAC

**CDMA**

- **CDMA**: code division multiple access
- **Channel use different codes**
  - in a given **frequency band**
  - over **period of time**
- **Analogy**: speaking
  - English, German, Chinese, Hindi
  - in the same room at the same time
  - easier to converse in a given language (code) if interference is in different languages (codes)
Spread Spectrum MAC

CDMA Types

• Direct sequence (DS)
  - symbols multiplied by higher frequency chipping sequence

• Frequency hopping (FH)
  - transmissions rapidly hop among different frequency carriers
    • pseudorandom sequence negotiated between tranceivers
Spread Spectrum MAC
DS CDMA Concepts

• All stations share same frequency band
  – unique code assigned to each station

• Each station has its own *chipping* sequence
  – unique code at chipping rate
  – encoded signal = (original data) \( \times \) (chipping sequence)
  – decoding: inner-product of encoded signal and chipping seq.

• Multiple stations transmit simultaneously
  – minimal interference if codes are *orthogonal*

*analogy*: [suggested by D. Broyles]
*conversations at the same time in different languages*
Spread Spectrum MAC
DS CDMA Encode/Decode Example

\[ Z_{i,m} = d_i \cdot c_m \]

\[ D_i = \sum_{m=1}^{M} Z_{i,m} \cdot c_m \]

[Kurose & Ross]
Spread Spectrum MAC
DS CDMA Decode Example with Interference

senders

data bits
\begin{align*}
d_1^1 &= -1 \\
d_2^1 &= -1
\end{align*}

code
\begin{align*}
1 &1 &1 &1 \\
1 &1 &1 &1 \\
1 &1 &1 &1
\end{align*}

channel, \( Z_{i,m}^* \)
\begin{align*}
2 &2 &2 &2 &2 &2
\end{align*}

\[
Z_{i,m}^1 = d_i^1 \cdot c_m^1
\]

\[
Z_{i,m}^2 = d_i^2 \cdot c_m^2
\]

receiver 1

\[
d_i^1 = \sum_{m=1}^{M} Z_{i,m}^* \cdot c_m^1
\]

\[
d_i = -1
\]
## Spread Spectrum MAC Characteristics

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Channel Partitioning</th>
<th>Coordinated Access</th>
<th>Random Access</th>
<th>Spread Spectrum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types</td>
<td>TDMA FDMA WDMA SDMA</td>
<td>token ring polling</td>
<td>ALOHA, slot CSMA</td>
<td>CDMA FH, DS</td>
</tr>
<tr>
<td>Complexity</td>
<td>low</td>
<td>high</td>
<td>low</td>
<td>high</td>
</tr>
<tr>
<td>Load Tolerance</td>
<td>high deterministic</td>
<td>higher</td>
<td>lower</td>
<td>varies</td>
</tr>
<tr>
<td>Consequence of Contention</td>
<td>–</td>
<td>degradation</td>
<td>collisions</td>
<td>degradation</td>
</tr>
<tr>
<td>Resilience</td>
<td>poor</td>
<td>wired: moderate</td>
<td>poor</td>
<td>resistant to</td>
</tr>
<tr>
<td>Examples</td>
<td>802.11 802.16</td>
<td>802.5 TR</td>
<td>Ethernet</td>
<td>802.11</td>
</tr>
</tbody>
</table>
MAC; Mobile and Wireless Networks

MW.4  Wireless Networks

MW.1  Wireless and mobile networking concepts
MW.2  MAC functions and services
MW.3  MAC algorithms
MW.4  Wireless networks
   MW.4.1  802.11 WLAN
   MW.4.2  802.16 WMAN and WiMAX
   MW.4.3  802.15 WPAN and Bluetooth
   MW.4.4  Sensor networks
MW.5  Mobile networks
Wireless Networks

802 Protocols by Geographical Scope

- IEEE 802.15  WPAN
- IEEE 802.11  WLAN
- IEEE 802.16  WMAN
Wireless Networks
MW.4.1  802.11 WLAN

MW.1  Wireless and mobile networking concepts
MW.2  MAC functions and services
MW.3  MAC algorithms
MW.4  Wireless networks
    MW.4.1  802.11 WLAN
    MW.4.2  802.16 WMAN and WiMAX
    MW.4.3  802.15 WPAN and Bluetooth
    MW.4.4  Sensor networks
MW.5  Mobile networks
Wireless Networks: WLAN
802.11 Overview

• IEEE 802.11
  – wireless links based loosely on Ethernet framing
    • 6B MAC addresses, 4B FCS
    • 802.2 SNAP/LLC subheader
      – enables simple cheap 802.3+802.11 hubs and switches
  • Unlicensed ISM/U-NII bands: 900 MHz, 2.4, 5.8 GHz
    – significant interference from FHSS 2.4 GHz cordless phones
  • Additional licensed bands: 3.7 GHz
Wireless Networks: WLAN

802.11 Relation to other 802 Wireless Protocols

- **IEEE 802.11**
  - first of the 802 wireless protocols
  - design motivated by Ethernet
    - sometimes called “wireless Ethernet”
Wireless Networks: WLAN

Wi-Fi Overview

- Wi-Fi
  - Wi-Fi alliance: www.wi-fi.org
    - note capitalisation and hyphen: Wi-Fi not WiFi nor Wifi
  - 802.11 standards compliance and interoperability testing
  - commonly (but incorrectly) used as synonym for 802.11

Wi-Fi ≠ 802.11!
802.11 WLAN
Deployment Scenarios

Motivation for deploying WLANs?
802.11 WLAN
Deployment Scenarios

• Motivation for WLAN deployment
  – cheaper than running Ethernet cables for desktops
  – allows untethered access for laptops and PDAs
802.11 WLAN
Deployment Scenarios

• Motivation for WLAN deployment
  – cheaper than running Ethernet cables for desktops
  – allows untethered access for laptops and PDAs

• Deployment scenarios
  – home networks
    • frequently the only network infrastructure
      *why?
802.11 WLAN
Deployment Scenarios

• Motivation for WLAN deployment
  – cheaper than running Ethernet cables for desktops
  – allows untethered access for laptops and PDAs

• Deployment scenarios
  – home networks
    • frequently the only network infrastructure
    • most homes not wired for networking
802.11 WLAN
Deployment Scenarios

- Motivation for WLAN deployment
  - cheaper than running Ethernet cables for desktops
  - allows untethered access for laptops and PDAs

- Deployment scenarios
  - home networks
  - office buildings
    - generally supplements wired LANs
      \textit{why?}
802.11 WLAN
Deployment Scenarios

- Motivation for WLAN deployment
  - cheaper than running Ethernet cables for desktops
  - allows untethered access for laptops and PDAs

- Deployment scenarios
  - home networks
  - office buildings
  - hotel lobbies, meeting rooms, classrooms, outdoor areas
    - large spaces impractical to wire
802.11 WLAN Deployment Scenarios

- Motivation for WLAN deployment
  - cheaper than running Ethernet cables for desktops
  - allows untethered access for laptops and PDAs

- Deployment scenarios
  - home networks
  - office buildings
  - hotel lobbies, meeting rooms, classrooms, outdoor area
  - wireless *hotspots*
    - free service to draw customers (e.g. Starbucks, McDonald’s)
    - free public service (e.g. MCI airport)
    - for-profit service (e.g. T-Mobile)
802.11 WLAN Deployment Scenarios

- Motivation for WLAN deployment
  - cheaper than running Ethernet cables for desktops
  - allows untethered access for laptops and PDAs

- Deployment scenarios
  - home networks
  - office buildings
  - hotel lobbies, meeting rooms, classrooms, outdoor area
  - wireless hotspots
  - public Internet service
    - free public service (e.g. Lancaster University)
    - fee-based service (e.g. Lawrence Freenet)
802.11 WLAN Standards Overview

- **802.11-2007**: current version of base standard
  - consists of 802.11-1999 +
    - 802.11a: 5.8 GHz high rate
    - 802.11b: 2.4 GHz higher rate (formerly most common)
    - 802.11e: QoS enhancements
    - 802.11g: 2.4 GHz further higher rate (currently most common)
    - 802.11i: security enhancements
  - recall that TGs get alpha-suffix in order of formation

- **802.11n**: draft standard for high rate MIMO
- **802.11r**: standard for fast roaming between BSs
- **802.11s**: draft standard for mesh networking
- **802.11y**: standard for 3.7 GHz 20W licensed
802.11 WLAN
Generic Frame Format

- **MAC Header** [30B]
  - frame control [2B]
  - duration/ID [2B]
  - address 1 [6B]
  - address 2 [6B]
  - address 3 [6B]
  - sequence control [6B]
  - address 4 [6B]
- **Frame body** [0–2312B]
- **Trailer: FCS** [4B]
802.11 WLAN
Header Format: Frame Control Type

- **Frame control** [2B]
  - protocol version [2b] = 00
  - type [2b]
    - 00 = management
    - 01 = control
    - 10 = data
    - 11 = reserved
  - subtype [4b]
    - dependent on type
802.11 WLAN
Header Format: Frame Control Addresses

- **Address n** [6B]
  - IEEE 802-1990 MAC address
  - types:
    - individual station address
    - multicast group 01-XX-XX-XX-XX-XX
    - broadcast address FF-FF-FF-FF-FF-FF
  - fields dependent on frame control type
    - BSSID: BSS AP address
    - DA: destination address (final recipient)
    - SA: source address of frame (individual)
    - RA: (immediate) receiver address
    - TA: transmitter address
802.11 WLAN
Body Format

- **Frame body** [0–2312B]
  - variable length
  - not present in control frames
802.11 WLAN
Trailer Format: CRC

- **FCS** \([4B]\)
  - frame check sequence
  - CRC-32
Management Frame

- Management frame (type=01 subtype [4b]):
  - beacon
  - (re)association
    - request
    - response
  - probe
    - request
    - response
  - disassociation
  - (de)authentication
802.11 WLAN
Control Frame

- Control frame (type=01 subtype [4b]):
  - collision avoidance
    - 1011 RTS
    - 1100 CTS
  - data transfer
    - 1101 ACK
    - 1000 BlockAckReq (802.11n)
    - 1001 BlockAck (802.11n)
  - contention free operation
    - 1110 CF-end
    - 1111 CF-end+CF-ACK
  - power save
    - 1010 PS-poll
802.11 WLAN
Data Frame

- Data frame (type=10)
  - duration (μs)
  - SA: source address
  - DA: destination address
  - BSSID of access point
  - sequence control
  - frame body
    - LLC/SNAP
    - payload
  - FCS
    - CRC-32
802.11 WLAN

Link Types

- IEEE 802.11: original 802.11 links at 1–2 Mb/s
- IEEE 802.11b, 802.11a: second set of link standards
- IEEE 802.11g: third link standard
- IEEE 802.11y: licensed 3.7 GHz
- IEEE 802.11n: current with 100 Mb/s link rate
- Typically referred to by temporary standard number
  - even after folded into 802.11 revision
  - e.g. 802.11a, 802.11b, 802.11g in 802.11-2007
802.11 WLAN

