Wireless and Mobile Networks

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

Audio/Video recordings of this lecture are available on-line at:
http://www.cse.wustl.edu/~jain/cse473-20/

Overview

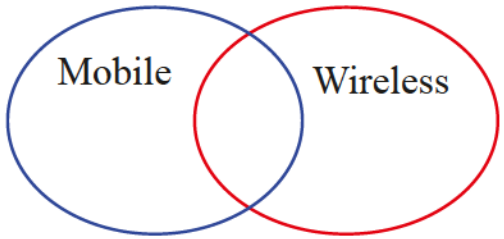
1. Wireless Link Characteristics
2. Wireless LANs and PANs
3. Cellular Networks
4. Mobility Management
5. Impact on Higher Layers

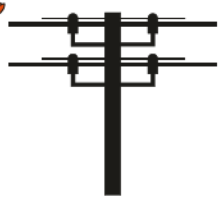
Note: This class lecture is based on Chapter 7 of the textbook (Kurose and Ross) and the figures provided by the authors.

Wireless Link Characteristics

- Mobile vs. Wireless
- Wireless Networking Challenges
- Peer-to-Peer or Base Stations?
- Code Division Multiple Access (CDMA)
  - Direct-Sequence Spread Spectrum
  - Frequency Hopping Spread Spectrum

Mobile vs Wireless

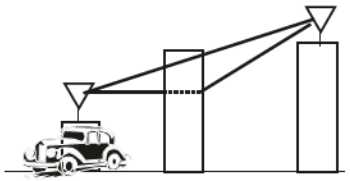




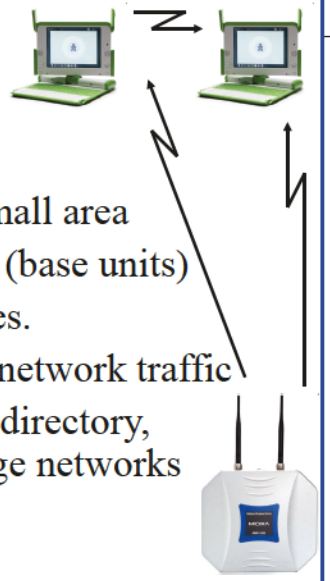
- Mobile vs Stationary
- Wireless vs Wired
- Wireless ⇒ media sharing issues
- Mobile ⇒ routing, addressing issues

Wireless Networking Challenges

1. Propagation Issues: Shadows, Multipath
2. Interference ⇒ High loss rate, Variable Channel
   ⇒ Retransmissions and Cross-layer optimizations
3. Transmitters and receivers moving at high speed
   ⇒ Doppler Shift
4. Low power transmission ⇒ Limited reach
   100mW in WiFi base station vs. 100 kW TV tower
5. License-Exempt spectrum ⇒ Media Access Control
6. Limited spectrum ⇒ Limited data rate
   Original WiFi (1997) was 2 Mbps.
   New standards allow up to 200 Mbps
7. No physical boundary ⇒ Security
8. Mobility ⇒ Seamless handover

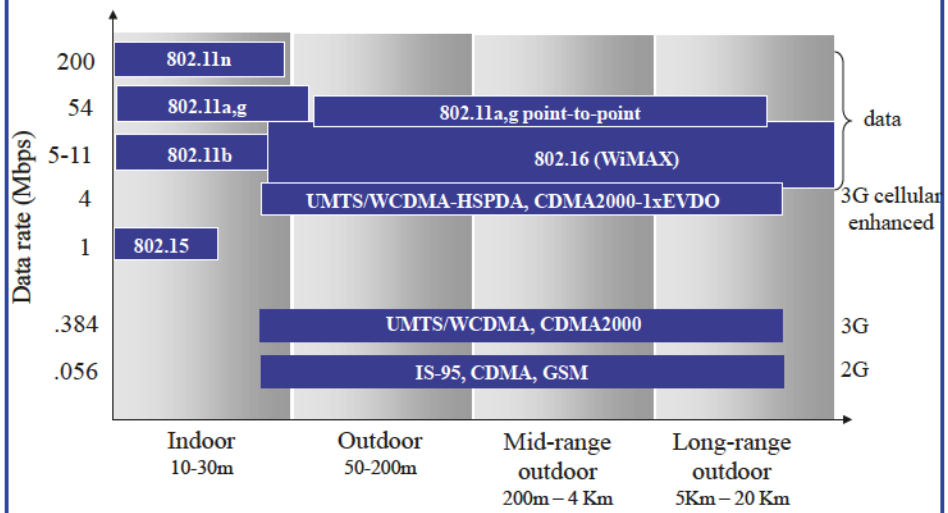


Peer-to-Peer or Base Stations?

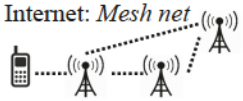
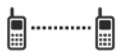
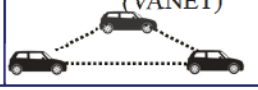


- Ad-hoc (Autonomous) Group:
  - Two stations can communicate
  - All stations have the same logic
  - No infrastructure, Suitable for small area
- Infrastructure Based: Access points (base units)
  - Stations can be simpler than bases.
  - Base provide connection for off-network traffic
  - Base provides location tracking, directory, authentication ⇒ Scalable to large networks
- IEEE 802.11 provides both.