Link Types: 802.11b

- IEEE 802.11b
  - 2.4 GHz ISM/U-NII band
  - formerly widest deployment
  - 11 Mb/s maximum MAC rate
    - actual performance *highly* dependent on environment
    - 5Mb/s goodput typical over 60m range with few obstructions
    - adequate for most home, SOHO, and hotspot use
    - exceeds rate of HFC and DSL access links
  - DSSS coding; all stations use same chipping sequences
    - *what does this mean?*
802.11 WLAN
Link Types: 802.11a

- IEEE 802.11a
  - 5.8 GHz ISM/U-NII band
    - higher rate alternative to 802.11b but more expensive
    - simultaneously available with 802.11b
      - a and b were IEEE 802.11 working group numbers
  - 54 Mb/s maximum MAC rate
    - actual performance *highly* dependent on environment
    - 24Mb/s goodput over 35m range typical
  - deployment limited to users that needed higher rate
    - high rate LAN applications
    - users and campuses with higher rate Internet access links
      - e.g. T3, 100M/1G Ethernet, SONET
802.11 WLAN
Link Types: 802.11g

- IEEE 802.11g
  - 2.4 GHz ISM/U-NII band
    - backward compatible with 802.11b
    - higher rate successor to 802.11b using OFDM
  - 54 Mb/s maximum MAC rate
    - actual performance highly dependent on environment
  - has become most common deployment
    - virtually all laptops and hubs are now 802.11g
    - many are a/b/g compatible
802.11 WLAN
Link Types: 802.11y

- **IEEE 802.11y**
  - 3 GHz *licensed* band
  - FCC “lite” licensing
    - nationwide license with non-interference requirements
  - 20mW
    - higher power for backhaul
    - e.g. hotspot meshing for city-wide 802.11 service
  - currently going through standards process
802.11 WLAN
Link Types: 802.11n

- **IEEE 802.11n**
  - current 802.11 bleeding edge
  - MAC rate of at least 100Mb/s
  - MIMO (multiple-input multiple-output) antenna technology

- **Draft standard agreed**
  - based on EWC proposal (Enhanced Wireless Consortium)
  - merge of competing TgnSync and WWiSE proposals

- **Many draft-compliant products now available**
  - e.g. MacBooks come with 802.11n built in
802.11 WLAN
Link Types: Future

• Work beginning on next versions of 802.11 links
  – 802.11 VHT (very high throughput) SG (study group)
• Diminishing returns possible in 2.4 and 5.8 GHz
  – next ISM bands at ~ 24 and 61 GHz
  – 802.15.3c standardising in 60 GHz band
• VHT split into two task groups
  – 802.11ac for < 6 GHz
  – 802.11ad for 60 GHz
802.11 WLAN
Link Types: 802.11ac

- IEEE 802.11ac under development
  - < 6 GHz (5.8 and perhaps 2.4 GHz)
    - no information publicly available yet
  - possible differences from 802.11n
    - higher order MIMO
    - SDMA (directional antennae)
    - higher bandwidth
    - striping multiple OFDMA channels within single link
802.11 WLAN
Link Types: 802.11ad

- **802.11ad** under development
  - 61.25 GHz (61.0–61.5) commonly called 60 GHz
  - 1 Gb/s MAC rate over 10 m (shorter range than 802.11n)

- **Expected PHY modifications**
  - new 802.11 clause for 60GHz ISM PHY
    - possible relationship with 802.15.3c
    - coexistence with other 60 GHz communication

- **Expected MAC and link modifications**
  - changes to support 60 GHz directional antennæ
  - multi-band capability
  - efficiency enhancements
  - fast session transfer to 802.11a/b/g/n (<6GHz)
# 802.11 WLAN

## Link Characteristics

<table>
<thead>
<tr>
<th>Link type</th>
<th>year</th>
<th>band (US)</th>
<th>channel bw (US)</th>
<th>channels us/eu/jp/*</th>
<th>coding</th>
<th>MAC rate</th>
<th>typical range</th>
<th>payload</th>
<th>typical goodput</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wavelan</td>
<td>1991</td>
<td>915 MHz</td>
<td>26 MHz</td>
<td></td>
<td>DSSS</td>
<td>1 – 2 Mb/s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11</td>
<td>1997</td>
<td>2.4 GHz</td>
<td>83.5 MHz</td>
<td>11</td>
<td>13</td>
<td>14</td>
<td>3</td>
<td>DSSS FHSS</td>
<td>1 – 2 Mb/s</td>
</tr>
<tr>
<td>802.11b</td>
<td>1999</td>
<td>2.4 GHz</td>
<td>83.5 MHz</td>
<td>11</td>
<td>13</td>
<td>14</td>
<td>3</td>
<td>DSSS FHSS</td>
<td>1 – 11 Mb/s</td>
</tr>
<tr>
<td>802.11a</td>
<td>1999</td>
<td>5.8 GHz</td>
<td>300 MHz</td>
<td>12</td>
<td>19</td>
<td>4</td>
<td>OFDM</td>
<td>6 – 54 Mb/s</td>
<td>35 m</td>
</tr>
<tr>
<td>802.11g</td>
<td>2003</td>
<td>2.4 GHz</td>
<td>83.5 MHz</td>
<td>8</td>
<td>OFDM DSSS</td>
<td>6 – 54 Mb/s</td>
<td>1 – 11 Mb/s</td>
<td>0–2304 B</td>
<td>24 Mb/s</td>
</tr>
<tr>
<td>802.11y</td>
<td>2008</td>
<td>3.7 GHz licensed</td>
<td>50 MHz</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11n</td>
<td>2010</td>
<td>2.4 GHz</td>
<td>83.5 MHz</td>
<td>83.5 MHz</td>
<td>OFDM MIMO</td>
<td>&lt; 248 Mb/s</td>
<td>75 m</td>
<td>0–7955 B</td>
<td>75 Mb/s</td>
</tr>
<tr>
<td>802.11ac</td>
<td>2012</td>
<td>5.8 GHz</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11ad</td>
<td>2012</td>
<td>61 GHz</td>
<td>500 MHz</td>
<td>*number non-overlapping</td>
<td></td>
<td>1 Gb/s</td>
<td>10 m</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• **Modes**
  – infrastructure mode: STAtions communicate through APs (access points)
  – ad hoc mode: STAtions communicate directly
• **BSS: basic service set**
  – 802.11 subnetwork covered by a single AP (access point)
  – typical mode of operation for home networks
• **ESS: extended service set**
  – 802.11 subnetwork covered by multiple APs sharing SSID
  – distribution system (DS) connects multiple BSSs
802.11 WLAN
Infrastructure Mode

- Infrastructure mode
  - STAtions communicate through APs (access points)
    - also called base station
  - in a BSS (basic service set)
  - most common 802.11 configuration
802.11 WLAN

Ad Hoc Mode

- Ad hoc mode
  - STAtions communicate directly with one another
  - access point infrastructure not needed
  - rarely used
    - occasionally used for inter-PC file transfer
    - generally sign of misconfigured PC
    - can be used as SSID DoS attack against AP
Wireless Networks: WLAN 802.11 Channels and Association

- Spectrum divided into *channels* at different freq.
  - 802.11g has 8 channels
  - AP administrator chooses frequency for AP
  - interference possible
    - channel can be same as that chosen by neighboring AP

- Host must *associate* with an AP
  - scans channels
  - listens for beacon frames containing APs SSID and MAC addr
  - selects AP to associate with
  - may perform authentication
  - typically run DHCP to get IP address in AP subnet
802.11 WLAN
MAC Options

- DCF: distributed coordination function
  - random access MAC: CSMA/CA
  - mandatory function
  - typically the only option used in 802.11 subnetworks
802.11 WLAN
MAC Options

- **DCF**: distributed coördination function
  - random access MAC: CSMA/CA
  - mandatory function
  - typically the only option used in 802.11 subnetworks

- **PCF**: point coördination function
  - contention-free MAC with polling and ACKs
  - optional function; not compliance tested by Wi-Fi
  - generally not used
  - not needed for small home networks
802.11 WLAN
MAC Options

• DCF: distributed coördination function
  – random access MAC: CSMA/CA
  – mandatory function
  – typically the only option used in 802.11 subnetworks

• PCF: point coördination function EECS 882
  – contention-free MAC with polling and ACKs
  – optional function; not compliance tested by Wi-Fi
  – generally not used
  – not needed for small home networks

• HCF: hybrid coördination function EECS 882
  – enhancements for QoS in 802.11e
802.11 WLAN

Deployment Characteristics

• Typical deployment
  – infrastructure mode: AP + STAs in a BSS
    • sensible to have some infrastructure for many LANs
    • scalability and administrative issues for ad hoc mode
    • IEEE 802.11 *does not* (yet) specify routing
  – DCF: CSMA
    • with or without CA: RTS/CTS
      *when CA should be used?*
**802.11 WLAN**

**Deployment Characteristics**

- **Typical deployment**
  - infrastructure mode: AP + STAs in a BSS
    - sensible to have some infrastructure for many LANs
    - scalability and administrative issues for ad hoc mode
    - IEEE 802.11 *does not* (yet) specify routing
  - DCF: CSMA
    - with or without CA: RTS/CTS
    - turn off CA for single laptop at home and no close neighbours
    - turn on CA for moderate to heavy load
    - check administrative options in access point
IEEE 802.11 is typically CSMA and CDMA hybrid

Variety of coding schemes...
- DSSS: direct sequence spread spectrum
- FHSS: frequency hopping spread spectrum (rarely used)
- OFDM: orthogonal frequency division multiplexing (newer)

...Over which CSMA/CA MAC is typically run
- CSMA with optional RTS/CTS

...Within FDMA
- one of a set of channels
• IEEE 802.11 is typically CSMA and CDMA hybrid
• Interframe spacing
  – guard times between transmissions
  – relative length determines priority

*why?*
IEEE 802.11 is typically CSMA and CDMA hybrid

Inter-frame spacing (IFS)
- guard times between transmissions
- relative length determines priority
- shorter IFS will transmit first; longer will sense channel busy

IFS types
- SIFS: short for control messages
- PIFS: PCF packet transmission
- DIFS: DCF frame transmission
- EIFS: extended for resynchronisation
Wireless Networks: WLAN
802.11 CSMA/CA MAC

- CSMA/CA: collision avoidance
  - RTS/CTS to reduce $Pr[\text{collision}]$
- Sender
  - sense and wait for DIFS interval
Wireless Networks: WLAN

802.11 CSMA/CA MAC

- **CSMA/CA**: collision avoidance
  - RTS/CTS to reduce Pr[collision]
- **Sender**
  - sense and wait for DIFS interval
  - if channel free send RTS
Wireless Networks: WLAN
802.11 CSMA/CA MAC

- **CSMA/CA**: collision avoidance
  - RTS/CTS to reduce Pr[collision]
- **Sender**
  - sense and wait for DIFS interval
  - if channel free send RTS
- **Receiver**
  - wait for SIFS interval
Wireless Networks: WLAN
802.11 CSMA/CA MAC

- **CSMA/CA**: collision avoidance
  - RTS/CTS to reduce \( \text{Pr}[\text{collision}] \)
- **Sender**
  - sense and wait for DIFS interval
  - if channel free send RTS
- **Receiver**
  - wait for SIFS interval
  - return **CTS** if channel idle
    - receiver hears nodes hidden from sender
Wireless Networks: WLAN
802.11 CSMA/CA MAC

- **CSMA/CA**: collision avoidance
  - RTS/CTS to reduce Pr[collision]
- **Sender**
  - sense and wait for DIFS interval
  - if channel free send RTS
- **Receiver**
  - wait for SIFS interval
  - return CTS if channel idle
- **Sender**
  - wait for SIFS interval
  - *why not DIFS*?
Wireless Networks: WLAN
802.11 CSMA/CA MAC

• CSMA/CA: collision avoidance
  – RTS/CTS to reduce Pr[collision]

• Sender
  – sense and wait for DIFS interval
  – if channel free send RTS

• Receiver
  – wait for SIFS interval
  – return CTS if channel idle

• Sender
  – wait for SIFS interval
  – DIFS already used to seize channel
Wireless Networks: WLAN
802.11 CSMA/CA MAC

- **CSMA/CA**: collision avoidance
  - RTS/CTS to reduce Pr[collision]
- **Sender**
  - sense and wait for DIFS interval
  - if channel free send RTS
- **Receiver**
  - wait for SIFS interval
  - return CTS if channel idle
- **Sender**
  - wait for SIFS interval
  - transmit frame
Wireless Networks: WLAN
802.11 CSMA/CA MAC

- CSMA/CA: collision avoidance
  - RTS/CTS to reduce Pr[collision]
- Sender
  - sense, wait for DIFS, send RTS
- Receiver
  - wait for SIFS, return CTS
- Sender
  - wait for SIFS, transmit frame
- Receiver
  - wait for SIFS interval and return ACK
Wireless Networks: WLAN
802.11 CSMA/CA MAC

- CSMA/CA: collision avoidance
  - RTS/CTS to reduce Pr[collision]
- Sender
  - sense, wait for DIFS, send RTS
- Receiver
  - wait for SIFS, return CTS
- Sender
  - wait for SIFS, transmit frame
- Receiver
  - wait for SIFS interval and return ACK
- Sender
  - must wait DIFS before next frame
Wireless Networks: WLAN
802.11 – 802.3 Switching and Bridging

- Ethernet frequently used to interconnect 802.11 APs
- Similar frame format makes bridging trivial
  - map addresses
  - copy LLC/SNAP
  - copy payload
  - copy FCS
802.11 WLAN

Handoff

- Within BSS: no handoff
- Inter-BSS within IP subnet
  - learning bridge in Ethernet switch
  - not fast enough for real-time traffic with authentication
- IAPP inter-access point protocol
  - 802.11F trial standard no longer in force
  - unique association throughout ESS
  - not fast enough for real-time traffic
- 802.11r: fast BSS transition \( \text{EECS 882} \)
  - overlaps association and authentication using cached keys
802.11 WLAN
Mesh Networking

- 802.11 specified ESS capability
  - 802.11s TG: mesh task group
  - draft standard
- **Mesh points**: relay APs or STAs
802.11 WLAN
802.11s Mesh Networking

- MAC enhancements
  - segregation mesh traffic / BSS using contention free period
  - RTS/CTX (request/clear to switch) to negotiate frequencies
- Multihop routing
  - layer 2 routing within LAN under Internet routing
  - HWMP (hybrid wireless mesh protocol) mandatory
    - based on AODV and tree-based routing
  - RA-OLSR (radio-aware optimised link state routing) optional
    - based on OLSR
  - other optional protocols allowed
Wireless Networks

MW.4.1  802.16 WMAN and WiMAX

MW.1  Wireless and mobile networking concepts
MW.2  MAC functions and services
MW.3  MAC algorithms
MW.4  Wireless networks
   MW.4.1  802.11 WLAN
   MW.4.2  802.16 WMAN and WiMAX
   MW.4.3  802.15 WPAN and Bluetooth
   MW.4.4  Sensor networks
MW.5  Mobile networks
Wireless Networks: WMAN

802.16 Overview

• **WirelessMAN:** Wireless MANs
  – IEEE 802.16 grouper.ieee.org/groups/802/16

• **Metropolitan wireless networks**
  – originally intended for *fixed* wireless access
  – standardisation and replacement for MMDS in 10 – 66 GHz
  – 802.16a additional operation in licensed bands 2 – 11 GHz
  – 802.16b additional operation in unlicensed 5.8 GHz band

• **Later support for mobility**
  – 802.16e
  – overlaps with IEEE 802.20 MBWA charter
Wireless Networks: WMAN

802.16 Relation to other 802 Wireless Protocols

- IEEE 802.16
  - part of 2nd set of 802 wireless protocols (802.15 & 802.16)
  - design motivated by MMDS
  - no similarity to 802.11/Ethernet framing or operation
Wireless Networks: WMAN

WiMAX Overview

- **WiMAX**
  - Worldwide Interoperability for Microwave Access
  - www.wimaxforum.org
  - note capitalisation: WiMAX not WiMax

- **802.16 standards compliance & interoperability tests**
  - similar in concept to Wi-Fi for 802.11

- **802.16 deployment scenarios & service architecture**
  - recall that 802 mission is L1 and L2 only

*WiMAX ≠ 802.16!*
Wireless Networks: WMAN

802.16 Physical and Link Characteristics

- **802.16 (original)**
  - 10-66 GHz licensed spectrum; LOS (line of sight)
  - 2 – 5 km transmission radius
  - 32 – 134 Mb/s

- **802.16a and 802.16b**
  - 2 – 11 GHz; non-LOS
  - 7 – 10 km typical; 50 km max transmission radius
  - 75 Mb/s
Wireless Networks: WMAN
802.16 Physical and Link Characteristics

- **802.16e**: mobile
  - 2 – 6 GHz; non-LOS
  - 2 – 5 km transmission radius
  - 15 Mb/s

- **802.16m**: advanced interface
  - 100 Mb/s mobile; 1 Gb/s fixed
  - currently under standardisation; expected ~2010
  - planned for LTE-advanced 4G mobile cellular telephony
# Wireless Networks: WMAN

## 802.16 Link Characteristics

<table>
<thead>
<tr>
<th><strong>Link type</strong></th>
<th>year</th>
<th>band</th>
<th>topology</th>
<th>channel BW</th>
<th>duplex</th>
<th>coding</th>
<th>MAC rate</th>
<th>typical range</th>
<th>payload</th>
<th>typical goodput</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMDS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.16</td>
<td>2001</td>
<td>10–66 GHz</td>
<td>point-to-multipoint</td>
<td></td>
<td>TDD &amp; FDD</td>
<td>SC</td>
<td>34–134 MB/s</td>
<td>2–5 km</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.16a</td>
<td>2002</td>
<td>2–11 GHz</td>
<td>point-to-multipoint</td>
<td></td>
<td>non-LOS</td>
<td>OFDM</td>
<td>OFDMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.16b</td>
<td></td>
<td>5.8 GHz UNII</td>
<td></td>
<td></td>
<td>non-LOS</td>
<td></td>
<td></td>
<td>0–2304 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.16e</td>
<td>2006</td>
<td>2–6 GHz</td>
<td>1.25–20 MHz</td>
<td></td>
<td>non-LOS</td>
<td>MIMO</td>
<td></td>
<td>0–2304 B</td>
<td>5 Mb/s</td>
<td></td>
</tr>
<tr>
<td>802.16m</td>
<td>2010</td>
<td>&gt;20MHz</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100 Mb/s</td>
<td>1 Gb/s</td>
</tr>
</tbody>
</table>
802.16 WMAN

Components

- **BS**: base station
  - directly connected to Internet infrastructure
  - arranged as mesh with other base stations

- **SS**: subscriber station
  - fixed SS
    - 802.16 communication with base station
    - connected to LAN infrastructure, *e.g.* Ethernet, 802.11
  - mobile SS
    - mobile node such as PDA using 802.16e
802.16 WMAN
Subnetwork Topologies

- **PMP**: point-to-multipoint topology
  - BS: base station communicates with multiple SSs
- **Mesh mode**
  - arbitrary mesh of BSs and SSs
802.16 WMAN
PMP Mode

- **PMP**: point-to-multipoint topology
  - **BS**: base station
    - communicates with multiple SSs
    - typically sectorised cell using multiple directional antennae
  - **SS** subscriber stations
    - communicate through BSs
802.16 WMAN

Mesh Mode

- Mesh mode
  - BS – SS (as in PMP)
  - BS – BS multihop relay to SS
  - BS – BS mesh network (e.g. for backhaul)
  - SS – SS ad hoc mode
802.16 WMAN
MAC and Link Layer Functions

• Link layer functions (called MAC layer in spec)
  – error control
    • ARQ
    • hybrid ARQ with OFDMA
  – scheduling and link adaptation for QoS

• Medium access control
  – SC (single carrier) with FDD or TDD
  – OFDMA (orthogonal frequency division multiple access)
802.16 WMAN
MAC and Link Layer: Duplexing

• 802.16 link duplexing options
  – FDD: frequency division duplexing
    • uplink and downlink assigned different frequencies
    • accommodates full-duplex SSs with multiple tranceivers
    • half-duplex SSs must retune between up-and downlink
    • permitted only for 802.16 licensed spectrum
  – TDD: time division duplexing
    • slots divided between upstream and downstream traffic
    • dynamic bandwidth adjustment
    • permitted for both 802.16 licensed and unlicensed bands
802.16 WMAN
TDD Physical Framing

- 802.16 TDD physical framing
  - preamble
  - broadcast control
    - DL map: map of downlink transmissions for this frame
    - UL map: map up uplink transmissions for next frame
  - data transmission bursts
  - TTG: transmit/receive transmission gap
    - allows transceivers to retune
  - variable boundary between down- and uplink subframes
    - dynamic bandwidth adjustment
### Generic Frame Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HT=0</td>
<td>1b</td>
<td>header type</td>
</tr>
<tr>
<td>EC=0</td>
<td>2B</td>
<td>encryption control</td>
</tr>
<tr>
<td>type</td>
<td>6b</td>
<td></td>
</tr>
<tr>
<td>CI: CRC indicator</td>
<td>1b</td>
<td></td>
</tr>
<tr>
<td>EKS: encryption key seq.</td>
<td>2B</td>
<td></td>
</tr>
<tr>
<td>LEN: length</td>
<td>11b</td>
<td></td>
</tr>
<tr>
<td>CID: connection id</td>
<td>6B</td>
<td></td>
</tr>
<tr>
<td>HCS: header check seq.</td>
<td>1B</td>
<td></td>
</tr>
</tbody>
</table>