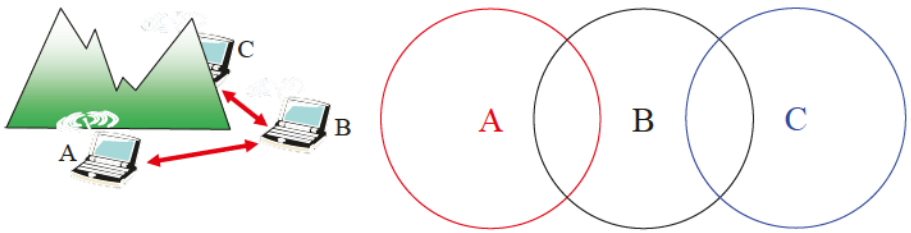
Characteristics of Selected Wireless Link Standards



Wireless Network Taxonomy

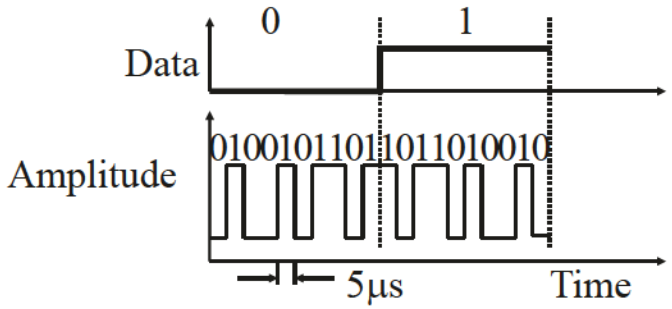
	Single hop	Multiple hops
Infrastructure (Access Points, Towers)	Host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet 	Host may have to relay through several wireless nodes to connect to larger Internet: *Mesh net* 
No Infrastructure	No base station (Bluetooth, ad hoc nets) 	Relay to reach other a given wireless node. Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc Network (VANET) 

Hidden Node Problem



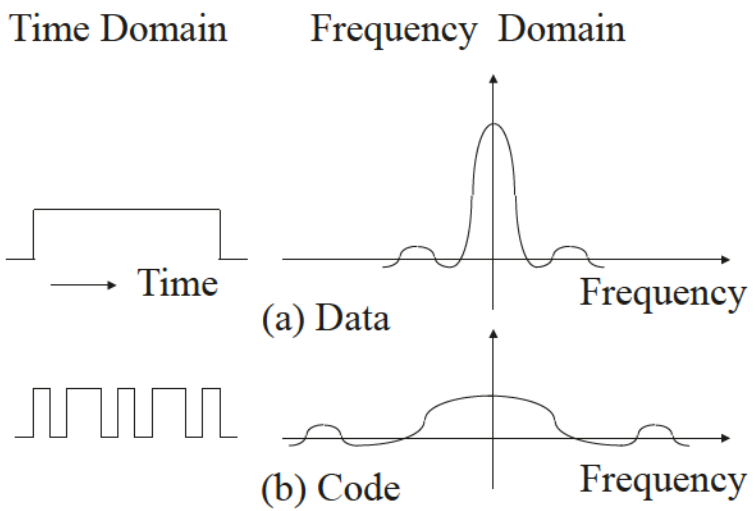
- B and A can hear each other
  B and C can hear each other
  A and C cannot hear each other
  ⇒ C is hidden for A and vice versa
- C may start transmitting while A is also transmitting
  A and C can't detect collision.
- Only the receiver can help avoid collisions

Direct-Sequence Spread Spectrum CDMA

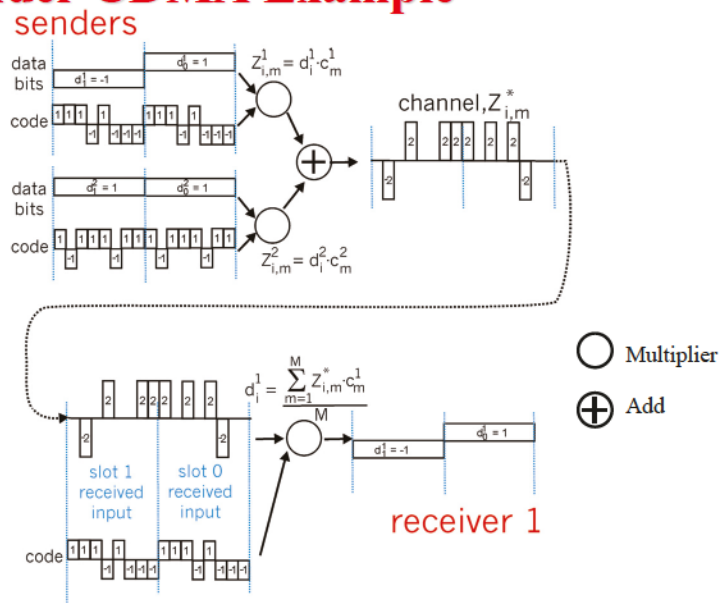


- Spreading factor = Code bits/data bit, 10-100 commercial (Min 10 by FCC), 10,000 for military
- Signal bandwidth >10 × data bandwidth
- Code sequence synchronization
- Correlation between codes ⇒Interference⇒□Orthogonal

DS Spectrum



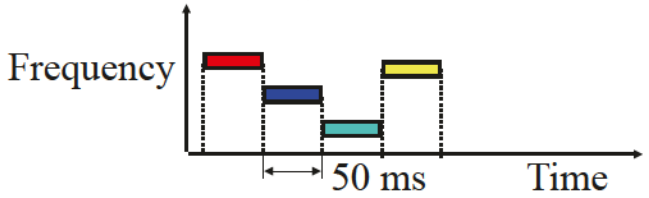
Two Sender CDMA Example



Homework 7A: CDMA Coding

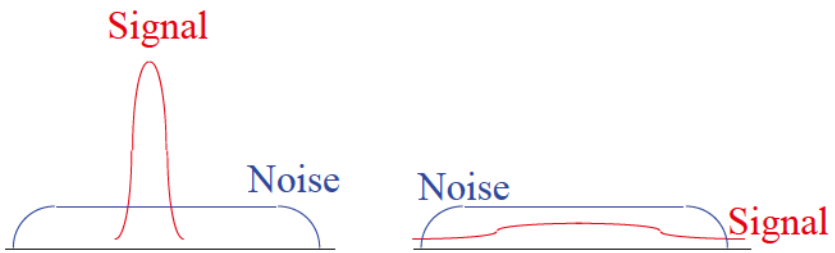
- [6 points] Two CDMA sender use the codes of (1, -1, 1, -1) and (1, -1, -1, 1). First sender transmits data bit 1 while the 2nd transmits –1 at the same time. What is the combined signal waveform seen by a receiver? Draw the waveform.