### Payload

- [0–2312B]

### Trailer: CRC

- [4B]
802.16 WMAN
MAC Traffic Classes

- Traffic Classes
  - constant bit rate service
  - real-time polling: rt-VBR
  - non-real-time polling: nrt-VBR
  - best effort
  - unsolicited grant service: connectionless
WiMAX WMAN
Reference Architecture

- 802.16 only specifies air interface
  - PHY, MAC, and link layers
  - insufficient for service deployment architecture (ala 3G)
- Need for implementation agreements for
  - equipment manufacturers
  - service providers
WiMAX WMAN
Reference Architecture

• 802.16 only specifies *air interface*
• Need for implementation agreements
• WiMAX forum reference architecture
  – specifies components, subnetworks, and their roles
  – specifies service architecture
    • including AAA, ...
  – specifies *reference points*
    • physical interfaces
    • conceptual links (protocol and service relationships)
WiMAX WMAN
Selected Reference Points

• ASN
  – access service network
  – WiMAX Forum ref points

• Intra-ASN RPs
  – R1: BS–SS
  – R6: GW–BS
  – R4: GW–GW

• Inter-ASN RPs
  – R3: GW
Wireless Networks

MW.4.3 802.15 WPAN and Bluetooth

MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
MW.4 Wireless networks
  MW.4.1 802.11 WLAN
  MW.4.2 802.16 WMAN and WiMAX
  MW.4.3 802.15 WPAN and Bluetooth
  MW.4.4 Sensor networks
MW.5 Mobile networks
Wireless Personal Networks
Introduction and Definitions

• PAN: local area network
  – links or subnetwork of shorter reach than LAN
  – replacement for interconnect cables
    • computer peripherals
    • mobile phone headsets
  – private intimate group of personal devices [IEEE 802]
    • in personal operating space (POS)
  – several meters: $O(10\ \text{m})$

• Examples
  – wired: USB, IEEE 1394 Firewire
  – wireless: IrDA, 802.15.1/Bluetooth, 802.15.3, Wireless USB
Wireless Networks: WPAN

Bluetooth History

• **Initial work done at Ericsson in Sweden**
  - Bluetooth named after Harald I

• **Bluetooth SIG** (special interest group)
  - industry consortium formed in 1998
  - mobile telephone vendors: Ericsson, Nokia
  - other electronics vendors: IBM, Intel, Toshiba

• **Proprietary specification development**
  - membership was required to see draft specifications
  - specifications now freely available (2.1 is current)
    • [www.bluetooth.com/Bluetooth/Learn/Technology/Specifications](http://www.bluetooth.com/Bluetooth/Learn/Technology/Specifications)
    • 1000+ page behemoth
Bluetooth WPAN
Network Topology

- Piconet
  - collection of devices in transmission range of master
  - master dictates timing; transmits in odd-numbered slots
  - up to 7 active slaves use even-numbered slots
  - up to 247 parked (inactive) devices
  - all slave–slave communication through master

- Scatternet
  - collection of piconets that share devices
Bluetooth WPAN
Architecture

- Stovepipe protocol stack for very specialised domain
  - driven by mobile telephone manufacturers
  - physical through application layer
- Application profiles define vertical protocol slices, e.g.:
  - generic access
  - telephony
  - printing
  - data transfer
- Not compatible with other protocol stacks
  - OSI, Internet, or IEEE 802
  - IEEE reworked as 802.15.1
Bluetooth WPAN
Protocol Stack

- HCI: host controller interface
- RFCCOMM: emulates serial port
- TCS: telephony control protocol specification
- SDP: service discovery protocol
Bluetooth WPAN
Deployment Status

- Deployment status
  - widely deployed in mobile telephones
    - most commonly used for wireless headsets
  - increasingly deployed in PDAs and laptop computers

Problems?
Bluetooth WPAN
Deployment Issues

• Problems and issues
  – closed development process driven by mobile telephony
  – incompatible with Internet and 802 architecture
    • rectified by IEEE 802.15.1 (future?)
  – interference not considered
    • interference with 802.11
    • poor scalability in dense deployments (e.g. 2001 CeBIT debacle)
  – numerous security flaws
  – competition looming from wireless USB
  – architectural limitations ...
Bluetooth WPAN
Architectural Limitations

- Significant architectural restrictions
  - 3-bit address space ⇒ only 8 active devices / piconet
    - *appalling* lack of foresight
      - evidently driven mobile telephone marketing folk
    - personal networks easily *far* exceed 8 devices
    - computer manufacturers (IBM, Intel) deny responsibility
  - master/slave configuration
  - scatternets consisting of multiple piconets
  - problems largely rectified by IEEE 802.15.3
    - future uncertain
Wireless Networks: WPAN

802.15 Relation to other 802 Wireless Protocols

- **IEEE 802.15**
  - part of 2nd set of 802 wireless protocols (802.15 & 802.16)
  - design motivated by Bluetooth
  - *no* similarity to 802.11/Ethernet framing or operation
802.15 WPAN

WPAN Overview

• WPAN: Wireless Personal Area Networks
  – IEEE 802.15 grouper.ieee.org/groups/802/15
• Personal and short-reach wireless network
  – shorter range than 802.11
  – initially motivated by Bluetooth & compatibility with 802.11
802.15 WPAN
Standards Overview: Links

- **IEEE 802.15**
  - wireless personal area networks

- **Personal and short-reach wireless network**
  - 802.15.1: standardisation of Bluetooth physical/MAC layers
  - 802.15.2: *co-existence* of 802.11 and 802.15 in 2.4 GHz
    - original goal of 802.15.1 was to *interoperate* with 802.11
  - 802.15.3: high rate and larger addresses
  - 802.15.4: low energy for sensor networks
  - 802.15.5: mesh networking (work in progress)
  - 802.15.6: BAN body area networks (work in progress)
  - 802.15.7: short range visible-light optical (work in progress)
IEEE 802.15
- wireless personal area networks

Personal and short-reach wireless network
- 802.15.1: standardisation of Bluetooth physical/MAC layers
- 802.15.2: co-existence of 802.11 and 802.15 in 2.4 GHz
  - original goal of 802.15.1 was to interoperate with 802.11
- 802.15.3: high rate and larger addresses
- 802.15.4: low energy for sensor networks
- 802.15.5: mesh networking (work in progress)
- 802.15.6: BAN body area networks (work in progress)
- 802.15.7: short range visible-light optical (work in progress)
802.15.1 and Bluetooth WPAN
Physical Layer Characteristics

- 2.4 GHz unlicensed ISM band implications?
802.15.1 and Bluetooth WPAN
Physical Layer Characteristics

- 2.4 GHz unlicensed ISM band
  - interference issues with 802.11b/g and cordless phones
802.15.1 and Bluetooth WPAN
Physical Layer Characteristics

- 2.4 GHz unlicensed ISM band
- Three power classes
  - class 1: 1–100 mW with power control in 2–8 dB steps
  - class 2: 0.25–2.5 mW with optional power control
  - class 3: max 1 mW with optional power control
- Three line coding options
  - GFSK (Gaussian FSK) line coding: 1b/symbol = 1Mb/s
  - $\pi/4$-DQPSK: 2b/symbol = 2Mb/s
  - 8-DQPSK: 3b/symbol = 3Mb/s
- Low sensitivity receivers for low cost
  - $-70$dBm for 0.1%BER at 1Mb/s, 0.01%BER at 2, 3 Mb/s
802.15.1 and Bluetooth WPAN
Medium Access Control

- **TDD (time division duplexing)**
  - simple to achieve over very short distances
    - independent clocks are frequently synchronised
  - $625\mu s$ / slot (27-bit slot number $k$)
  - transmissions use 1, 3, or 5 slots
  - *masters* begin transmission in even slot

```
master

\[k\,\,k+1\,\,k+2\,\,k+3\,\,k+4\,\,k+5\,\,k+6\,\,\ldots\]

slave
```
• TDD (time division duplexing)
  - simple to achieve over very short distances
    • independent clocks are frequently synchronised
  - 625μs / slot (27-bit slot number $k$)
  - transmissions use 1, 3, or 5 slots
  - masters begin transmission in even slot; slaves in odd slot
802.15.1 and Bluetooth WPAN
Medium Access Control

- TDD
- FHSS (frequency hopping spread spectrum)
  - FHSS robust to narrow-band interference
  - 79 1MHz bands between 2.402 and 2.4835 GHz (US)
  - pseudorandom hopping sequence determined by master
  - 1600 | 3200 hop/s in connection for data transfer| control
  - *significant interference with 802.11 DSSS*

\[ f(k) \quad f(k+1) \quad f(k+2) \quad f(k+3) \quad f(k+4) \quad f(k+5) \quad f(k+6) \quad \ldots \]

master

slave
802.15.1 and Bluetooth WPAN

Piconet

- **Piconet**: up to 256 devices
  - transmission range of master
802.15.1 and Bluetooth WPAN

Piconet

- **Piconet**: up to 256 devices
  - transmission range of master
- **Master** dictates timing
  - transmits in odd-numbered slots
802.15.1 and Bluetooth WPAN

Piconet

- **Piconet**: up to 256 devices
  - transmission range of master
- **Master** dictates timing
  - transmits in odd-numbered slots
- **Slaves**
  - max of only 7 active at a time
  - use even-numbered slots
**802.15.1 and Bluetooth WPAN**

**Piconet**

- **Piconet**: up to 256 devices
  - transmission range of **master**
- **Master** dictates timing
  - transmits in odd-numbered slots
- **Slaves**
  - max of only 7 active at a time
  - use even-numbered slots
  - all slave–slave communication through **master**
802.15.1 and Bluetooth WPAN

Piconet

- **Piconet**: up to 256 devices
  - transmission range of **master**
- **Master** dictates timing
  - transmits in odd-numbered slots
- **Slaves**
  - max of only 7 active at a time
  - use even-numbered slots
  - all slave–slave communication through master
- **Parked** (inactive) devices
  - max 247
802.15.1 and Bluetooth WPAN

Scatternet

- Scatternet
  - collection of piconets that share devices
- Barely mentioned in the Bluetooth specs
  - theoretical construct to deflect criticism on architectural limits of Bluetooth?
Wireless Networks: WPAN

802.15.3 Overview

- 802.15 Task Group 3: High Rate PANs
  - higher data rates: 11 – 55 Mb/s
  - multimedia and QoS
  - ad-hoc and peer-to-peer networking
  - better co-existence with 802.11
802.15.3 WPAN

Piconets

- Piconets
  
  *how to improve over Bluetooth/802.15.1?*
802.15.3 WPAN

Piconets

- Piconets: 64K devices
  - 16 b DEV address
  - peer-to-peer data
    - *doesn’t* need to go via PNC

*why do we need a controller?*
802.15.3 WPAN

Piconets

- Piconets: 64K devices
  - 16 b DEV address
  - peer-to-peer data
    - *doesn’t* need to go via PNC
  - PNC: piconet coördinator
    - *beacons* to all DEVs in piconet
    - distributes timing
MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
MW.4 Wireless networks
   MW.4.1 802.11 WLAN
   MW.4.2 802.16 WMAN and WiMAX
   MW.4.3 802.15 WPAN and Bluetooth
   MW.4.4 Sensor networks
MW.5 Mobile networks
Wireless Networks

Sensor Network Overview

- Wireless sensor network (WSN) motivation
  - remote sensing of environmental conditions
    - e.g. temperature, chemical/radiological conditions
  - perhaps remote actuation of control systems

- Sensor network characteristics
  - network of sensors (and perhaps actuators)
  - may be deployed in large numbers in remote areas
  - low-power operation frequently essential
  - in-network data-fusion
**WSN Architecture**

**Components**

- **Sensor**
  - device that senses information from environment
- **Actuator**
  - device that controls environment
- **Sink**
  - destination of sensor data for processing or storage
- **Gateway**
  - interworking between WSN and data network
    - typically the Internet
WSN Characteristics

Introduction

• Defining characteristics of WSNs
  – wireless nodes
  – energy efficiency critical
    • difficult or impossible to replace battery
  – large scale
    • sensor fields may have thousand or millions of nodes
    • ad hoc: manual configuration impractical
WSN Characteristics

Differences from WPANs

- WPAN: wireless personal network
- Energy concerns
  - WPAN nodes have rechargeable or replaceable batteries
  - WSN energy management more critical
- Limited mobility
  - many sensors are stationary
  - initial self-organisation more important
    - dynamic reoptimisation less critical
    - network must react to failed nodes that have no energy left
**WSN Characteristics**

**Differences from MANETs**

- **MANET**: mobile ad hoc network
- **Energy concerns**
  - WPAN nodes have rechargeable or replaceable batteries
  - WSN energy management more critical
  - low duty cycle of sensors helps
- **Limited mobility**
  - many sensors are stationary
WSN Characteristics
Differences from other Networks

• WSNs are *data centric*
  – information important
  – not necessarily related to particular nodes

• Examples
  – average temperature of a region
  – mapping of a storm or wildfire
  – location of an animal

*Consequence?*
WSN Characteristics

In-Network Processing

• WSNs frequently manipulate data *in the network*
  – sensor nodes not only relay multihop traffic...
  – but also process it on the way
• More energy efficient
  – processing generally cheaper than transmission
  – e.g. nodes compute average, max, or min value
    • significantly reduces communication cost
  – referred to as *sensor fusion*
WSN Characteristics
In-Network Processing Types

- Aggregation
  - compute statistical functions on the way to the sink
  - average, min, max, etc.
- Edge detection
  - compute and convey boundaries between values
  - e.g. isotherms, isobars, storm edges, wildfire boundaries
- Trajectory tracking
  - e.g. animal movement
- Other variants possible...
Wireless Sensor Networks

Application Examples

- Environmental monitoring
  - long term, e.g. climate change
  - short term, e.g. wildfire mapping
- Medical and health
  - vital signs and ongoing biochemical monitoring
  - automated drug dosing
- Intelligent buildings
  - fine-grained monitoring and control of temperature
- Military and homeland security
  - situational awareness

Many more!
Wireless Sensor Networks
Architectures

• Multihop
  – communication with limited transmission power
  – may conserve energy
    • but may not:
      energy use for transit traffic
Wireless Networks: WPAN
802.15.4 Overview

• 802.15.4
  – 20 – 250 kb/s with multi-month to -year battery life target
  – peer-to-peer networking
  – extended addresses: 16 and 64 bit

• Generally intended for wireless sensor networks
MAC; Mobile and Wireless Networks

MW.5 Mobile Networks

MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
MW.4 Wireless networks
MW.5 Mobile networks
  MW.5.1 DHCP and Mobile IP
  MW.5.2 Mobile ad hoc networks and MANET protocols
  MW.5.3 Mobile cellular telephony
Mobility Overview

• So far, we’ve been assuming fixed nodes
  – end systems and intermediate systems (switches/routers)

• Mobility
  – ability to move a device through the network

• Spectrum of mobility
  – fixed: no movement (may still be wireless!)
  – mobile: changes point of attachment to network
    • requiring reconnection, e.g. DHCP
    • allowing handoff, e.g. mobile IP, cellular telephony
  – nomadic: frequent high-mobility
Mobile Wireless Networks

Characteristics

- Mobile networks
  - wireless needed to enable mobility
- Dynamicity as nodes move
  - layer 1 and 2 effects: link characteristics change
    - e.g. signal strength, bandwidth, delay
  - layer 3 effects: topologies change
    - induces route changes
  - layer 4 effects: end-to-end path characteristics change
    - e.g. throughput, goodput, delay
Mobile Wireless Networks
Network Elements: Mobile Node

- **Base station** (BS)
- **Mobile node** (MN)
  - wireless node that moves
Mobile Wireless Networks
Network Elements: Mobile Node

- **Base station** (BS)
- **Mobile node** (MN)
  - wireless node that moves
  - roams among base stations
    - *handoff* between cells
    - e.g. mobile telephone
Mobile Wireless Networks

Network Elements: Mobile Node

- **Base station** (BS)
- **Mobile node** (MN)
  - wireless node that moves
  - roams among base stations
    - *handoff* between cells
    - e.g. mobile telephone
Mobile Wireless Networks
Network Elements: Mobile Node

- **Base station** (BS)
- **Mobile node** (MN)
  - wireless node that moves
  - roams among base stations
  - move with respect to one-another
    - ad hoc network
Mobile Wireless Networks
Network Elements: Mobile Node

- **Base station** (BS)
- **Mobile node** (MN)
  - wireless node that moves
  - roams among base stations
  - move with respect to one-another
    - ad hoc network
MAC; Mobile and Wireless Networks

MW.5.1 DHCP and Mobile IP

MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
MW.4 Wireless networks
MW.5 Mobile networks
   MW.5.1 DHCP and Mobile IP
   MW.5.2 Mobile ad hoc networks and MANET protocols
   MW.5.3 Mobile cellular telephony
IP Mobility
Overview

- Problem: node mobility between IP subnets
  - need to revisit IP-address/node bindings
DHCP

Overview

- DHCP: dynamic host configuration protocol [RFC 2131]
- Allows node to dynamically obtain IP address
  - as well as other configuration parameters, e.g. DNS server
- Benefits
  - reduces manual configuration
  - allows mobile nodes to easily move attachment point

Problems?
DHCP
Overview

- DHCP: dynamic host configuration protocol [RFC 2131]
- Allows node to dynamically obtain IP address
  - as well as other configuration parameters, e.g. DNS server
- Benefits
  - reduces manual configuration
  - allows mobile nodes to easily move attachment point
- Problems
  - no *handoff* capabilities
  - flows and sessions interrupted during move
Mobile IP

Overview

- Mobile IP [RFC 3220] (designed by C.E. Perkins)
  - designed to enable untethered Internet access
  - with limited mobility
  - without disrupting higher level protocol flows
Mobile IP
Overview

- **Mobile IP** [RFC 3220] (designed by C.E. Perkins)
  - designed to enable untethered Internet access
  - with limited mobility
  - without disrupting higher level protocol flows

- **Simple way of forwarding IP packets to mobile nodes**
Mobile IP Architecture

Home Network

- **Home network**: permanent (normal) home of MN
  - MN: mobile node
  - permanent address assigned from home network block
  - e.g. 128.119.40.186 assigned from 128.119.40/24
Mobile IP Architecture

Visited Network

- **Home network**: permanent (normal) home of MN
- **Visited Network**: temporary location of MN
  - e.g. 79.129.13/24
Mobile IP Architecture

Visited Network

- **Home network:** permanent (normal) home of MN
- **Visited Network:** temporary location of MN
  - e.g. 79.129.13/24

*problem?*
Mobile IP Architecture

Visited Network

- **Home network**: permanent (normal) home of MN
- **Visited Network**: temporary location of MN
  - home IP addr not in visited block: packets fwd to wrong net
    - e.g. 128.119.40.186 ≠ 79.129.13/24
Mobile IP Architecture

Visited Network

- **Home network**: permanent (normal) home of MN
- **Visited Network**: temporary location of MN
  - home IP addr not in visited block: packets fwd to wrong net

*solution?*
Mobile IP Architecture

Visited Network

- **Home network**: permanent (normal) home of MN
- **Visited Network**: temporary location of MN
  - home IP addr not in visited block: packets fwd to wrong net
  - use DHCP to get address in visiting net: all flows interrupted
Mobile IP Architecture

Visited Network

- **Home network**: permanent (normal) home of MN
- **Visited Network**: temporary location of MN
  - home IP addr not in visited block: packets fwd to wrong net

\textit{solution?}
**Mobile IP Architecture**

**Visited Network**

- **Home network**: permanent (normal) home of MN
- **Visited Network**: temporary location of MN
  - home IP addr not in visited block: packets fwd to wrong net
  - mobile IP *agents* forward on behalf of MN
Mobile IP Architecture

Home Agent

- **Home network** receives traffic destined for MN
  - *home agent* (HA) receives traffic destined for MN
Mobile IP Architecture

Foreign Agent

- **Home agent (HA)** forwards on behalf of MN to visited
- **Foreign agent (FA)** intercepts and relays to MN
Mobile IP Architecture

Foreign Agent

- **Home agent (HA)** forwards on behalf of MN to visited
- **Foreign agent (FA)** intercepts and relays to MN
Mobile IP Architecture

Reverse Path

- **Home agent (HA)** forwards on behalf of MN to visited
- **Foreign agent (FA)** intercepts and relays to MN

Does MN need to use agents to send to CN?
Mobile IP Architecture
Reverse Path

- **Home agent** (HA) forwards on behalf of MN to visited
- **Foreign agent** (FA) intercepts and relays to MN
- MN can address datagrams directly to CN

**issues?**
Mobile IP Architecture

Triangle Routing

- **Home agent** (HA) forwards on behalf of MN to visited
- **Foreign agent** (FA) intercepts and relays to MN
- MN can address datagrams directly to CN
  - *triangle routing*: forward path ≠ reverse path
Mobile IP Architecture

Direct Routing

- Direct routing
  - overcomes triangle routing problem
- Correspondent requests care-of address
  - home agent replies
  - correspondent sends packets directly to COA
- Problem
  - additional signalling complexity and handoff latency
Mobile IP Protocol