Frequency Hopping Spread Spectrum



- Pseudo-random frequency hopping
- Spreads the power over a wide spectrum
  ⇒ Spread Spectrum
- Developed initially for military
- Patented by actress Hedy Lamarr (1942)
- Narrowband interference can't jam

Spectrum



(a) Normal (b) Frequency Hopping

Review: Wireless Link Characteristics

1. Wireless is not the same as mobile. However, most mobile nodes are wireless.
2. Wireless signal is affected by shadows, multipath, interference, Doppler shift
3. A wireless network can be ad-hoc or infrastructure based.
4. Multi-hop ad-hoc networks are called MANET
5. It is not possible to do collision detection in wireless
6. Code division multiple access is commonly used in wireless

Ref: Section 7.2, Review Exercises R3-R4

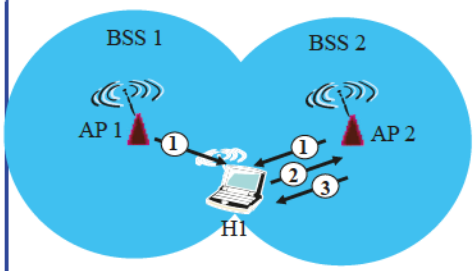
Wireless LANs and PANs

- IEEE 802.11 Wireless LAN PHYs
- 4-Way Handshake
- IEEE 802.11 MAC
- 802.11 Frame Format
- 802.11 Frame Addressing
- 802.11 Rate Adaptation
- Power Management
- IEEE 802.15.4
- IEEE 802.15.4 MAC
- ZigBee Overview

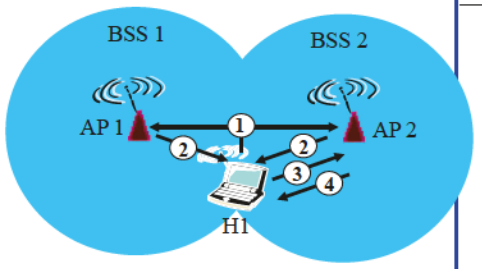
IEEE 802.11 Wireless LAN PHYs

- **802.11**: 2.4 GHz, 1-2 Mbps
- **802.11b**: 2.4 GHz, 11 Mbps nominal
  - Direct sequence spread spectrum (DSSS) in physical layer
  - All hosts use the same chipping code
- **802.11a**: 5.8 GHz band, 54 Mbps nominal
- **802.11g**: 2.4 GHz band, 54 Mbps nominal
- **802.11n**: 2.4 or 5.8 GHz, Multiple antennae, up to 200 Mbps
- These are different PHY layers. All have the same MAC layer.
- All use CSMA/CA for multiple access
- All have base-station and ad-hoc network versions
- Supports multiple priorities
- Supports time-critical and data traffic
- Power management allows a node to doze off

802.11: Passive/Active Scanning

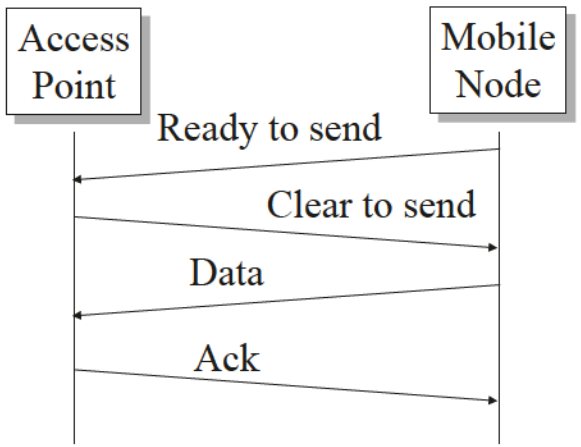


Passive Scanning:
(1) Beacon frames sent from APs
(2) Association Request frame sent: H1 to selected AP
(3) Association Response frame sent: selected AP to H1



Active Scanning:
(1) **Probe Request** frame broadcast from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent: selected AP to H1

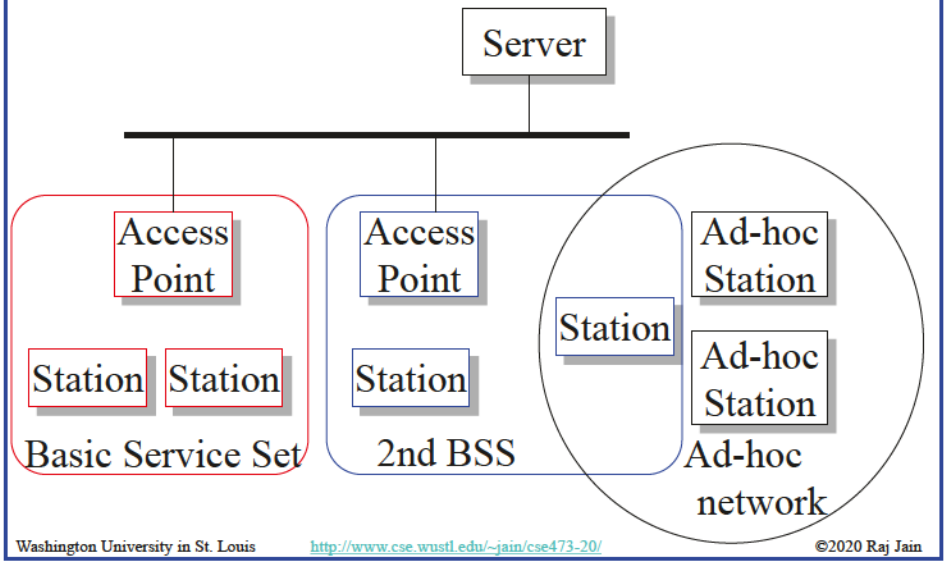
4-Way Handshake



IEEE 802.11 MAC

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Listen before you talk. If the medium is busy, the transmitter backs off for a random period.
- Avoids collision by sending a short message:
  Ready to send (RTS)
  RTS contains dest. address and duration of message.
  Tells everyone to backoff for the duration.
- Destination sends: Clear to send (CTS)
- Can not detect collision ⇒ Each packet is acked.
- MAC level retransmission if not acked.

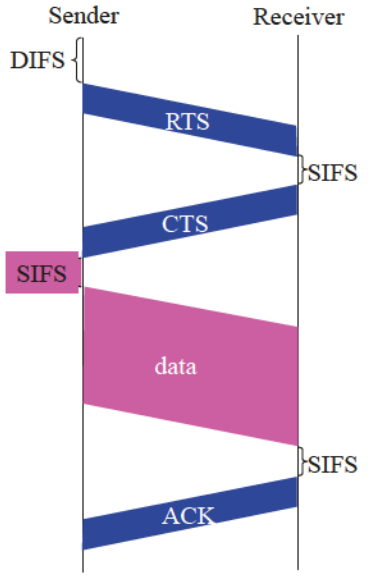
IEEE 802.11 Architecture



Architecture (Cont.)

- Basic Service Area (BSA) = Cell
  Area: Geographical area = a room, or a building
- Each BSA may have several wireless LANs
- Extended Service Area (ESA) = Multiple BSAs interconnected via Access Points (AP) = Multiple rooms in your home with different extenders advertising the same SSID
- Basic Service Set (BSS)
  = Set of stations associated with an AP = $\{MAC_1,\ldots,MAC_n\}$.
  Each BSS has a Service Set ID (SSID), e. g., WUSTL-Guest
- Extended Service Set (ESS)
  = Set of stations in an ESA
- Ad-hoc networks coexist and interoperate with infrastructure-based networks.

Transmission Example



SIFS, DIFS are intervals set by the standards. 11b and 11ac have different values.

RTS, CST, ACK are each one slot time long.

Each frame has a duration field.

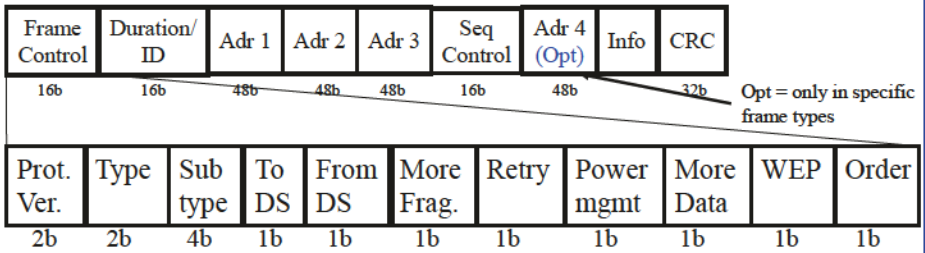
Every frame is heard by every one.

Homework 7B: WiFi Transmission

- [6 points] Suppose an 802.11b station is configured to always reserve the channel with the RTS/CTS sequence. Suppose this station suddenly wants to transmit 1,000 bytes of data, and all other stations are idle at this time. Using SIFS of 10us and DIFS of 50us, and ignoring propagation delay and assuming no bit errors, calculate the time required to transmit the frame and receive the acknowledgment. Assume a frame without data (RTS/CTS/Ack) is 32 bytes long and the transmission rate is 11 Mbps.

Ref: Problem P7

Wi-Fi Frame Format



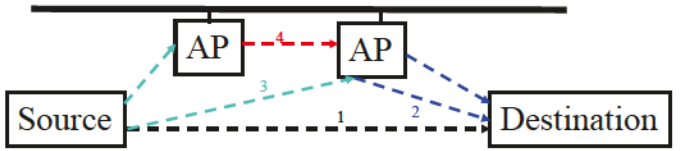
- Type: Control, management, or data
- Sub-Type: Association, disassociation, re-association, probe, authentication, de-authentication, CTS, RTS, Ack, …
- Retry/retransmission
- Going to Power Save mode
- More buffered data at AP for a station in power save mode
- Wireless Equivalent Privacy (Security) info in this frame
- Strict ordering

MAC Frame Fields

- **Duration/Connection ID**:
  - If used as duration field, indicates time (in μs) channel will be allocated for successful transmission of MAC frame. Includes time until the end of Ack
  - In some control frames, contains association or connection identifier
- **Sequence Control**:
  - 4-bit fragment number subfield
    - For fragmentation and reassembly
  - 12-bit sequence number
  - Number frames between given transmitter and receiver

802.11 Frame Address Fields

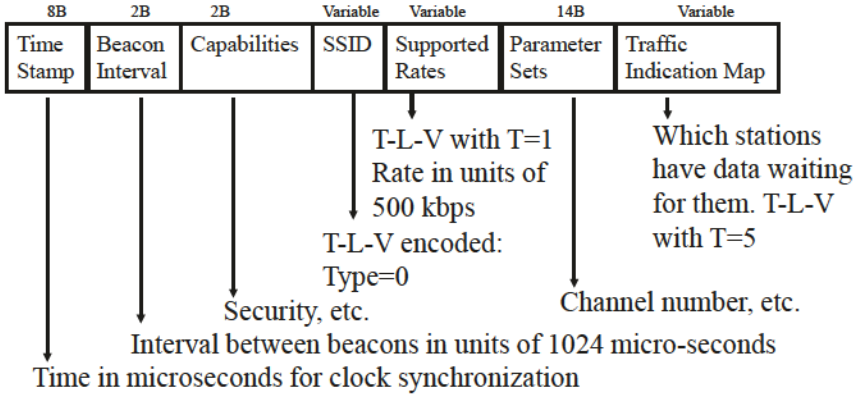
- All stations filter on "Address 1"



	To Distribution System	From Distribution System	Address 1	Address 2	Address 3	Address 4
1	0	0	Destination Address	Source Address	BSS ID	-
2	0	1	Destination Address	BSS ID	Source Address	-
3	1	0	BSS ID	Source Address	Destination Address	-
4	1	1	Receiver Address	Transmitter Address	Destination Address	Source Address

Beacon Frame Format

- Info field in the 802.11 frame (after Address 4)



Ref: Nayarasi, "802.11 Mgmt: Beacon Frame," https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame/

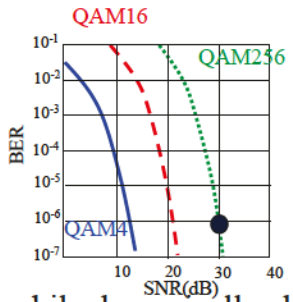
Lab 7:WiFi

[14 Points] Download the Wireshark traces from http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

Open *Wireshark_802_11.pcap* in Wireshark. Select **View → Expand All**. Answer the following questions. There is no need to attach screen captures.