Overview

What steps must be taken?
Mobile IP Protocol
Overview

• Agent discovery
• Registration
• Tunneling
• Handoff
Mobile IP Protocol
Agent Discovery

• Agent discovery process
  – home and foreign agents advertise their service
  – mobile nodes solicit the existence of an agent

• ICMP message
  – router advertisement: type = 9
  – mobility agent advertisement extension: code = 16
Mobile IP Protocol

Registration

- Registration process for mobile nodes
  - request forwarding services from foreign agent
  - registers care-of address with home agent
    - directly
    - via foreign agent
  - renew binding about to expire
  - deregister from foreign agent

- UDP messages
  - mobile IP message header
Mobile IP Protocol

Tunneling

- **Tunneling**
  - home agent tunnels datagrams to care-of address

- **Methods**
  - IP-in-IP encapsulation
  - minimal encapsulation [RFC 2004]
    - eliminates redundant fields from IP-in-IP
  - GRE (generic routing encapsulation) [RFC 1701, 1702]
Mobile IP Protocol
Handoff

• Handoff: mobile node moves to new visited network
• Procedure
  – mobile node deregisters with old foreign agent
  – mobile node registers with new foreign agent
  – new foreign agent registers with home agent
  – home agent updates care-of-address for mobile
  – packets continue to be forwarded to mobile
    • new care-of-address
Mobile IP Protocol
Handoff

- Handoff: mobile node moves to new visited network
- Procedure
  - mobile node deregisters with old foreign agent
  - mobile node registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent updates care-of-address for mobile
  - packets continue to be forwarded to mobile
    - new care-of-address

*Problem?*
Mobile IP Protocol

Handoff

- Handoff: mobile node moves to new visited network
- Procedure
  - mobile node deregisters with old foreign agent
  - mobile node registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent updates care-of-address for mobile
  - packets continue to be forwarded to mobile
    - new care-of-address
- Problem
  - hand-off delay
  - packet loss during handoff
Mobile IP Protocol
Advantages and Disadvantages

Advantages?
Mobile IP Protocol
Advantages and Disadvantages

• Advantages
  – very simple mechanism
Mobile IP
Advantages and Disadvantages

• Advantages
  – very simple mechanism

• Disadvantages
  – hand-off latency may be seconds
    • registration
    • authentication
    • many optimisations proposed
  – triangle routing
    • different forward and reverse paths
  – security issues
    • ingress and firewall address filtering of address mismatches
Mobile IP
Reality

• IP routers
  – most supported mobile IP for a long time

• Service providers
  – some deployment within cellular telephony service providers

• Users
  – very little actual use

  why?
Mobile IP Reality

• IP routers
  – most supported mobile IP for a long time

• Service providers
  – some deployment within cellular telephony service providers

• Users
  – very little actual use
  – DHCP reattachment sufficient for many applications
    • email and Web transactions
  – not yet much continuous wireless coverage
    • very few users roam among 802.11 hot spots
  – could change with 802.16 and PDAs
MAC; Mobile and Wireless Networks

MW.5.2 MANETs

MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
MW.4 Wireless networks
MW.5 Mobile networks
  MW.5.1 DHCP and Mobile IP
  MW.5.2 Mobile ad hoc networks and MANET protocols
  MW.5.3 Mobile cellular telephony
Mobile Ad Hoc Networking

Overview

- Mobile ad hoc networks
  - MANETs in IETF jargon (pronounced ma-net *not* ma-nay)
- Mobile
  - nodes are untethered: *nomadic*
- Ad hoc
  - no pre-existing infrastructure is assumed
  - auto-configuration of nodes
  - self-organisation of networks
  - example: group of users meets in cave and forms a network
Mobile Ad Hoc Networking
Multihop Networking

- Multihop
  - nodes act as both end and intermediate systems
  - users carry transit traffic
  - security and performance implications
Mobile Ad Hoc Networking
Protocol Overview

• Neighbour discovery
• Link formation
• Self-organisation
• Topology optimisation and maintenance
Mobile Ad Hoc Networking

Neighbour Discovery

- Nodes emit beacons to announce their presence
  - known frequencies and codes used for announcements
- Establishes set of directly reachable nodes
Mobile Ad Hoc Networking
Link Formation

- Pairwise negotiation of link formation
  - interested nodes answer beacons
  - exchange identification, node and link characteristics
  - layer 2 connectivity structure
- Maintain link adjacencies
  - e.g. keepalive messages
Mobile Ad Hoc Networking
Self-Organisation and Federation

- Communicating nodes self-organise into federations
  - address acquisition
  - hierarchical cluster formation and leader election
    - based on administrative concerns, security, role/task based
  - bootstrap routing topology
Mobile Ad Hoc Networking
Topology Optimisation and Maintenance

- Topology maintenance of federations
  - merge/split
    - group mobility, dynamic coalitions
  - heal partition
Mobile Ad Hoc Networking
Topology Optimisation and Maintenance

• Topology maintenance of nodes
  – node mobility
  – leave/join from/to federation
  – resolution to identifier vs. topological address reassignment

leave then join
Mobile Ad Hoc Networking

Impact of Mobility

- Dynamic nodes and topologies
  - changing links, clustering, and federation topology
  - difficult to achieve routing convergence
- Control loop delay
  - mobility may exceed ability of control loops to react
- Impacts QOS
Mobile Ad Hoc Networking

Impact of Mobility

- Dynamic nodes and topologies
  - changing links, clustering, and federation topology
  - difficult to achieve routing convergence
- Control loop delay
  - mobility may exceed ability of control loops to react
- Impacts QOS
  - changes in inter-node distance
    - requires power adaptation
    - changes density and impacts degree of connectivity
  - latency issues (routing optimisations temporary)
Mobile Ad Hoc Networking

Impact of Mobility

- Dynamic nodes and topologies
  - changing links, clustering, and federation topology
  - difficult to achieve routing convergence

- Control loop delay
  - mobility may exceed ability of control loops to react

- Impacts QoS
  - changes in inter-node distance
    - requires power adaptation
    - changes density and impacts degree of connectivity
  - latency issues (routing optimisations temporary)
Mobile Ad Hoc Networking
Routing Algorithms

• Types
  – proactive or table driven
    • compute routes that may be needed
    • low communication startup latency
    • overhead of continuous route maintenance
  – reactive or on-demand
    • compute routes only when needed
    • higher startup latency
    • lower overall overhead
Mobile Ad Hoc Networking
Routing Algorithm Examples

• Many proposals
  – many within the IETF MANET working group
  – specialized domains: e.g. supersonic military aircraft

• Examples:
  – AODV: ad hoc on-demand distance vector
  – DSR: dynamic source routing

• No one protocol can possibly be right for all scenarios
  – adaptive framework needed to negotiate protocols
Mobile Ad Hoc Networking
Routing Algorithms: AODV

- AODV: ad hoc on-demand distance vector
  - distance vector algorithm
  - acquires and maintains routes only on demand
    - routes cached while in use
    - routes purged after use
Mobile Ad Hoc Networking
Routing Algorithms: DSR

- DSR: dynamic source routing
  - source routing: packets carry source routes
  - source routes constructed on-demand
MAC; Mobile and Wireless Networks

MW.5.3 Mobile Cellular Telephony

MW.1 Wireless and mobile networking concepts
MW.2 MAC functions and services
MW.3 MAC algorithms
MW.4 Wireless networks
MW.5 Mobile networks
  MW.5.1 DHCP and Mobile IP
  MW.5.2 Mobile ad hoc networks and MANET protocols
  MW.5.3 Mobile cellular telephony
Mobile Wireless Telephony
Motivation

- Untethered replacement for wired phones

*scenarios?*
Mobile Wireless Telephony

Motivation

• Untethered replacement for wired phones
  – cordless phone replacement within premises
Mobile Wireless Telephony

Motivation

- Untethered replacement for wired phones
  - cordless phone replacement within premises
  - mobile telephones for use anywhere
  - including while moving: driving, riding train or bus
Mobile Wireless Telephony

Motivation

- Untethered replacement for wired phones
  - cordless phone replacement within premises
  - mobile telephones for use anywhere
    - including while moving: driving, riding train or bus

- Design goals
  - seamless mobility is prime requirement
Mobile Wireless Telephony

Motivation

- Untethered replacement for wired phones
  - cordless phone replacement within premises
  - mobile telephones for use anywhere
    - including while moving: driving, riding train or bus

- Design goals
  - seamless mobility is prime requirement

*how is this different from mobile IP?*
Mobile Wireless Telephony

Motivation

• Untethered replacement for wired phones
  – cordless phone replacement within premises
  – mobile telephones for use anywhere
    • including while moving: driving, riding train or bus

• Design goals
  – seamless mobility is prime requirement: handoff
  – more aggressive requirement than for mobile IP
Wireless Telephony
Early History

- 1947– 1977 (0G)
  - 1946: FCC allocates 33 FM channels in 35,150,450 MHz band
  - 1947: operator relay begins to US passenger trains
  - 1960s: direct dialing from automobiles in home area
    - extremely limited channel capacity
  - 1977: Bell Labs begins first AMPS 1G cellular trial in Chicago
Cellular Network Topology

Motivation

- Goal: wireless telephony everywhere

  *Problem: how to place base stations?*
Cellular Network Topology

Motivation

• How to place base stations

randomly?
Cellular Network Topology

Motivation

• How to place base stations
  – random: difficult for network traffic engineering
Cellular Network Topology

Motivation

- How to place base stations
  - random: difficult for network traffic engineering
  
  *alternative?*
Cellular Network Topology

Motivation

• How to place base stations
  – regular tessellation in *cellular* structure
  
  *what shape?*
Cellular Network Topology

Motivation

- How to place base stations
  - regular tessellation in *cellular* structure
    square grid?
Cellular Network Topology

Motivation

• How to place base stations
  – regular tessellation in *cellular* structure
  – square grid: very non-uniform distance between transmitters
    • range of 1 to 1.414 units

*alternative?*
Cellular Network Topology
Hexagonal Cell Structure

- How to place base stations
  - hexagonal tessellation is most efficient packing of circles
    - e.g. beehive
  - reality: exact location constrained by economics & regulation
Cellular Network Topology
Hexagonal Cell Structure

- Hexagonal cell plan

*Problem?*
Cellular Network Topology

Hexagonal Cell Structure

- Hexagonal cell plan
- Problem: interference between adjacent cells

*Solution?*
Cellular Network Topology
Hexagonal Cell Structure

- Hexagonal cell plan
- Adjacent cells need to use different frequencies
  - avoid inter-cell interference
  - signal-strength sensing for handoff

*how to allocate?*
Cellular Network Topology

Frequency Reuse

- Hexagonal cell plan
- Frequency reuse
  - plan to assign frequencies to cells
  - 4 frequency plan
Cellular Network Topology