1. Frame 1 is a beacon frame. Ignore the first 24 bytes. (The frame control field is 80:00.) What is the SSID of the access point that is issuing this beacon frame?
2. What (in hexadecimal notation) is the source MAC address on Frame 1.
3. What (in hexadecimal notation) is the destination MAC address on the Frame 1?
4. What (in hexadecimal notation) is the MAC BSS ID in Frame 1?
5. Frame 50 is a Probe Request and Frame 51 is a Probe response. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?

802.11 Rate Adaptation



QAM=Quadrature Amplitude Modulation

$QAM2^n = n$ bits/Hz

dB = Deci-Bel

$= 10 \log_{10} \frac{\text{Power Out}}{\text{Power In}}$

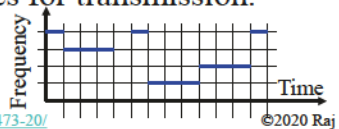
- Base station and mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies
- SNR decreases ⇒BER increase as node moves away from base station
- When BER becomes too high, switch to lower transmission rate but with lower BER

Power Management

- A station can be in one of three states:
  - Transmitter on
  - Receiver only on
  - Dozing: Both transmitter and receivers off.
- Access point (AP) buffers traffic for dozing stations.
- AP announces which stations have frames buffered. Traffic indication map included in each beacon. All multicasts/broadcasts are buffered.
- Dozing stations wake up to listen to the beacon. If there is data waiting for it, the station sends a poll frame to get the data.

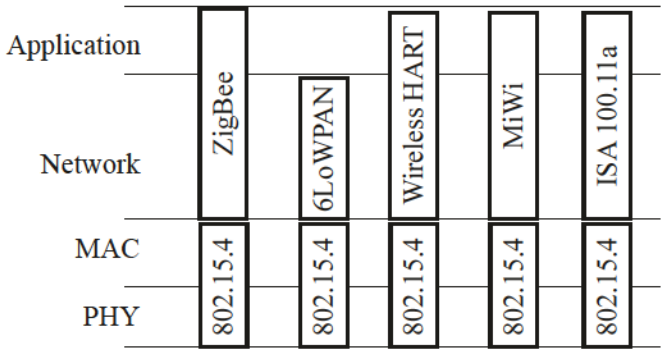
Bluetooth

- Started with Ericsson's Bluetooth Project in 1994
- Named after Danish king Herald Blatand (AD 940-981) who was fond of blueberries
- Radio-frequency communication between cell phones over short distances
- IEEE 802.15.1 approved in early 2002 is based on Bluetooth
- Key Features:
  - Lower Power: 10 μA in standby, 50 mA while transmitting
  - Cheap: $5 per device
- A piconet consists of a master and several slaves. Master determines the timing and polls slaves for transmission.
- Frequency hopping spread spectrum



IEEE 802.15.4

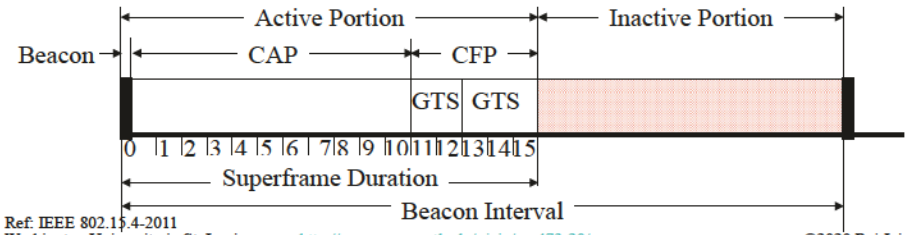
- Low Rate Wireless Personal Area Network (LR-WPAN)
- Used by several "Internet of Things" protocols: ZigBee, 6LowPAN, Wireless HART, MiWi, and ISA 100.11a
- Lower rate, short distance ⇒ Lower power ⇒ Low energy



IEEE 802.15.4 MAC

Beacon-Enabled CSMA/CA

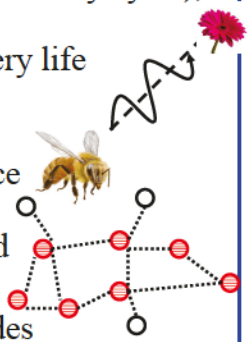
- Coordinator sends out beacons periodically
- Part of the beacon interval is inactive ⇒ Everyone sleeps
- Active interval consists of 16 slots
- Contention Access Period (CAP). Slotted CSMA.
- Contention Free Period (CFP)
  - Guaranteed Transmission Services (GTS): For real-time services. Periodic reserved slots.



Ref: IEEE 802.15.4-2011

ZigBee Overview

- Industrial monitoring and control applications requiring small amounts of data, turned off most of the time (<1% duty cycle), e.g., wireless light switches, meter reading
- Ultra-low power, low-data rate, multi-year battery life
- **Range**: 1 to 100 m, up to 65000 nodes.
- IEEE 802.15.4 MAC and PHY. Higher layer, interoperability by ZigBee Alliance
- Named after zigzag dance of the honeybees Direction of the dance indicates location of food
- Multi-hop ad-hoc mesh network



Multi-Hop Routing: message to non-adjacent nodes
Ad-hoc Topology: No fixed topology. Nodes discover each other
Mesh Routing: End-nodes help route messages for others
Mesh Topology: Loops possible

Ref: ZigBee Alliance, http://www.ZigBee.org

Review: Wireless LANs and PANs

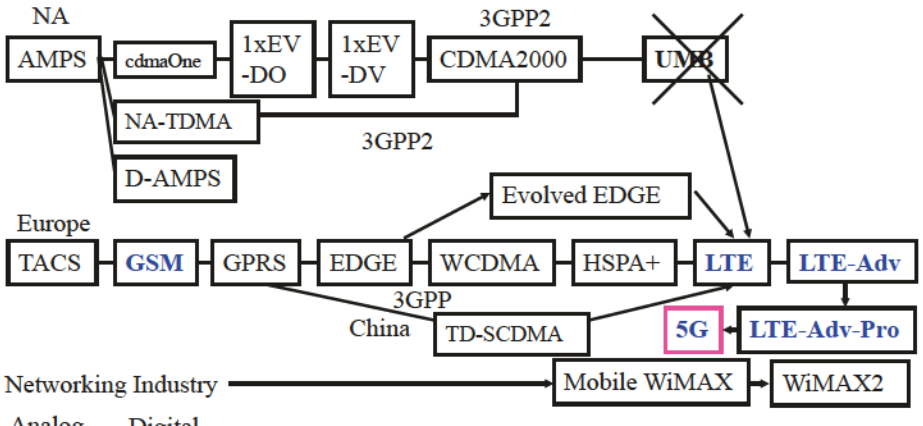
1. IEEE 802.11 PHYs: 11, 11b, 11g, 11a, 11n, …
2. IEEE 802.11 MAC uses CSMA/CA with a 4-way handshake: RTS, CTS, data, and ack
3. IEEE 802.11 network consists of ESS consisting of multiple BSSs each with an AP.
4. 802.11 Frame Format may have up to 4 addresses and includes final destination's MAC which may not be wireless
5. Power management allows stations to sleep.
6. Bluetooth uses frequency hopping spread spectrum
7. IEEE 802.15.4 PHY layer allows coordinators to schedule transmissions of other nodes
8. ZigBee uses IEEE 802.15.4

Ref: Section 7.3, Review Exercises R5-R13

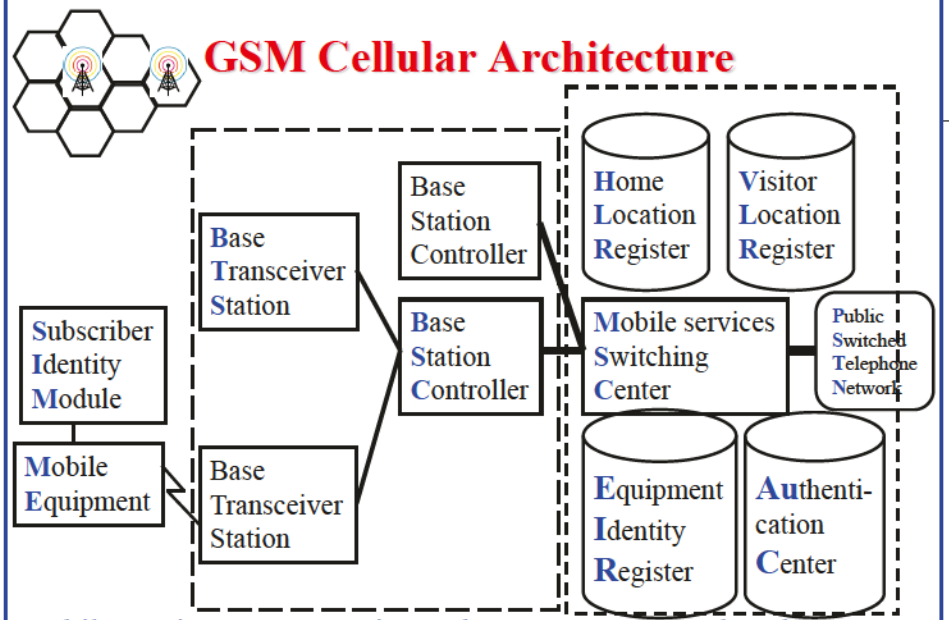
Overview Cellular Networks

- Evolution of Cellular Technologies
- GSM Cellular Architecture
- Evolved Packet System (EPS)

Cellular Telephony Generations



GSM Cellular Architecture



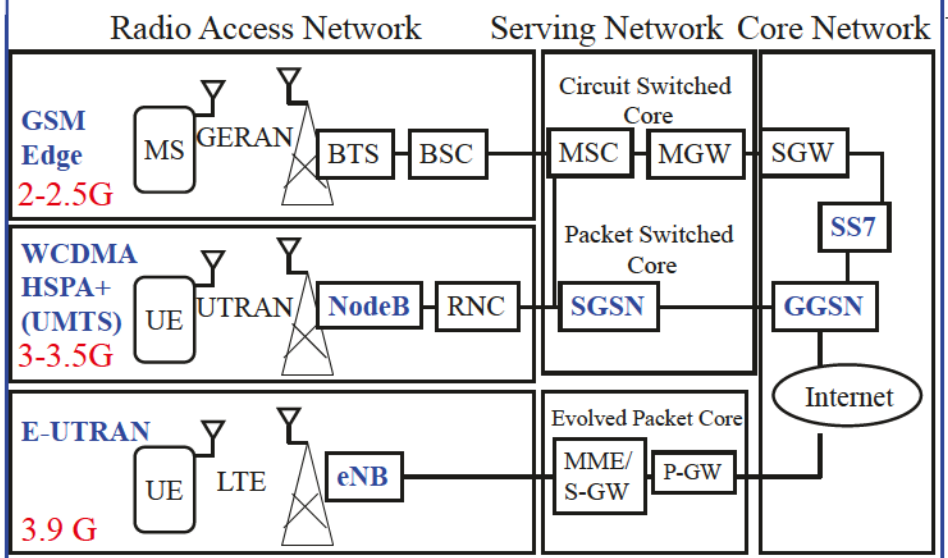
Cellular Architecture (Cont.)

- Base station controller (BSC) and Base transceiver station (BTS)
- One BTS per cell.
- One BSC can control multiple BTS.
  - Allocates radio channels among BTSs.
  - Manages call handoffs between BTSs.
  - Controls handset power levels
- Mobile Switching Center (MSC) connects to PSTN and switches calls between BSCs. Provides mobile registration, location, authentication. Contains Equipment Identity Register.

Cellular Architecture (Cont.)

- Home Location Register (HLR) and Visitor Location Register (VLR) provide call routing and roaming
- VLR+HLR+MSC functions are generally in one equipment
- Equipment Identity Register (EIR) contains a list of all valid mobiles.
- Authentication Center (AuC) stores the secret keys of all SIM cards.
- Each handset has a International Mobile Equipment Identity (IMEI) number.

Evolved Packet System (EPS)



Review: Cellular Networks

1. 1G was Analog voice, 2G was Digital voice, 3G was CDMA with voice and high-speed data, 4G is high-speed data
2. A cellular system has a RAN with BTS, BSC and a network subsystem with HLR, VLR, MSC, EIR, and AuC
3. 3G replaced RAN with UTRAN and BTS with NodeB. 4G uses eNB.