Frequency Reuse

- Hexagonal cell plan
- Frequency reuse
  - plan to assign frequencies to cells
  - 7 frequency plan
Cellular Network Topology

Increasing Capacity

- Cell plan designed for a given traffic load

*what happens when traffic increases?*
Cellular Network Topology

Increasing Capacity: Add Spectrum

- Add channels
  - constrained by available spectrum
  - e.g. channels added to US AMPS (taken from UHF television)
Cellular Network Topology

Increasing Capacity: Dynamic Assignment

- Add channels
- Frequency borrowing
  - adjust long-term allocation between cells
    - limited applicability
  - dynamically load balance channels among cells
    - complexity
Cellular Network Topology

Increasing Capacity: Sectorisation

- Add channels
- Frequency borrowing
- Sectorisation (SDMA)
  - replace omnidirectional antenna with directional antennæ
  - 3, 4, and 6 sector designs common
Cellular Network Topology
Increasing Capacity: Cell Splitting

- Add channels
- Frequency borrowing
- Sectorisation
- Cell splitting
  - overlay *microcells*
  - or *picocells*
Cellular Network Topology
Increasing Capacity: Cell Splitting

- Add channels
- Frequency borrowing
- Sectorisation
- Cell splitting
- Combination of techniques
Cellular Network Mobility

Problem

How to support mobility between cells?
Handoffs (handovers) for mobility between cells
  - without call/connection termination
Cellular Network Mobility

Handoffs

• Handoffs (handovers) for mobility between cells
  – without call/connection termination
• Handoff types
  – hard handoff: break-before-make
  – soft handoff: make-before-break

Metrics?
Cellular Network Mobility

Handoff Metrics

- Handoff metrics
  - call dropping probability
  - handoff delay (due to signalling)
  - interruption duration (time MT not connected to either BS)
    - results in silence for voice and packet loss for data
  - probability of unnecessary handoff
Cellular Network Mobility
Handoff Strategies

- Handoff strategies: relative signal strength
  - handoff to BS with stronger signal

problem?
Cellular Network Mobility

Handoff Strategies

- Handoff strategies: relative signal strength
  - handoff to BS with stronger signal
  - ping-pong oscillations between adjacent base stations
  alternatives?
Cellular Network Mobility

Handoff Strategies

- Handoff strategies: relative signal strength
  - handoff to BS with stronger signal
  - ping-pong oscillations between adjacent base stations

- Handoff optimisations
  - thresholds
  - *hysteresis*
  - predictive
    - future signal strength
  - combinations

Based on [Stallings 2005] fig. 10.7b
Mobile Telephone Network
Roaming

• Roaming between service providers
  – handoff
  – service and billing agreements
Mobile Telephone Network
Architecture Overview

- Network divided in **cells** each covered by **base station**
  - hexagonal packing of circles
  - adjacent cells use different frequencies (**spatial reuse**)
- **Mobile terminals** move among cells
- Cells interconnected by **mobile switching centers**
Mobile Telephone Network

Generations

- **1G**: analog voice
- **2G**: digital voice
  - **2.5G**: 2nd generation with new data services
  - emerged with delay of 3G past planned deployment in 2000
- **3G**: moderate-rate data access
- **4G**: high-rate data access
  - ITU req: 1Gb/s stationary / 100Mb/s moving data rate
Mobile Telephone Network
US Recent History

- 1978–present: analog to digital and data services
  - 1977: Bell Labs begins first AMPS cellular trial in Chicago
    - 2000 car phones manufactured by OKI, E.F. Johnson, Motorola
  - 1979: first AMPS deployment in Tokyo by NTT
  - 1984: first commercial US AMPS deployment
  - 1991: first digital deployment – GSM in Germany
    - 14.4 kb/s
  - 2000: GPRS general packet radio service) for GSM
    - up to 64kb/s
    - begins to replace CDPD in US
  - 2003: FCC requires number portability for wireless service
Mobile Cellular Telephony
First Generation: Analog Voice

• 1G: analog voice
• 2G: digital voice
• 3G: moderate-rate data access
• 4G: high-rate data access
Mobile Cellular Telephony
First Generation: Analog Voice

- 1G (first generation) mobile telephony
  - voice: analog modulation of analog signal
  - control: analog modulation of digital signal
  - data: no support

- Development
  - trials in 1970s
  - first commercial services in 1980s
  - ubiquitous in 1990s
    - most cities & along freeways, motorways, autobahnen
Mobile Cellular Telephony
Prehistory: Mobile Radio Telephone

- Mobile radio telephone (0G) problem?
Mobile Cellular Telephony
Prehistory: Mobile Radio Telephone

- Mobile radio telephone (0G)
  - all calls required operator assistance
  - not scalable

*Solution?*
Mobile Cellular Telephony
Prehistory: Mobile Radio Telephone

• Mobile radio telephone (0G)
  – all calls required operator assistance
  – expensive service restricted to selected metro areas
    • no ability to roam
  – not scalable for mass deployment
• Solution: cellular mobile telephone network
1G Mobile Cellular Telephony

Characteristics

- First generation: analog cellular telephony
- Handsets
  - large and bulky
  - similar in size to wired phones with lead-acid batteries
    - e.g. "bag phone"
  - later more compact with NiCd batteries with poor life
    - e.g. 1989 Motorola MicroTAC (total area coverage) flip phone
- Call characteristics
  - attenuation and noise resulted in variable quality
  - quality degraded significantly when roaming between cells
1G Mobile Cellular Telephony
Deployed Systems

• 1G deployments: multiple incompatible systems
  – AMPS (advanced mobile phone system)
    • US, South America, Australia, China, Japan
  – NMT (Nordic mobile telephone)
    • Nordic countries, Switzerland, Eastern Europe, Soviet Union
  – TACS (total access communications system)
    • United Kingdom, Ireland, Japan (JTAC)
  – B-Netz, C-Netz
    • West Germany, Austria, Portugal, South Africa
  – RTM (radio telephone mobile)
  – Radiocom 2000

Consequence to user?
1G Mobile Cellular Telephony deployed systems

- 1G deployments: multiple incompatible systems
  - AMPS (advanced mobile phone system)
    - US, South America, Australia, China, Japan
  - NMT (Nordic mobile telephone)
    - Nordic countries, Switzerland, Eastern Europe, Soviet Union
  - TACS (total access communications system)
    - United Kingdom, Ireland, Japan (JTAC)
  - B-Netz, C-Netz
    - West Germany, Austria, Portugal, South Africa
  - RTM (radio telephone mobile)
    - Italy
  - Radiocom 2000
    - France

- No ability to roam between systems and countries
1G Mobile Cellular Telephony

AMPS History

- AMPS (advanced mobile phone system)
  - US, South America, Australia, China
  - 1977: Bell Labs begins first AMPS cellular trial in Chicago
    - 2000 car phones manufactured by OKI, E.F. Johnson, Motorola
  - 1979: first AMPS deployment in Tokyo by NTT
  - 1984: first commercial US AMPS deployment
  - late 1990s: AMPS superceded by 2G digital in major markets
  - 2008: FCC ends AMPS service requirement
1G Mobile Cellular Telephony
AMPS US Deployment

- FCC granted two licenses for each market
  - A: second service provider (e.g. Cellular One)
  - B: incumbent wireline provider (e.g. RBOC)
  - each allocated 333 voice + 21 control channels
  - later expanded to 416 voice channels
    - FCC reclaimed UHF TV channels 70 – 83
- Initially A/B network manually provisioned in phone
  - phone identified by EIN
  - no automatic roaming between carriers
  - special roaming codes needed to receive calls
1G Mobile Cellular Telephony
AMPS Link Characteristics

- **AMPS** (advanced mobile phone system)
  - US, South America, Australia, China
- **Frequency bands:** $2 \times 25$ MHz
  - base station: 869 – 894 MHz
  - handset: 824 – 849 MHz, 3W max
- **Channels:** 30 kHz bandwidth
  - 790 full-duplex analog voice channels
    - FM with no encryption
  - 2 (rev & fwd) $\times$ 42 full-duplex digital control channels
    - 10 kb/s FSK framed with BCH error coding
- **Cells:** 2 – 20 km diameter

based on [Stallings 2005] Table10.4
1G Mobile Cellular Telephony

AMPS Operation

- Handset has NAM (numeric assignment module) in ROM
  - telephone number + serial number
- NAM transmitted to MSC
  - phone number used for billing
  - stolen phones locked out
- User dials optional PIN and phone number
  - NAM and PIN transmitted in clear
    - NAM cloning became common theft-of-service
- MSC
  - replies to handset with voice channel assignment
  - completes call to destination through PSTN

Based on [Stallings 2005] Table 10.4
2G Mobile Cellular Telephony
Motivation and Characteristics

Problems with 1G cellular telephony?
2G Mobile Cellular Telephony
Motivation and Characteristics

• Problems with 1G cellular telephony
  – analog voice transmission subject to noise and interference
  – developed reputation for poor quality

Solution?
2G Mobile Cellular Telephony
Motivation and Characteristics

- Problems with 1G cellular telephony
  - analog voice transmission subject to noise and interference
  - developed reputation for poor quality
- Solution
  - digital coding of voice channels
Mobile Cellular Telephony
Second Generation: Digital Voice

- **1G**: analog voice
- **2G**: digital voice
  - 2.5G: 2nd generation with new data services
  - 2.75G: 2nd generation with enhanced data rates
- **3G**: moderate-rate data access
- **4G**: high-rate data access
2G Mobile Cellular Telephony

Characteristics

• Second generation: *digital* cellular telephony

• Handsets
  – smaller than analog sets
    • driven by more compact digital components and Moore’s law
  – later premium phones very small
    • e.g. 1996 Motorola StarTAC: 1st small clamshell

• Call characteristics
  – marketing claim: clear voice with no dropped calls
  – reality:
    • better quality when signal strong
    • *worse* quality when signal very weak, especially during handoff
2G Mobile Cellular Telephony
Deployed Systems: TDMA

- 2G TDMA deployments
  - GSM (Groupe Spécial Mobile) →
    (global system for mobile communications)
    - Europe and most of the world
  - iDEN (integrated digital enhanced network)
    - developed by Motorola
    - US (Nextel), Canada (Telus Mobility)
  - D-AMPS (digital AMPS) IS-136 using AMPS channels
    - US (US Cellular former AT&T Wireless), Canada (Rogers)
  - PDC (personal digital cellular)
    - Japan (NTT DoCoMo), South Korea

- 2G CDMA deployments
2G Mobile Cellular Telephony

Deployed Systems: CDMA

- 2G TDMA deployments
- 2G CDMA deployments
  - IS-95 cdmaOne
    - developed by Qualcomm
    - US (many carriers including Sprint and Verizon), Canada, Mexico, Australia, Korea, China, India, Israel, Sri Lanka, Venezuela, Brasil
    - became dominant system in the US
    - now losing US market share to GSM (T-Mobile, at&t/Cingular)
# 2G Mobile Cellular Telephony

## Link Characteristics

<table>
<thead>
<tr>
<th></th>
<th>AMPS</th>
<th>D-AMPS</th>
<th>GSM</th>
<th>cdmaOne</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>analog</td>
<td>digital</td>
<td>digital</td>
<td>digital</td>
</tr>
<tr>
<td><strong>Coding</strong></td>
<td>FM</td>
<td>TDMA</td>
<td>TDMA</td>
<td>CDMA</td>
</tr>
<tr>
<td><strong>Band MHz BS</strong></td>
<td>869 – 894</td>
<td>869 – 894</td>
<td>935 – 960</td>
<td>869 – 894</td>
</tr>
<tr>
<td><strong>MT</strong></td>
<td>824 – 849</td>
<td>824 – 849</td>
<td>890 – 915</td>
<td>824 – 849</td>
</tr>
<tr>
<td><strong>Channel BW</strong></td>
<td>30 kHz</td>
<td>30 kHz</td>
<td>200 kHz</td>
<td>1.25 MHz</td>
</tr>
<tr>
<td><strong>Duplex channels</strong></td>
<td>790 + 42</td>
<td>832</td>
<td>125</td>
<td>20</td>
</tr>
<tr>
<td><strong>Mux. degree</strong></td>
<td>1</td>
<td>3</td>
<td>8</td>
<td>35</td>
</tr>
<tr>
<td><strong>Max. xmit. power</strong></td>
<td>3 W</td>
<td>3 W</td>
<td>20 W</td>
<td>200 mW</td>
</tr>
<tr>
<td><strong>Modulation</strong></td>
<td>FM + FSK</td>
<td>$\pi/4$ DQPSK</td>
<td>GMSK</td>
<td>QPSK</td>
</tr>
</tbody>
</table>

Based on [Stallings 2005] Table 10.5
Overview

• Groupe Spécial Mobile (GSM)
  – formed in 1987 by CEPT
    Conférence européeenne des administrations des postes et des télécommunications
    European conference of Postal and Telecommunication Administrations
  – 1987: MOA signed toward common European deployment
  – 1990: ETSI standard published
    European Telecommunications Standards Institute

• Renamed Global System for Mobile communication
  – recent standards freely available from www.etsi.org

• Most widely deployed system worldwide
  – except North America, Japan, Korea
2G GSM TDMA
Link Characteristics

- Symmetric forward / reverse links

<table>
<thead>
<tr>
<th>Band</th>
<th>400/450 MHz</th>
<th>850 MHz</th>
<th>900 MHz</th>
<th>1800 MHz</th>
<th>1900 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use</td>
<td>1G reuse</td>
<td>N. America</td>
<td>original</td>
<td></td>
<td>N. America</td>
</tr>
<tr>
<td>Forward</td>
<td></td>
<td></td>
<td>935 – 960</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reverse</td>
<td></td>
<td></td>
<td>890 – 915</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- TDMA within FDMA with slow FHSS (1hop /4.615 ms)
  - 125 full-duplex channels
  - 8 logical channels (slots) /frame
  - 1 hop / 4.615 ms to improve multipath resistance
2G GSM TDMA

Channels

- **TCH**: traffic channels
  - voice: full rate (28.8 kb/s) and half rate (11.4 kb/s)
  - data: 4.8, 9.6, and 14.4 kb/s
  - data to 57.6 kb/s with HSCSD channel group enhancement

- **CCH**: control channels for signalling
  - **BCCH**: broadcast CCH
    - broadcast of information to all MSs
  - **CCCH**: common CCH
    - connection management
  - **DCCH**: dedicated CCH
    - bidirectional signalling channels
2.5G GSM TDMA

GPRS Overview

- **GPRS**: General Packet Radio Service
  - data packet transport over GSM
- **Data rate varies**
  - based on multi-slot allocation
    - various combinations of downlink/uplink
  - based on adaptive coding: 8 – 20 kb/s per slot
  - theoretical maximum of 107 kb/s per 5 slots
    - not a normal service offering
EDGE: Enhanced Data Rates for GSM Evolution
  - enhanced data packet transport over GSM
  - meets technical definition of 3G
    - but slower than current 3G technologies UMTS and EV-DO

Data rate varies
  - 236.8 kb/s per 4 slots
IS-95 CDMA

Overview

- Developed by Qualcomm in 1990
- Standardised as TIA/EIA IS-95 (interim standard 95) [Telecommunications Industry Association] [Electronic Industries Alliance] in 1993
- Branded by CDG [CDMA Development Group] as cdmaOne
CDMA vs. TDMA
Advantages and Disadvantages

- CDMA advantages
  - resistance to interference and fading
  - resistance to multipath interference
    - orthogonal chipping sequences
  - physical layer confidentiality
    - but not impossible to crack!
  - graceful degradation as load increases
CDMA vs. TDMA
Advantages and Disadvantages

• CDMA advantages
  – resistance to interference and fading
  – resistance to multipath interference
    • orthogonal chipping sequences
  – physical layer confidentiality (but not impossible to crack!)
  – graceful degradation as load increases

• CDMA disadvantages
  – self-jamming from non-synchronised users
    • no equivalent of TDMA guard bands
  – power management more important
  – soft handoff required (why?)
    • more complex
IS-95 CDMA
2G Voice Network Architecture

- **BTS**: base transceiver station
  - cell tower and transceivers
- **BSC**: base station controller
  - intelligence for multiple BTSs
- **MSC**: mobile switching center
IS-95 CDMA

Link Characteristics

- Asymmetric forward / reverse links
- Forward link
  - 824 – 849 MHz
    (same frequency band as AMPS)
  - 1.228 MHz carriers, each with:
    - 64 CDMA DSSS logical channels
      - pilot (0): timing, phase, signal strength for handoff
      - paging (1–7): signalling messages for mobile terminals
      - synch. (32): 1200 b/s for identification of cellular system
      - traffic (8–31, 33–63) 9600 b/s
IS-95 CDMA
Link Characteristics

• Asymmetric forward / reverse links
• Reverse link
  – 869 – 894 MHz
    (same frequency band as AMPS)
  – 1.228 MHz carriers, each with:
    – up to 94 CDMA DSSS logical channels
      • \( \leq 32 \) for signalling
      • \( \leq 62 \) traffic
        unique ESN-based code per user
Mobile Cellular Telephony
Third Generation: Moderate Rate Data

• 1G: analog voice
• 2G: digital voice
• 3G: moderate-rate data access
• 4G: high-rate data access
3G Mobile Cellular Telephony
Motivation and Characteristics

Problems with 2G cellular telephony?
3G Mobile Cellular Telephony
Motivation and Characteristics

- Problems with 2G cellular telephony
  - nothing really, for voice...
3G Mobile Cellular Telephony
Motivation and Characteristics

- Problems with 2G cellular telephony
  - nothing really, for voice...
  - but not engineered for data and Internet access
3G Mobile Cellular Telephony
Motivation and Characteristics

• Problems with 2G cellular telephony
  – nothing really, for voice...
  – but not engineered for data and Internet access
  • but is this really the right device to access the Internet?
3G Mobile Cellular Telephony
Motivation and Characteristics

• Problems with 2G cellular telephony
  – nothing really, for voice...
  – but not engineered for data and Internet access
    • but is this really the right device to access the Internet?

Response?
3G Mobile Cellular Telephony
Motivation and Characteristics

• Problems with 2G cellular telephony
  – nothing really, for voice...
  – but not engineered for data and Internet access
    • but is this really the right device to access the Internet?

• Response of mobile service providers
  – hack data services into and onto cellular infrastructure
3G Mobile Cellular Telephony
Motivation and Characteristics

• Problems with 2G cellular telephony
  – nothing really, for voice...
  – but not engineered for data and Internet access
    • but is this really the right device to access the Internet?

• Response of mobile service providers
  – hack data services into and onto cellular infrastructure

• Market advantage
  – widely deployed wireless infrastructure
  – way ahead of 802.11
  – predates 802.16
3G Mobile Cellular Telephony
Standards and Interfaces

- **IMT-2000**: International Mobile Telecommunications 2000
  - ITU-R standard M.1457 for 3G networking
3G Mobile Cellular Telephony
Standards and Interfaces

- Five IMT-2000 air interfaces
  - IMT-DS: direct sequence
    - W-CDMA in UMTS
  - IMT-MC: multicarrier
    - CDMA2000 standardised by 3GPP (3G Partnership Project)
  - IMT-TD: time division
    - TD-CDMA standardised by 3GPP2
  - IMT-SC: single carrier
    - EDGE
  - IMT-FT: frequency time
    - DECT: ETSI standard digital enhanced cordless telephone
  - OFDMA TDD WMAN in 2007
    - based on 802.16e
cdma2000 EV-DO
Data Network Architecture

- **BTS:** base transceiver station
  - **DOM:** data-only module
- **RNC:** radio network controller
  - **AAA:** authentication, auth., & acct.
- **PDSN:** packet data serving node
Mobile Cellular Telephony
Fourth Generation: High Rate Data

- 1G: analog voice
- 2G: digital voice
- 3G: moderate-rate data access
- 4G: high-rate data access
Fourth Generation Mobile Networking
Overview

• IMT-advanced (international mobile telecommunications)
  – ITU-R M.2133, M.2134

• ITU target
  – 100 Mb/s mobile
  – 1 Gb/s stationary

• Emerging service offerings
  – many based on 802.16
  – not actually 4G
    • buy may be spun as 4G by service providers
    • should be called 4.5 or 4.9G
Fourth Generation Mobile Networking
Emerging Standards: LTE

- Two competing standards
  - LTE based on UMTS GSM standards (work by 3GPP)
    - LTE appears to have won
  - UMB based on CDMA2000 (work by 3GPP2)
    - Qualcomm has ended work on UMB

- LTE: long term evolution (3GPP release 8)
  - E-UTRAN: evolved UMTS terrestrial radio access network
    - OFDMA downlink, SC-FDMA uplink (single carrier)
    - FDD or TDD link duplexing
  - AIPN: all IP network
  - data rates below that mandated by ITU for 4G
Fourth Generation Mobile Networking
Emerging Standards: LTE Advanced

- LTE Advanced
  - evolution of LTE to comply with ITU IMT-advanced
  - expected as part of 3GPP release 10
  - planned to be real 4G
Further Reading

MAC; Mobile and Wireless Networks

Acknowledgements

Some material in these foils comes from the textbook supplementary materials:

- Tannenbaum,
  *Computer Networks*
- Kurose & Ross,
  *Computer Networking: A Top-Down Approach Featuring the Internet*
- Sterbenz & Touch,
  *High-Speed Networking: A Systematic Approach to High-Bandwidth Low-Latency Communication*
  http://hsn-book.sterbenz.org