Ref: Section 7.4, Review Exercises R14-R17

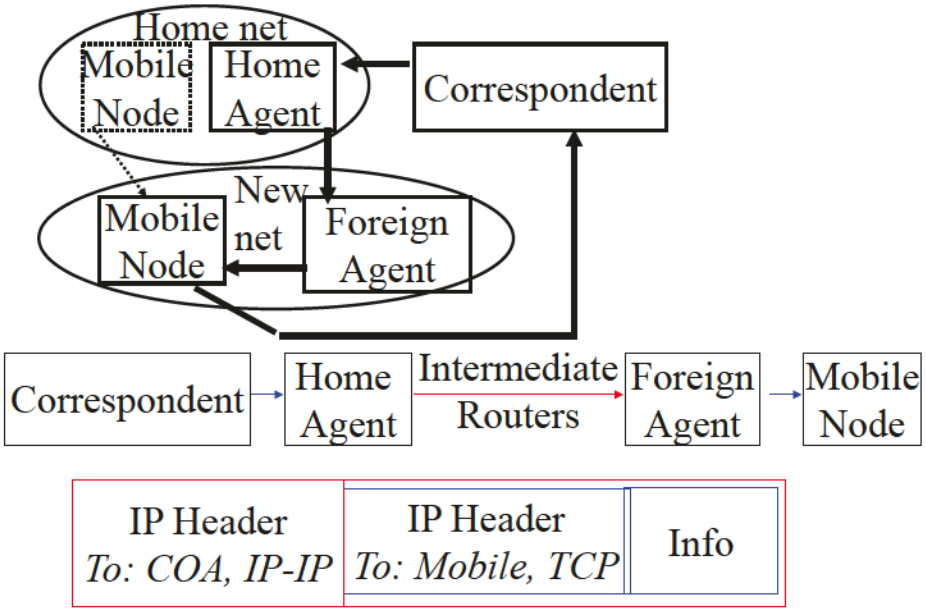
Mobility Management

- Mobile IP
- GSM: Routing to Mobile
- GSM Handoff
- Mobility: GSM versus Mobile IP

Mobility: Mr. Smith Goes to Washington

- We need:
  - An agent at home office: Home Agent
  - An agent at foreign office: Foreign Agent

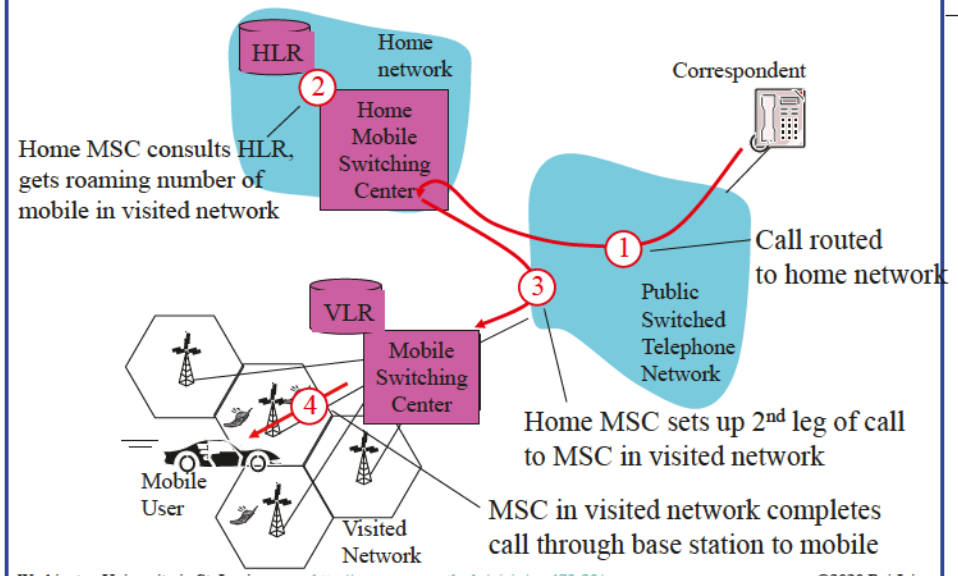
Mobile IP: Mechanisms



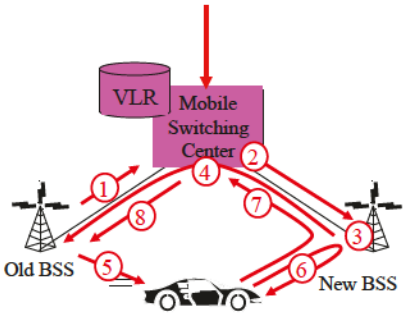
Mechanism (Cont.)

- Mobile node finds foreign agents via solicitation or advertising
- Mobile registers with the foreign agents and informs the home agent
- Home agent intercepts mobile node's datagrams and forwards them to the care-of-address
- Care-of-address (COA): Address of the end-of-tunnel towards the mobile node. May or may not be foreign agent
- At COA, datagram is extracted and sent to mobile

GSM: Routing to Mobile



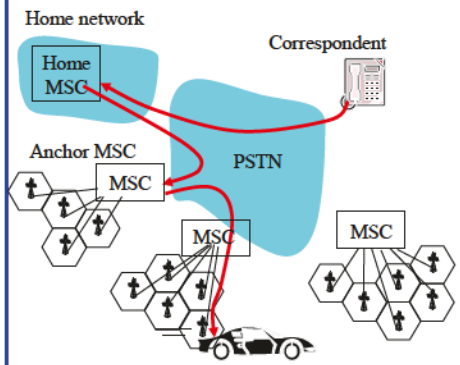
GSM: Handoff with Common MSC



1. Old BSS informs MSC of impending handoff, provides list of 1^+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. New BSS allocates radio channel for use by mobile
4. New BSS signals MSC, old BSS: ready
5. Old BSS tells mobile: perform handoff to new BSS
6. Mobile, new BSS signal to activate new channel
7. Mobile signals via new BSS to MSC: handoff complete. MSC reroutes call

8 MSC-old-BSS resources released

GSM: Handoff between MSCs



- *Anchor MSC:* first MSC visited during call
  - Call remains routed through anchor MSC
- New MSCs add on to end of MSC chain as mobile moves to new MSC
- IS-41 allows optional path minimization step to shorten multi-MSC chain

Review: Mobility Management

- Mobile IP uses Home Agent as an Anchor
  Packets are tunneled from Home Agent to Care-of-Address
- GSM uses HLR and VLR for mobility. All packets are routed through home network
- Handoff between towers in a single network is done through MSC

Ref: Sections 7.6 and 7.7, Review Exercises R18-R20

Impact on Higher Layer Protocols

- Layered Architecture ⇒ Upper layers are independent of lower layers
- Wireless ⇒ High error rate ⇒ Frequent packet losses
  ⇒ Triggers TCP congestion control even if no overload
- TCP modifications:
  - Local Recovery: Link level retransmissions and error correction
  - Wireless-aware TCP Sender:
    Distinguish overload (sustained) and random errors
  - Split-Connection: Host1-to-AP + AP-to-Host2

Summary

1. Code division multiple access "was" commonly used in wireless networks
2. IEEE 802.11 uses CSMA/CA with RTS, CTS, data, and ack. A frame may have up to 4 addresses.
3. Bluetooth and ZigBee are PANs that use very little energy
4. Cellular networks have evolved from analog voice to digital voice and finally to high-speed data.
5. Mobile IP uses home agents as anchors.
6. Cellular networks use MSCs to manage mobility.
7. Frequent packet losses due to errors may confuse TCP as network congestion.

CSE 574S: Wireless and Mobile Networking

1. How is wireless different from wired communication?
2. What are the protocols that are used in **IoT**?
3. Why do we need new protocols for IoT?
4. How does **WiFi** work? How 10 Mbps to 10 Gbps?
5. How is **Bluetooth** different from WiFi?
6. How is **ZigBee** different from WiFi?
7. What are other newer wireless protocols for IoT? LORAWAN
8. What is the basic difference between 1G/2G/3G/4G/5G
9. What new features came in with **4G**?
10. What new techniques enabled **5G**?
11. What about 6G? When and how?

Acronyms

1xEV-DO	1 times Evolution to Data Only
1xEV-DV	1 times Evolution to Data and Voice
3GPP1	3rd Generation Partnership Project
6LowPAN	IPv6 over Low Power Personal Area Networks
ACK	Acknowledgement
AMPS	Advanced Mobile Phone System
AP	Access Point
BER	Bit Error Rate
BSA	Basic Service Area
BSC	Base station controller
BSS	ID Basic Service Set Identifier
BTS	Base transceiver station
CA	Collision Avoidance
CAP	Contention Access Period
CDMA	Code Division Multiple Access
CEPT	Committee of European Posts and Telecom

Acronyms (Cont)

- CFP Contention Free Period
- COA Care-Of-Address
- CRC Cyclic Redundancy Check
- CSMA Carrier Sense Multiple Access
- CTS Clear to Transmit
- D-AMPS Digital Advanced Mobile Phone System
- dB Deci-Bel
- DCN Data Communication Network
- DHCP Dynamic Host Control Protocol
- DIFS Distributed Inter-Frame Spacing
- DSSS Direct Sequence Spread Spectrum
- E-UTRAN Evolved UTRAN
- EDGE Enhanced Data rate for GSM evolution
- EGPRS Enhanced GPRS
- EIA Electronic Industry Association
- EIR Equipment Identity Register

Acronyms (Cont)

- eNB evolved Node B
- ESA Extended Service Area
- ESS Extended Service Set
- FCC Federal Communications Commission
- FDMA Frequency Division Multiple Access
- GERAN GSM Enhanced Radio Access Network
- GGSN Gateway GPRS Support Node
- GHz Giga-Hertz
- GPRS General Packet Radio Service
- GSM Global System for Mobile Communications
- GTS Guaranteed Transmission Service
- GW Gateway
- HART Highway Addressable Remote Transducer Protocol
- HLR Home Location Register
- HSPA High Speed Packet Access
- HSPDA High Speed Packet Download Access

Acronyms (Cont)

- ID Identifier
- IEEE Institution of Electrical and Electronics Engineers
- IFS Inter-frame space
- IMEI International Mobile Equipment Identity
- IP Internet Protocol
- IS International Standard
- ISA International Society of Automation
- ISDN Integrated Switched Digital Network
- kW Kilo-Watt
- LAN Local Area Network
- LR Long-Range
- LTE Long-Term Evolution
- mA Milli-Ampere
- MAC Media Access Control
- MANET Mobile Ad-hoc Network
- MGW Media Gateway

Acronyms (Cont)

- MHz Mega Hertz
- MIMO Multiple Input Multiple Output
- MME Mobility Management Entity
- MS Mobile Subscriber
- MSC Mobile Switching Center
- mW Milli-Watt
- NA North America
- NAT Network Address Translator
- NodeB Node B (Base Station)
- PAN Personal Area Network
- PC Personal Computer
- PHY Physical Layer
- PIFS Point-Coordination Inter-Frame Spacing
- PSTN Public Switched Telephone Network
- QAM Quadrature Amplitude Modulation

Acronyms (Cont)

- RAN Radio Access Network
- RNC Radio Network Controller
- RTS Ready to send
- SCDMA Synchronous CDMA
- SGSN Service GPRS Support Node
- SGW Serving Gateway
- SIFS Short Inter-Frame Spacing
- SIM Subscriber Identification Module
- SNR Signal to Noise Ratio
- SS7 Signaling System 7
- SSID Service Set Identifier
- SYN Synchronizing Frame
- TACS Total Access Communications System
- TCP Transmission Control Protocol
- TD-SCDMA Time Duplexed Synchronous Code Division Multiple Access
- TDMA Time Division Multiple Access

Acronyms (Cont)

- TIA Telecom Industry Association
- TV Television
- UE User Element
- UK United Kingdom
- UMB Ultra Mobile Broadband
- UMTS Universal Mobile Telecommunications System
- UTRAN UMTS Terrestrial Radio Access Network
- VANET Vehicular Ad-hoc Network
- VLR Visitor Location Register
- WCDMA Wide-band CDMA
- WEP Wired Equivalend Privacy
- WiFi Wireless Fidelity
- WPAN Wireless Personal Area Network

Scan This to Download These Slides

Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse473-20/i_7wmn.htm

Related Modules

CSE 567: The Art of Computer Systems Performance Analysis
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw

CSE 570: Recent Advances in Networking (Spring 2013)
https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Spring 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw