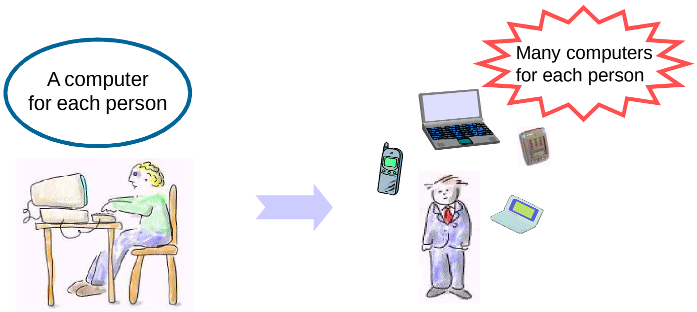
Wireless and Mobile Networks

Acknowledgements
These Slides have been adapted from the originals made available by J. Kurose and K. Ross

Background

- Internet explosion
- Wireless communications
- Increasing diffusion of portable/wearable devices



Current Experience

- Internet Access anywhere, anytime,
  - WiFi, GPRS/UMTS, WiMax, …
- by means of a variety of devices
  - Laptops, PDAs, smart phones, cell-phones
- for traditional and novel services
  - Web browsing, E-mail, File Sharing
  - Music/Video on the move
  - Location-based and context-aware applications
  - Personalized services
  - …

Current Experience

A lot of intelligent devices around us

- **Wearable devices**
  - Cell-phone, SmartPhone, Head-set, Cameras, Sensors, …
- **At office**
  - PC, Laptop, Printer, Access Point, ..
- **At home**
  - TV, Wash machine, …
- **On the car**
  - Sensors, processors, actuators
- **In the external environment**
  - Base stations, Access Points, Displays, Sensors …

Long-term Perspective

Pervasive (or Ubiquitous) Computing

"Specialized elements of hardware and software, connected by wires, radio waves and infrared, will so **ubiquitous** that no one will notice their presence"

User devices will interact with ambient devices to take intelligent decisions depending on the user context

Without or with minimal user intervention (invisible computing)

Communications between devices will occur mainly through wireless technologies

(Mark Weiser, 1991)

Pervasive/Ubiquitous Computing

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

Consider writing, perhaps the first information technology. [...] Today this technology is ubiquitous in industrialized countries. Not only do books, magazines and newspapers convey written information, but so do street signs, billboards, shop signs and even graffiti.

The constant background presence of these products of "literacy technology" does not require active attention, but the information to be conveyed is ready for use at a glance. It is difficult to imagine modern life otherwise.

Mark Weiser, The Computer for the 21st Century, *Scientific American, Special Issue on Communications, Computers, and Networks*, September, 1991.

Ubiquitous Internet

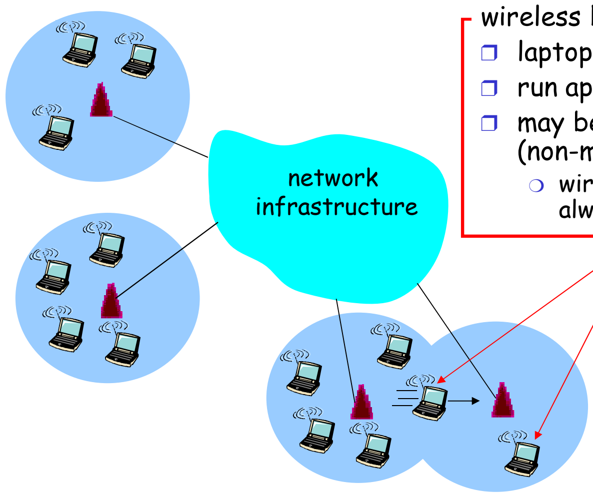
- Ubiquitous Internet Access
  - anywhere, anytime, with any device

- Two important (but different) challenges
  - *wireless:* communication over wireless link
  - *mobility:* handling the mobile user who changes point of attachment to network

Roadmap

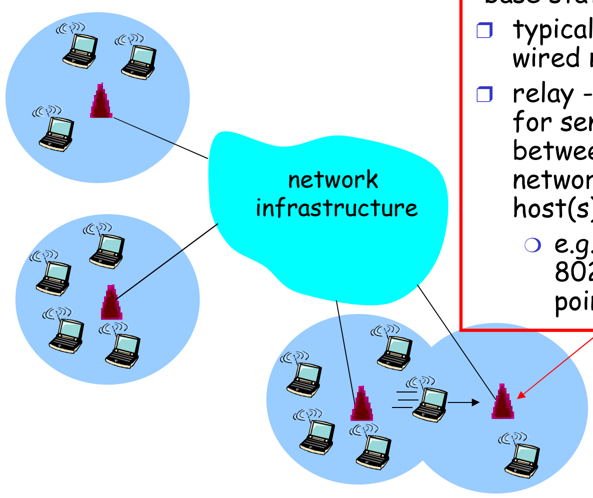
- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks

Elements of a wireless network



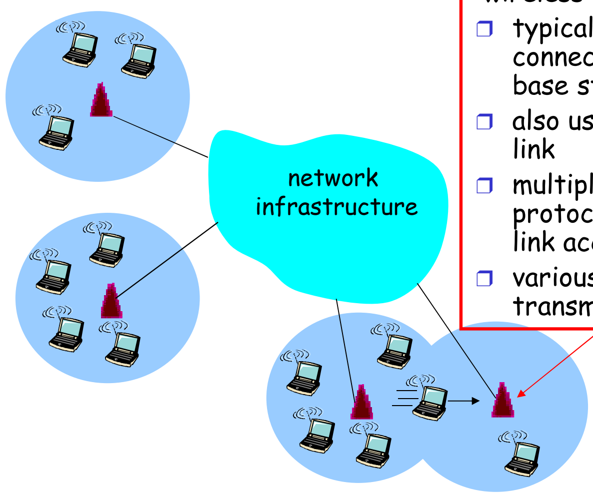
wireless hosts
- laptop, PDA, IP phone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

Elements of a wireless network



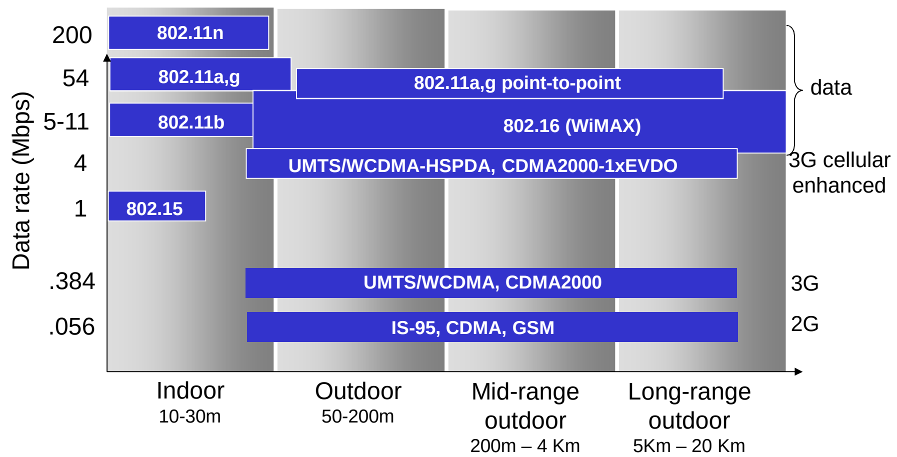
base station
- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

Elements of a wireless network



wireless link
- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Characteristics of selected wireless link standards



Wireless Link Characteristics (1)

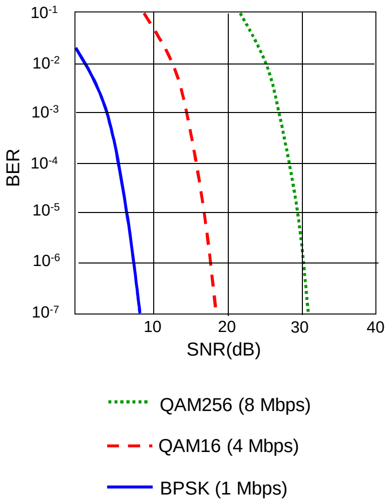
Differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more "difficult"

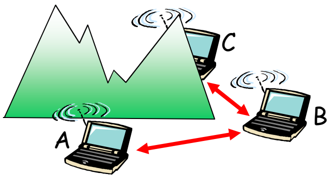
Wireless Link Characteristics

- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")
- *SNR versus BER tradeoffs*
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



Wireless network characteristics

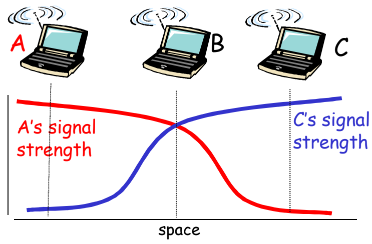
Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other

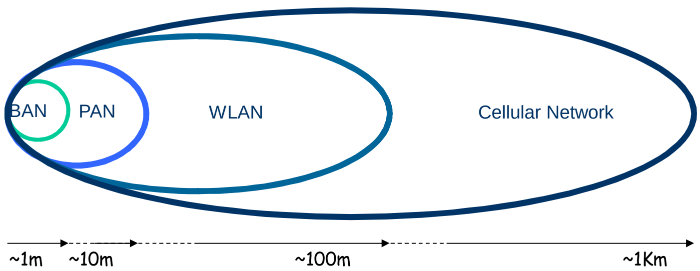
means A, C unaware of their interference at B



Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

Wireless Network Classification

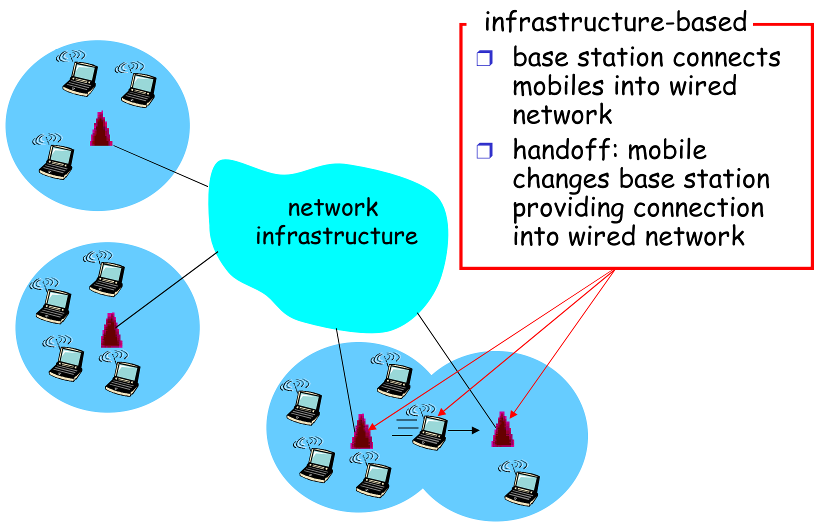


Cellular Network	GSM/GPRS/UMTS
WLAN	IEEE 802.11 (WiFi)
PAN	IEEE 802.15.1/4 (Bluetooth, ZigBee)
BAN	IEEE 802.15.1/4 (Bluetooth, ZigBee)

Wireless Network Classification (2)

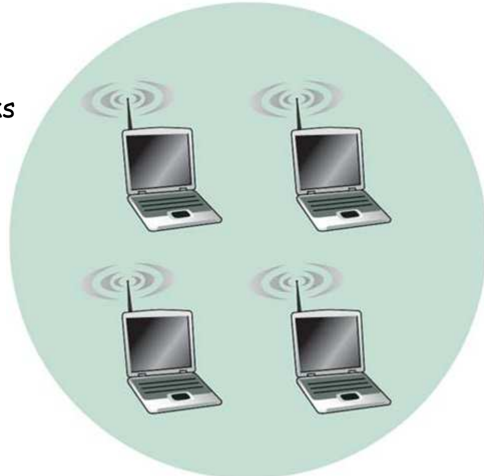
- Infrastructure-based Networks
- Infrastructure-less (Ad hoc) Networks
- Hybrid Networks

Infrastructure-based Networks



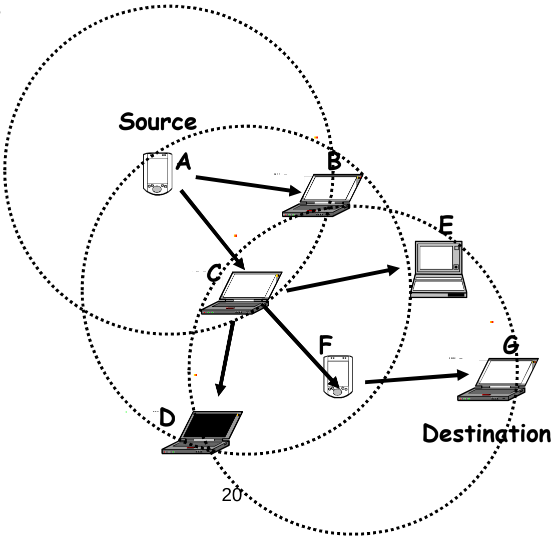
Infrastructure-less (Ad Hoc) Networks

- No fixed infrastructure
  - All links are wireless
  - Also called ad hoc networks
- Nodes
  - Static
  - Mobile
- Dynamic Configuration
  - Join and Leave
  - Mobility
  - Limited Energy



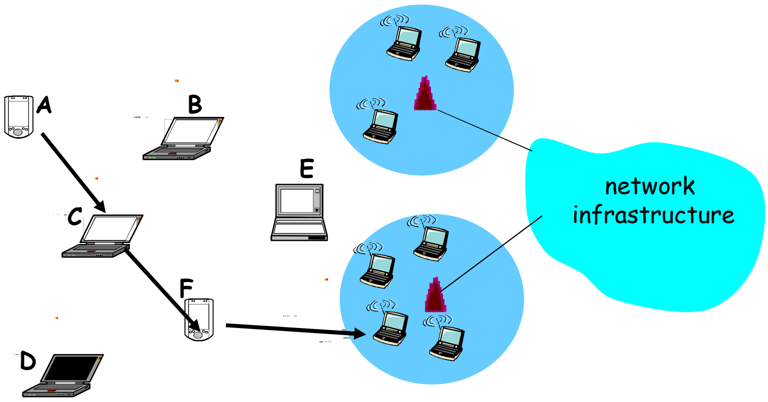
Multi-hop Ad Hoc Networks

- **Multi-hop Communication**
  - Intermediate nodes act as routers
  - Appropriate routing protocols needed
- **Delivery may fail due to**
  - Node Movements/Failures
  - Selfish nodes
- **Peer-to-peer**
  - Nodes may be client and server at the same time



20

Hybrid Networks



Wireless Network Taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	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 nets, sensor nets*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Roadmap

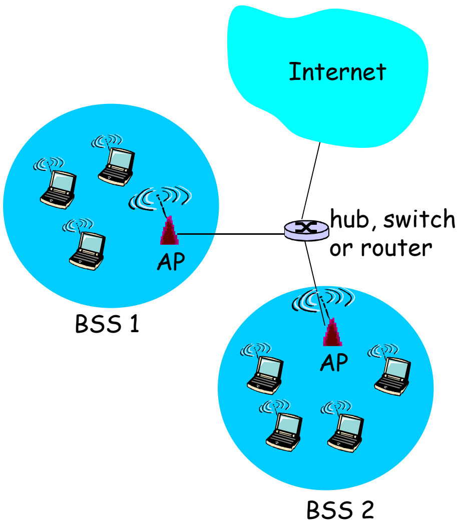
- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks

IEEE 802.11 Wireless LAN

- 802.11b
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
- 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- 802.11n: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

802.11 LAN architecture

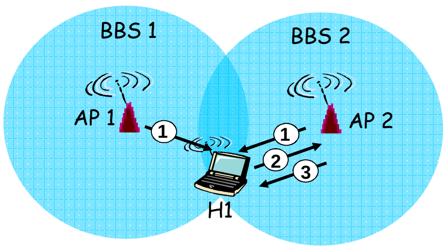


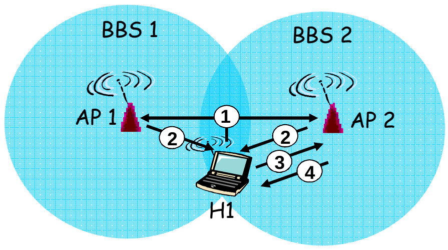
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication
  - will typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning



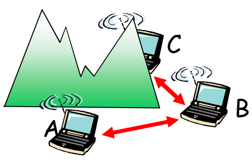


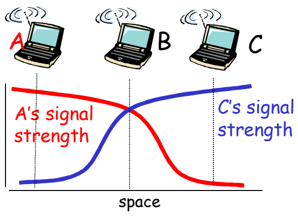
Passive Scanning:
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP (AP2)
(3) association Response frame sent: selected AP (AP2) to H1

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 (AP2)
(4) Association Response frame sent: selected AP (AP2) to H1

IEEE 802.11 MAC Protocol

- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult sense collisions when transmitting
    - Single antenna
    - Collisions occur at the receiver while sensing is at the transmitter
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





CSMA/CA Algorithm

802.11 sender

1 if sense channel idle for **DIFS** then

transmit entire frame (no Collision Detection)

2 if sense channel busy then

start random backoff time

timer counts down while channel idle

transmit when timer expires

if no ACK, increase random backoff interval, repeat 2

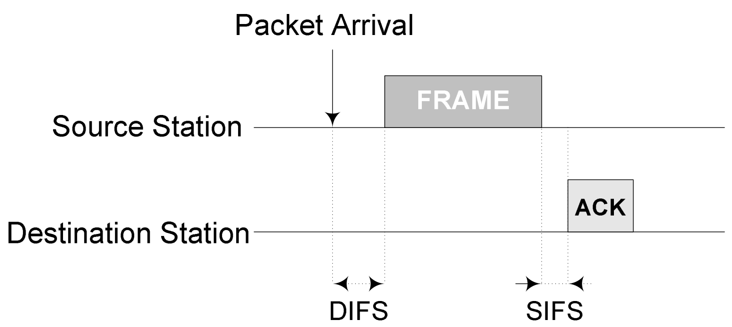
802.11 receiver

- if frame received OK

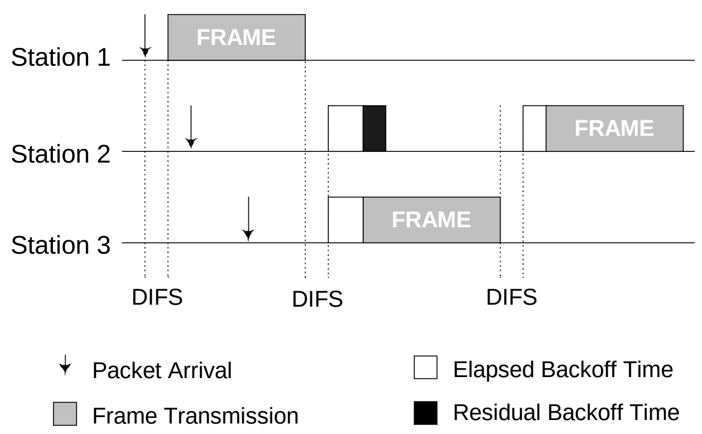
return ACK after **SIFS** (ACK needed due to hidden terminal problem)

CSMA/CA Algorithm

- ARQ Scheme
  - ACK required for both channel errors and collisions



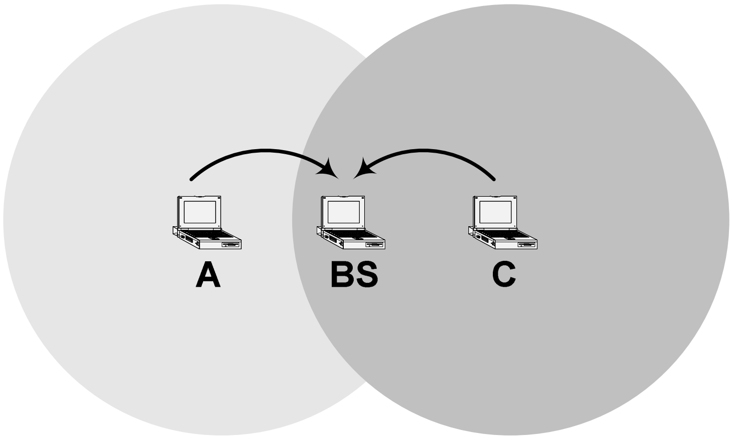
CSMA/CA Algorithm



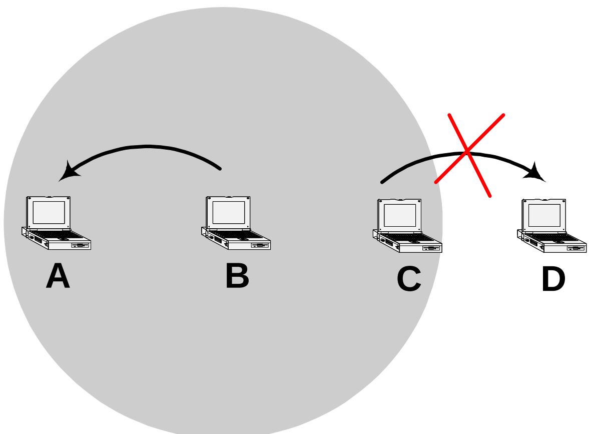
Backoff Algorithm

- Backoff interval
  - a slotted random time with uniform distribution in [0, CW-1]
- Contention Window (CW)
  - Initially, CW=Cwmin
  - While missed ACK, CW=2*CW
  - Until CW=CWmax
- CWmin e CWmax are MAC parameters depending on the physical layer

Hidden Node Problem



Exposed Node Problem



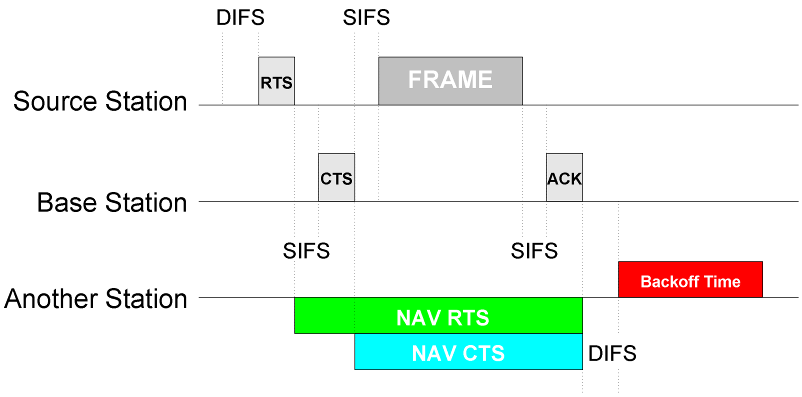
Virtual Carrier Sensing

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely using small reservation packets!

Virtual Carrier Sensing



Definitions

- Transmission Range (TX_Range)
  - range within which a transmitted frame can be **successfully received**
  - determined by the transmission power and the radio propagation properties
- Carrier Sensing Range (CS_Range)
  - range within which another stations **senses** a transmission
  - depends on the sensitivity of the receiver (the receive threshold) and the radio propagation properties
- Interference Range (IF_range)
  - range within which stations in receive mode will be **interfered with** by a transmitter, and thus suffer a loss.
  - usually larger than the transmission range
  - depends on the distance between the sender and receiver, and the path loss model.

Is RTS/CTS Really Effective?

- It assumes that

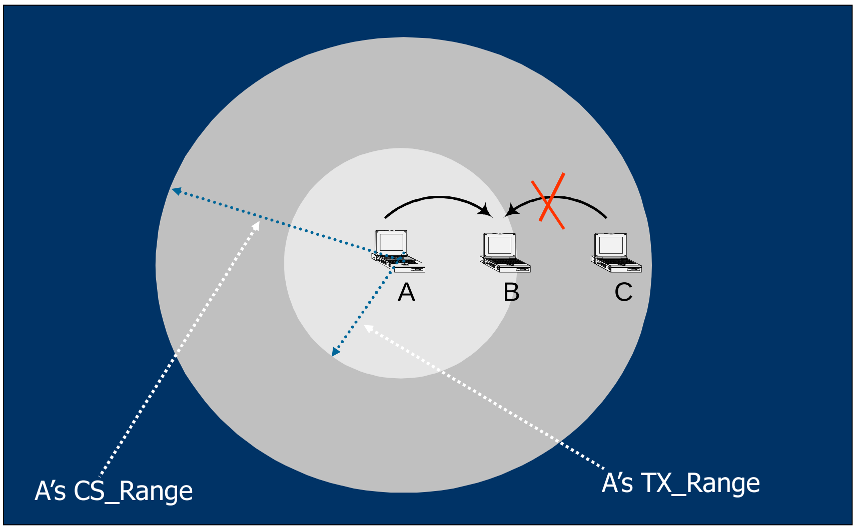
  CS_Range = TX_Range

- In practice

  CS_Range > 2*TX_Range

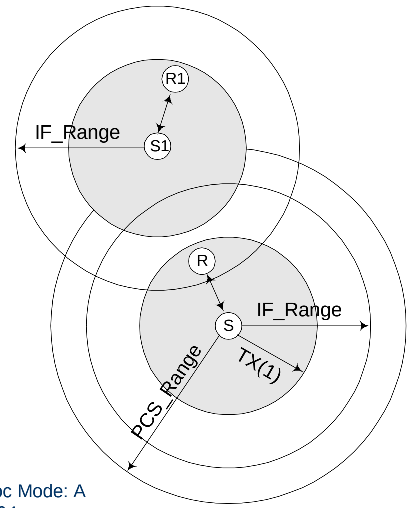
- The Hidden Node problem never occurs
  - In the form described above
- The RTS/CTS is useless
  - Only introduces overhead

Is RTS/CTS Really Effective?



Hidden Node Problem in Reality

- S and S1 are hidden to each other
- R is inside the IF_Range of S1
- S and S1 transmit simultaneously ➔ collision at R
- RTS/CTS does not provide any help



G. Anastasi, E. Borgia, M. Conti, E. Gregori, "Wi-Fi in Ad Hoc Mode: A Measurement Study", Proceedings of the *IEEE PerCom 2004,* Orlando (Florida), March 14-17, 2004.

802.11 Frame: Addressing

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

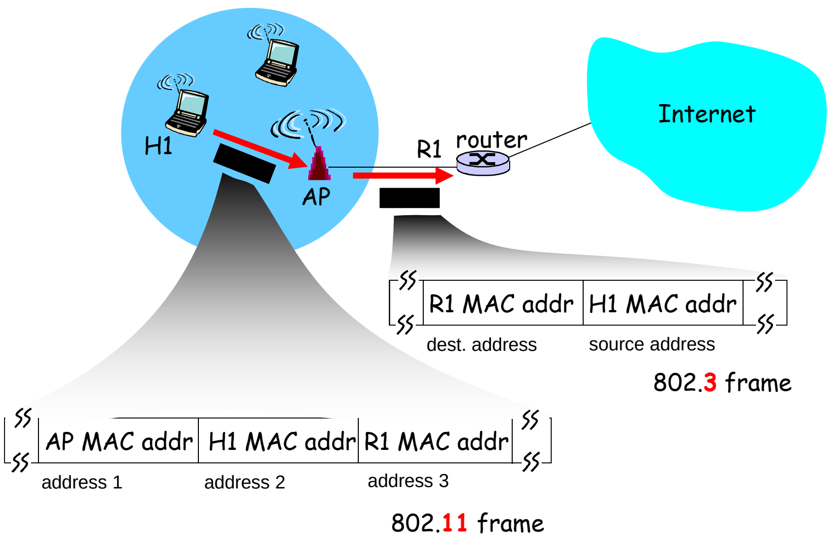
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

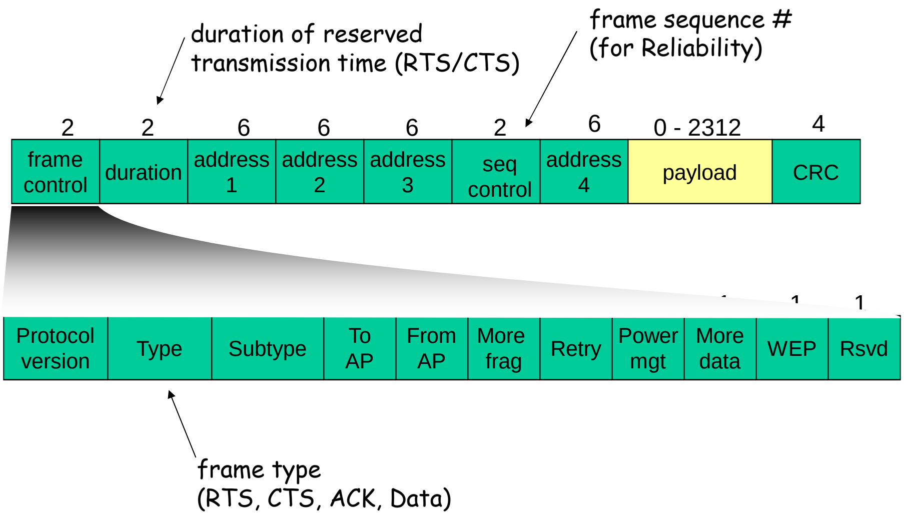
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 Frame: Addressing

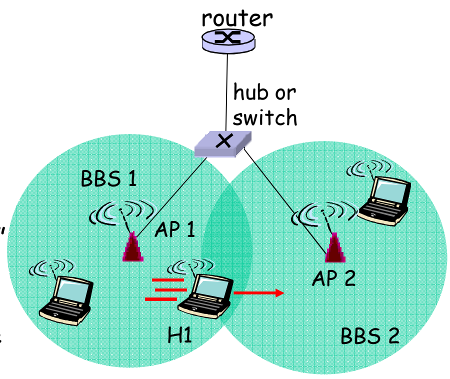


802.11 Frame: Other Fields



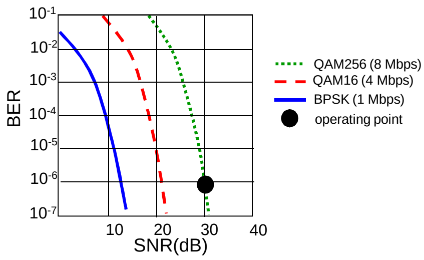
Mobility within Same Subnet

- H1 remains in same IP subnet
  - IP address can remain the same
- switch: which AP is associated with H1?
  - self-learning: switch will see frame from H1 and "remember" which switch port can be used to reach H1
    - AP2 can send a broadcast message after re-association
  - 802.11f is developing inter-AP protocol for mobility handling



Rate Adaptation

- As mobile moves, SNR varies
- base station or mobile node dynamically change transmission rate
  - physical layer modulation technique



1. As node moves away from base station SNR decreases and BER increases

2. When BER becomes too high, switch to lower transmission rate but with lower BER

Power Management

- Mobile Nodes have limited energy budget
  - The wifi card account for a significant energy consumption (up to 50% in palmtop computers)

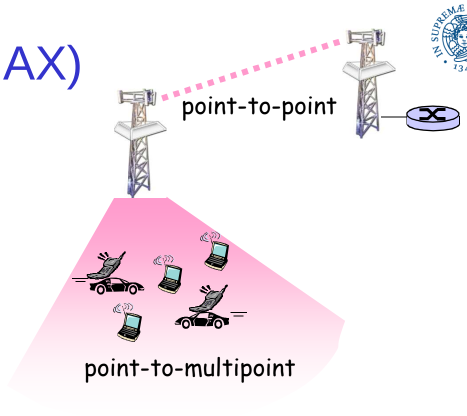
- 802.11 Power Management
  - Based on periodic Beacon frames
    - Emitted by AP every 100 ms
    - Beacons include clock information for synch
  - Allow to save up to 90% of energy
  - Limited impact on performance

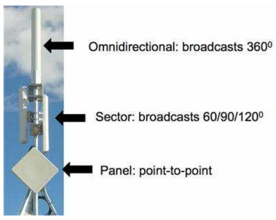
Power Management

- node-to-AP:
  - "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- AP-to-node
  - Beacons include the list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

IEEE 802.16 (WiMAX)

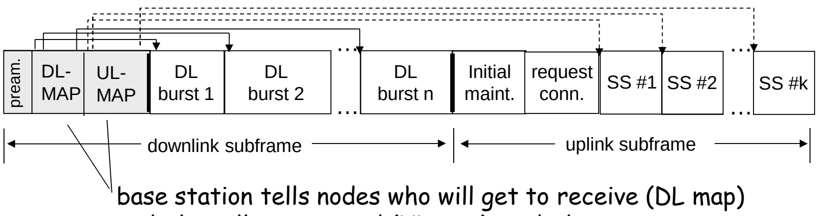
- Infrastructure based
  - transmissions to/from base station by hosts with omnidirectional antenna
  - base station-to-base station backhaul with point-to-point antenna
- unlike 802.11:
  - range ~ 10 Km ("city rather than coffee shop")
  - ~14 Mbps





WiMAX: Downlink/Uplink Scheduling

- Time Division Duplex (TDD)
  - down-link subframe: base station to node
  - uplink subframe: node to base station



base station tells nodes who will get to receive (DL map) and who will get to send (UL map), and when

- WiMAX standard provide mechanism for scheduling, but not scheduling algorithm

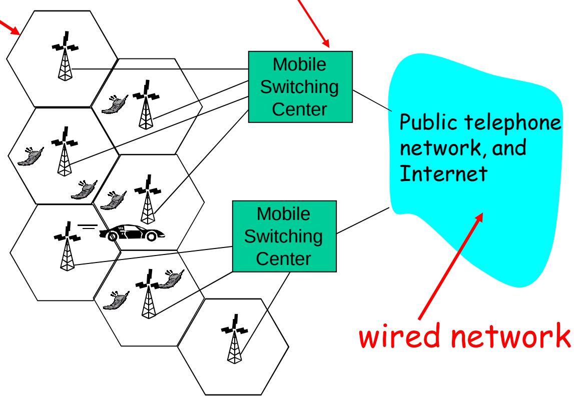
Roadmap

- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks

Cellular Network Architecture

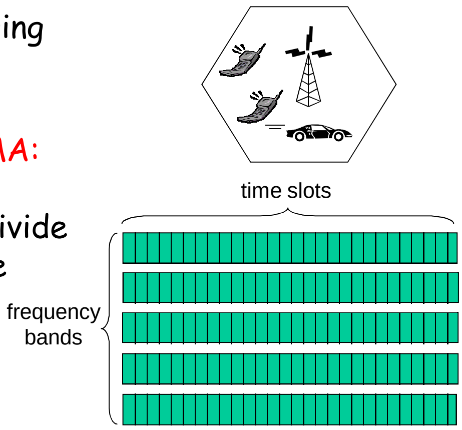
MSC
- connects cells to wide area net
- manages call setup
- handles mobility

cell
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS



Cellular Networks: the First Hop

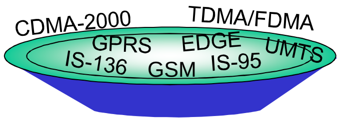
Two techniques for sharing mobile-to-BS radio spectrum
- combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots
- CDMA: code division multiple access



Cellular Standards: Brief Survey

2G systems: voice channels

- GSM (Global System for Mobile Communications): combined FDMA/TDMA
  - most widely deployed
  - Speech coded at 13 kbps
- IS-136 TDMA: combined FDMA/TDMA (North America)
- IS-95 CDMA: code division multiple access



Don't drown in a bowl
of alphabet soup: use this
for reference only

Cellular Standards: Brief Survey

2.5 G systems: voice and data channels

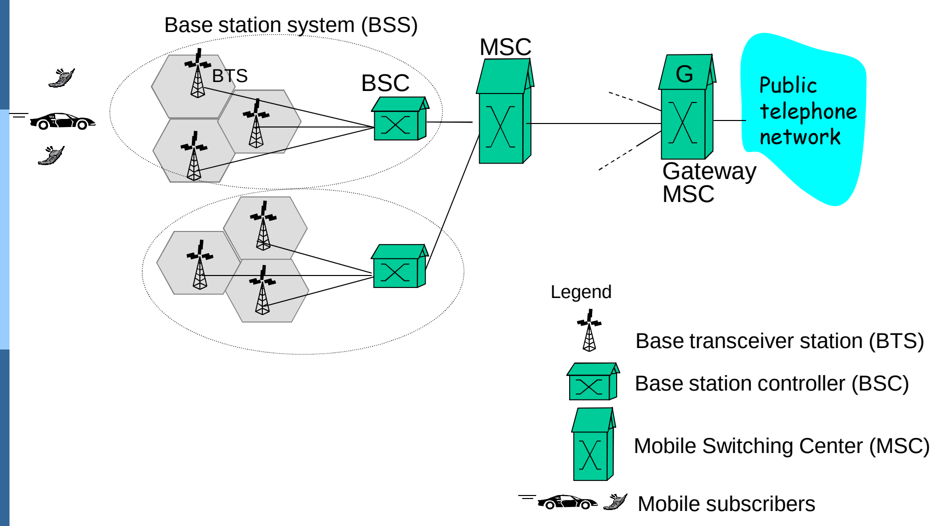
- for those who can't wait for 3G service: 2G extensions
- General Packet Radio Service (GPRS)
  - evolved from GSM
  - data sent on multiple channels (if available)
  - data rates up to 115 Kbps
- Enhanced Data Rates for Global Evolution (EDGE)
  - also evolved from GSM, using enhanced modulation
  - data rates up to 144 K (driving), 384 K (outdoor), 2M (indoor)
- CDMA-2000 (phase 1)
  - evolved from IS-95
  - data rates up to 144Kbps

Cellular Standards: Brief Survey

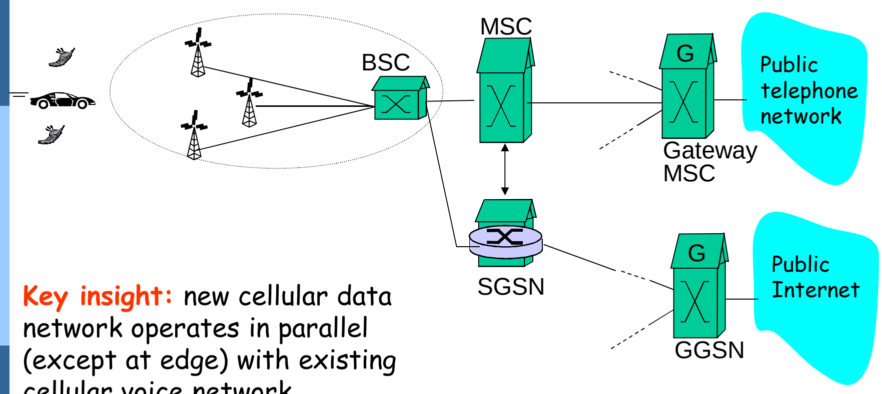
3G systems: voice/data/video

- Universal Mobile Telecommunications Service (UMTS)
  - data service: High Speed Uplink/Downlink Packet Access (HSDPA/HSUPA): 3 Mbps
- CDMA-2000: CDMA in TDMA slots
  - data service: 1xEvolution Data Optimized (1xEVDO) up to 14 Mbps

GSM Network Architecture

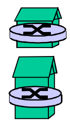


GSM/GPRS network architecture



Key insight: new cellular data network operates in parallel (except at edge) with existing cellular voice network

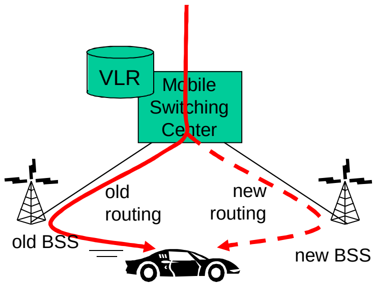
- voice network unchanged in core
- data network operates in parallel



Handling Mobility in Cellular Networks

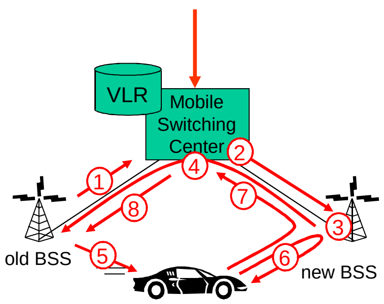
- **Home network:** network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
- **Home location register (HLR):** database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)
- **Visited network:** network in which mobile currently resides
  - could be home network
- **Visitor location register (VLR):** database with entry for each user currently in network

GSM Handoff with Common MSC



- Handoff goal:
  - route call via new base station (without interruption)
- Reasons for handoff:
  - stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - load balance: free up channel in current BSS
  - GSM doesn't mandate why to perform handoff (policy), only how (mechanism)
- Handoff initiated by old BSS

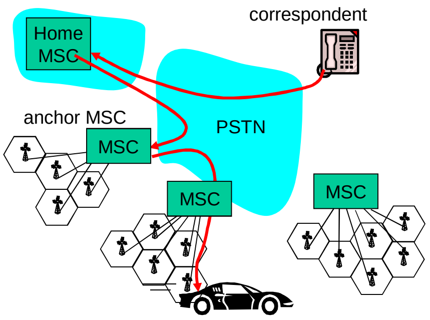
GSM Handoff with Common MSC



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

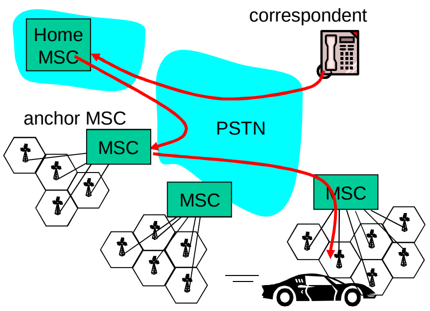
GSM Handoff between MSCs



(a) before handoff

- 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

GSM Handoff between MSCs



(b) after handoff

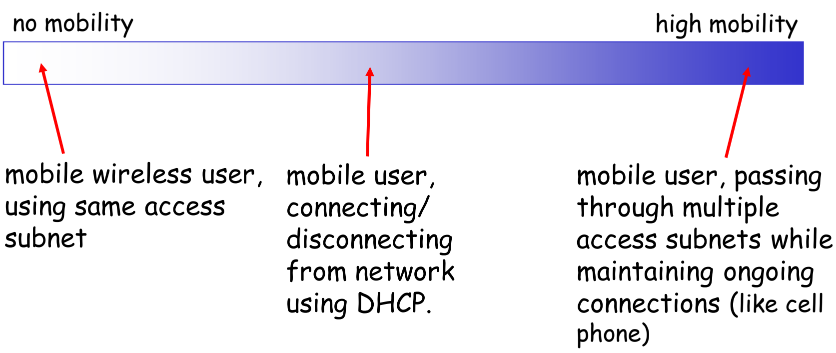
- anchor MSC: first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC

Roadmap

- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks

What is Mobility?

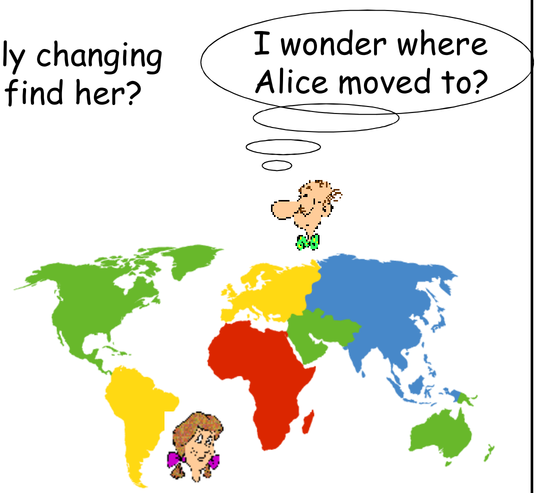
- Spectrum of mobility, from the Internet perspective:



How to Handle Mobility?

Consider friend frequently changing addresses, how do you find her?

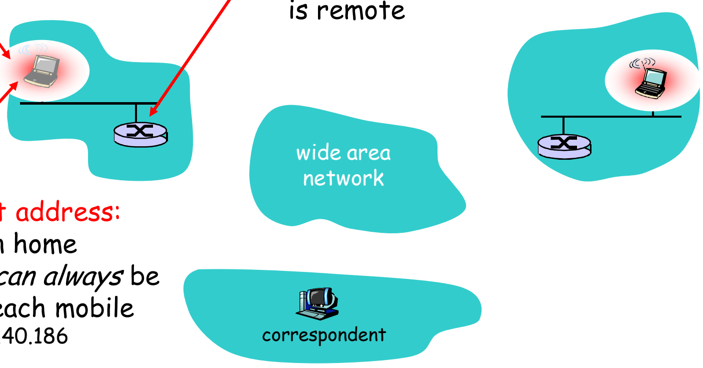
- search all phone books?
- expect her to let you know where he/she is?
- call her parents?



Mobility: Addressing

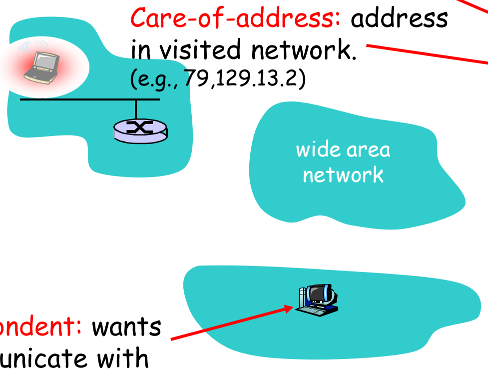
home network: permanent "home" of mobile
(e.g., 128.119.40/24)

home agent: entity that will perform mobility functions on behalf of mobile, when mobile is remote



Permanent address: address in home network, *can always* be used to reach mobile
e.g., 128.119.40.186

Mobility: Addressing



Routing to a Mobile Node

- Let routing handle it: routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- Let end-systems handle it:
  - indirect routing: communication from correspondent to mobile goes through home agent, then forwarded to remote
  - direct routing: correspondent gets foreign address of mobile, sends directly to mobile

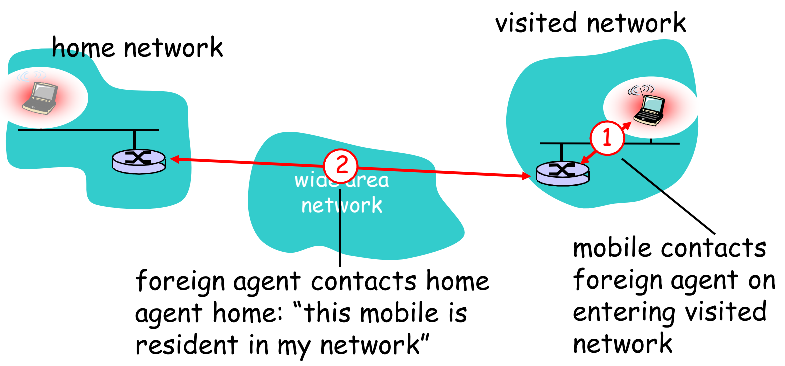
Routing to a Mobile Node

- Let routing handle it ... ters advertise permanent address of mobi... residence via usual routing table e...
  - routing table ... ere each mobile located
  - no changes to e... ems

not scalable to millions of mobiles

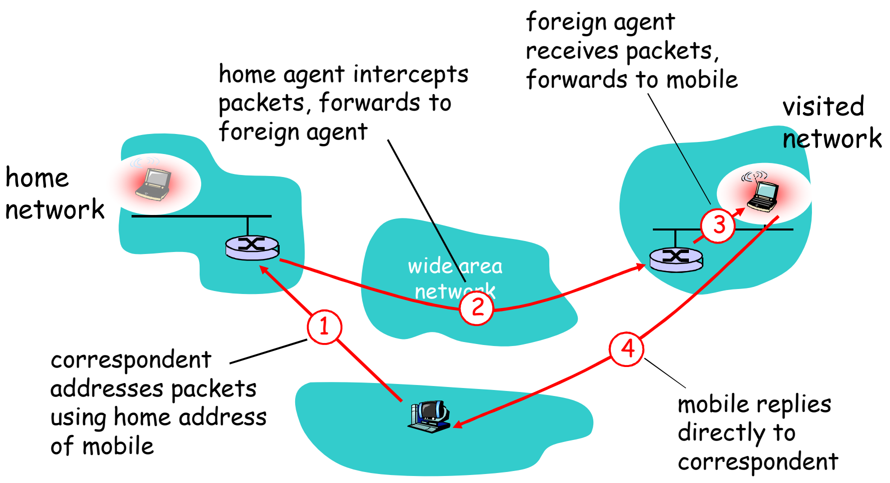
- Let end-systems handle it:
  - indirect routing: communication from correspondent to mobile goes through home agent, then forwarded to remote
  - direct routing: correspondent gets foreign address of mobile, sends directly to mobile

Mobility: Registration



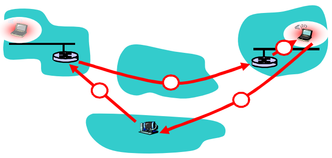
End result:
- Foreign agent knows about mobile
- Home agent knows location of mobile

Indirect Routing



Indirect Routing: Comments

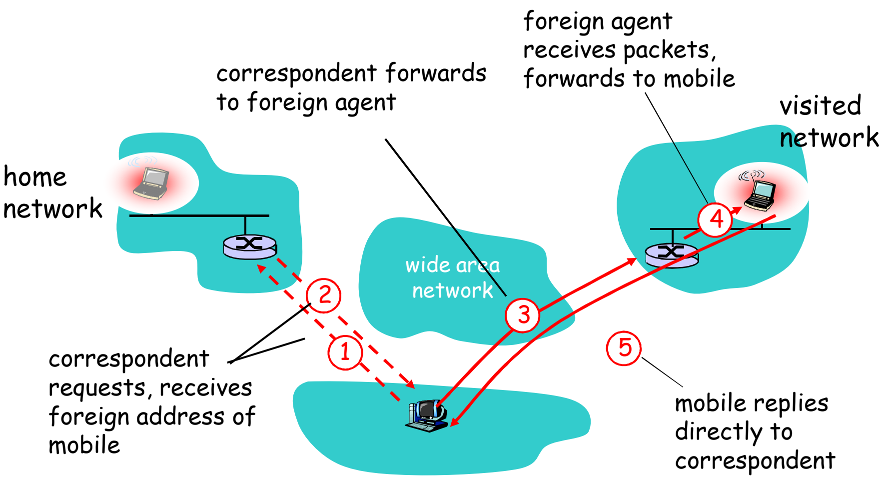
- Mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network



Indirect Routing: Moving between Networks

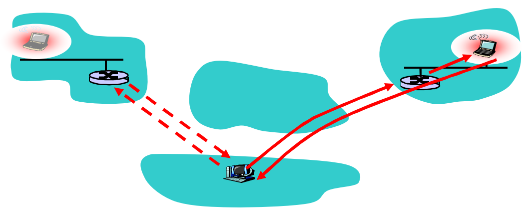
- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: *on going connections can be maintained!*

Direct Routing



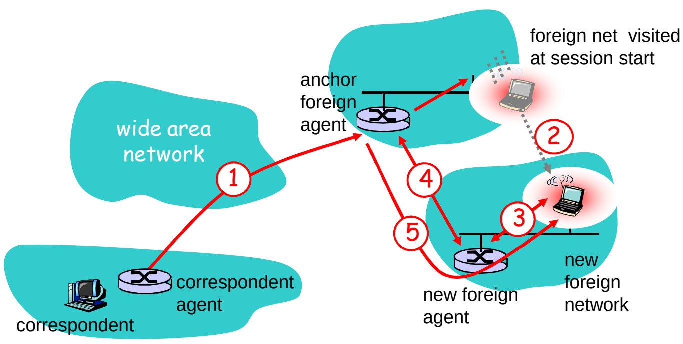
Direct Routing: Comments

- overcome triangle routing problem
- non-transparent to correspondent: correspondent must get care-of-address from home agent
  - what if mobile changes visited network?



Accommodating mobility with direct routing

- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)



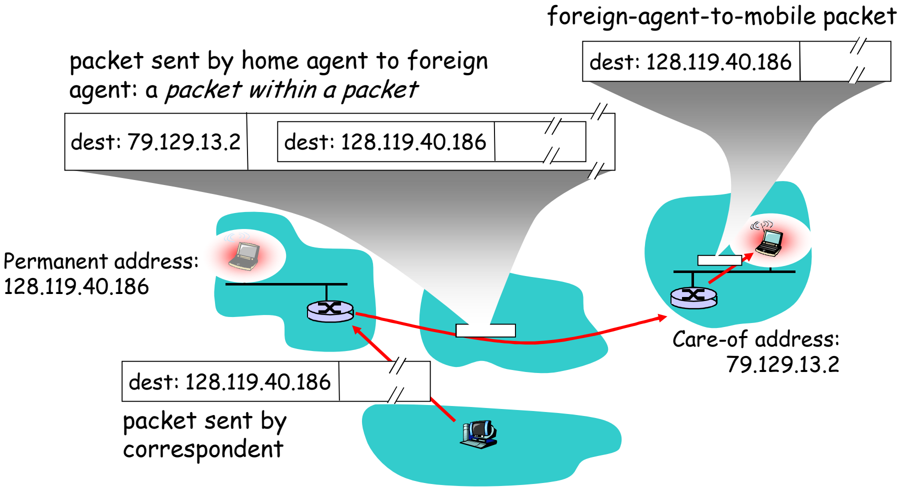
Roadmap

- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks

Mobile IP

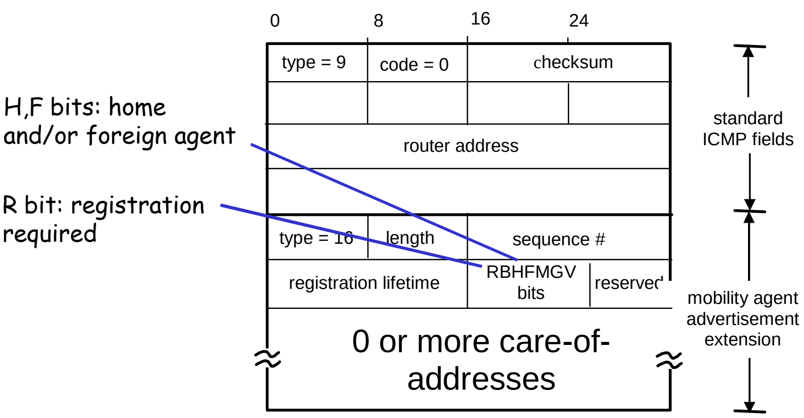
- RFC 3344
- has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- three main components:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent

Mobile IP: Indirect Routing



Mobile IP: Agent Discovery

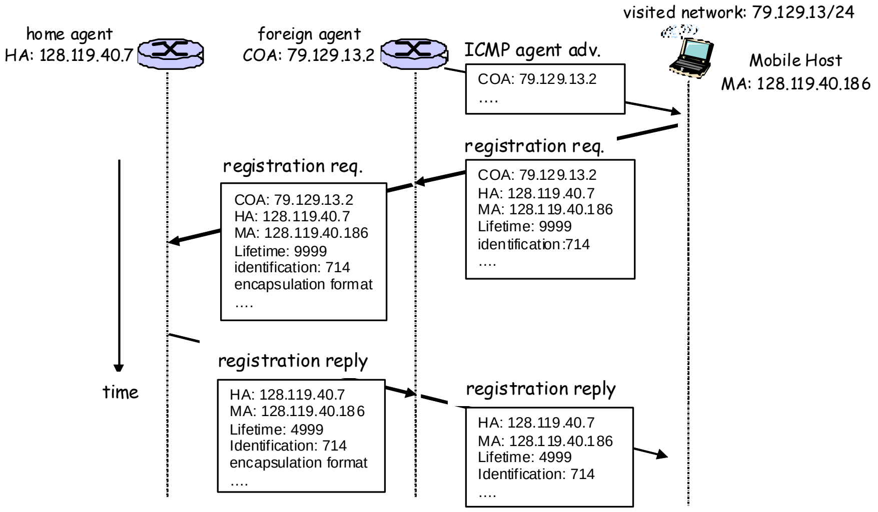
- agent advertisement: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)



Mobile IP: Registration

- Once MN has received a COA from FA, that address must be registered with HA
- Registration is a 4-step process
  - Registration request from MN to FA
    - Includes registration lifetime
  - Registration request forwarded by FA to HA
  - Registration reply from HA to FA
    - Includes actual registration lifetime (may be less than the required registration lifetime)
  - Registration reply forwarded to MN
- Requests/Replies sent as UDP datagram to/from port 434

Mobile IP: Registration Example



Roadmap

- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks

Impact on Higher Layer Protocols

- logically, impact *should* be minimal …
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- … but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handoff
  - TCP misinterprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic
  - limited bandwidth of wireless links
  - Limited storage of portable device

TPC Extensions for Wireless/Mobile

- Local Recovery
  - 802.11 ARQ
  - FEC
- TCP sender modifications
  - Distinction between losses due to channel errors and congestion
- Split connection
  - Convetional TCP connection over the wired network
  - Customized transport connection over the wireless link

Mobility is not necessarily an issue

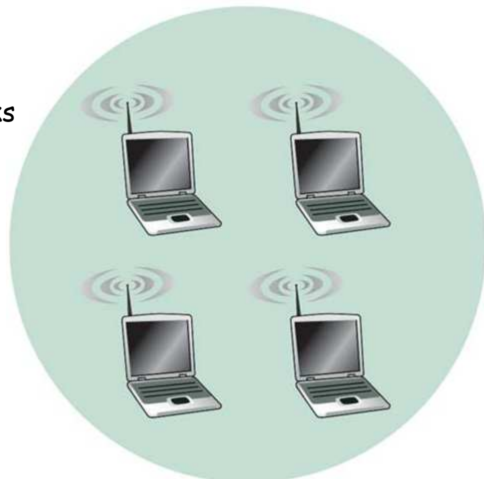
- Location-based applications
- Context-aware applications

Roadmap

- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks

Infrastructure-less (Ad Hoc) Networks

- No fixed infrastructure
  - All links are wireless
  - Also called ad hoc networks
- Nodes
  - Static
  - Mobile
- Dynamic Configuration
  - Join and Leave
  - Mobility
  - Limited Energy

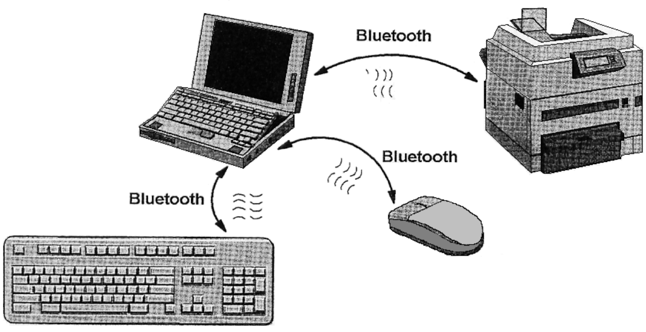


WPAN Bluetooth (IEEE 802.15.1)

- Short range radio at 2.4 GHz
  - Available globally for unlincensed users
  - Low-power
  - Low-cost
  - Cable replacement
  - Devices within 10m can share up to 700 Kbps (1 Mbps nominal)
  - Universal short-range wireless capability

Application areas

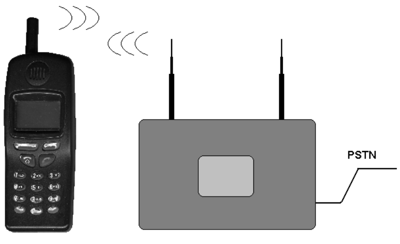
- Cable replacement
  - No need for numerous cable attachments
  - Automatic synchronization when devices within range



Application Areas

Wireless Voice Transmission

- Cordless headset
- Three-in-one phones
  - cellular, cordless, walkie-talkie



Other Application Areas

Ad hoc networking

- Can establish connections between devices in range
- Devices can imprint on each other so that authentication is not required for each instance of communication
- Support for object exchange
  - Files
  - Calendar entries
  - Business cards
  - …

Bluetooth Piconet

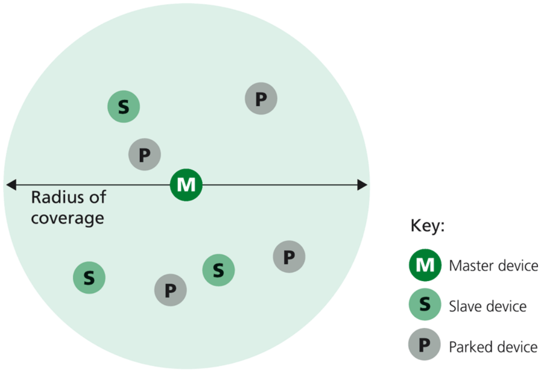
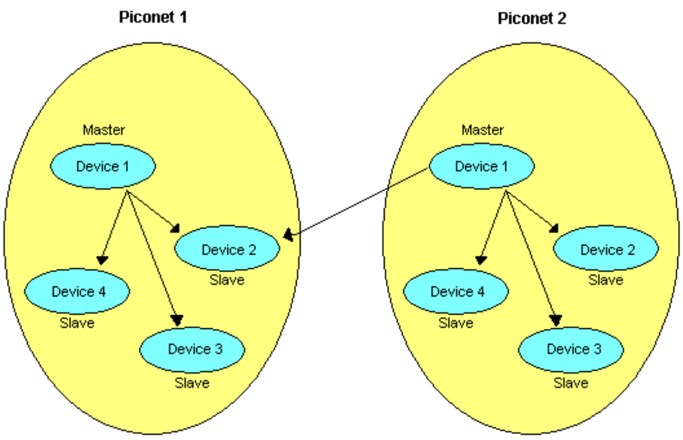
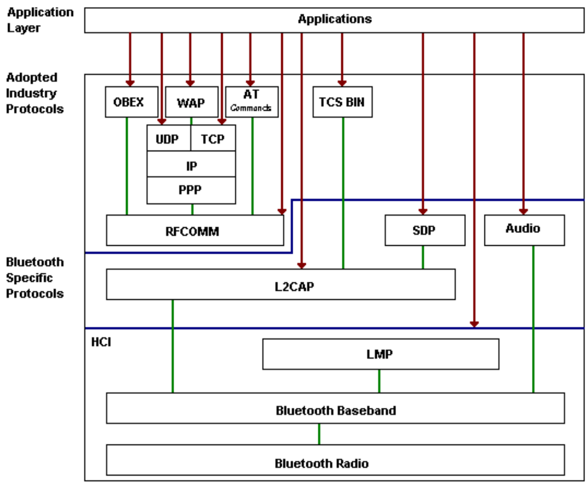


Figure 6.14 ♦ An 802.15 piconet

Piconet e Scatternet



Bluetooth Architecture



95

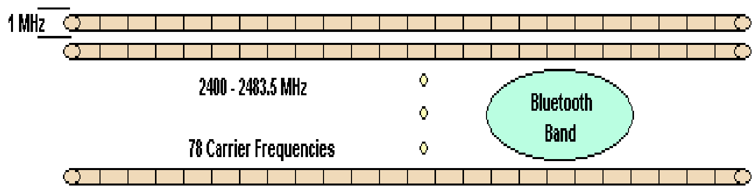
Bluetooth Architecture

Bluetooth protocols are organized into three levels

- Bluetooth-specific protocols
- Adopted industry protocols
  - Existing protocols included in the Bluetooth protocol stack
    - TCP/IP, PPP, WAP, ObEX
  - Allows Bluetooth to be used transparently in legacy application
- Applications

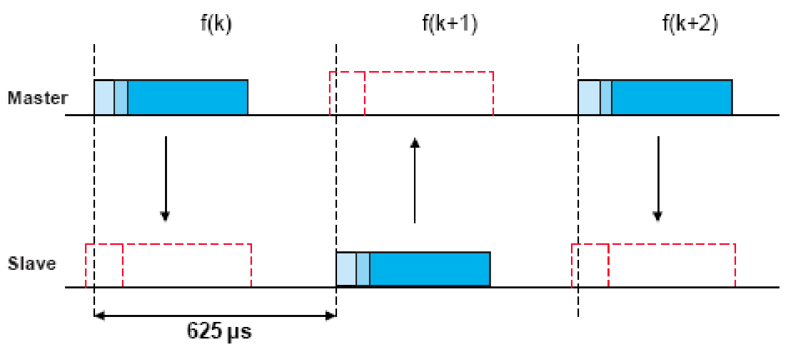
96

Frequency bandwidth



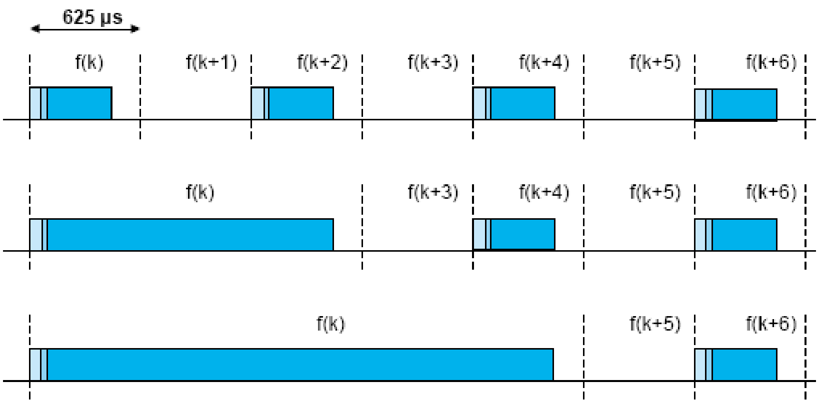
97

TDD and Timing

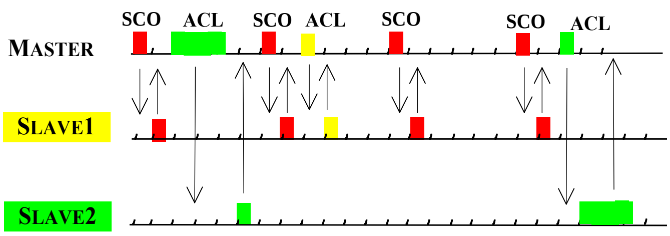


98

Multi-slot Packets



Connection types



Operation Modes

- Active Mode
  - The device is continuously active
  - No more than 7 active device at a time within a piconet
  - Each node is assigned a 3-bit Active Member Address (AMA)
- Sniff mode
  - Used to reduce energy consumption in devices that are only sporadically active
  - The device does not hear all odd slots
  - It is usually sleeping and wakes up once in a while
  - The device holds the 3-bit address
- Hold mode
  - The device is not able to receive ACL packets for a pre-negotiated time interval
  - It holds the 3-bit address

101

Operation Modes

- Park mode
  - The device must release the 3-bit address to the master
  - It remains however synchronized to the master
    - Wakes up periodically to get Hopping Synchronization Packets containing the master clock and its frequency hopping sequence
  - Only the device clock is running
    - Energy saving mode
  - In addition to 7 active slaves in the piconet there may be up to 255 parked devices
    - If there already 7 active slaves a parked device must wait until one of the active members switches to the parked mode

102

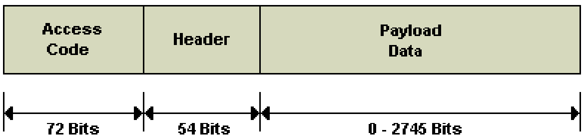
MAC protocol

Polling scheme

- The master has the full control of the channel
  - slaves' transmissions are scheduled by the master
- Whenever a slave receives a packet from the master it is allowed to send a packet in the next set of 1, 3 or 5 slots
- If the slave has no data to send it replies with a NULL packet (no payload)
- If the master has no data to send uses a POLL packet to enable a slave to transmit in the next odd slot

103

Packet format



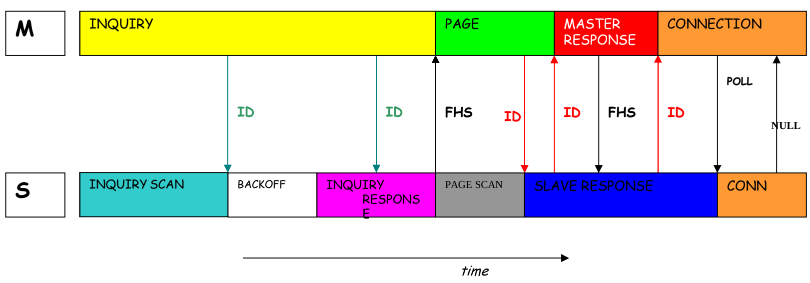
- Access code
  - Channel Access Code: used to identify the piconet
  - Device Access Code: used by the master to page the slave
  - Inquiry Access Code: used to find the address of a neighbor device
- Header
  - AM Address (3 bits) : identifies one of the 7 active stations (0: master)
  - Type (4 bits) : indicates the type/contents in the payload
  - Flow (1 bit): used for flow control in ACL mode (stop=0, resume=1)
  - ARQN (1 bit): indicates the type of acknowledgement (ACK=1, NACK=0)
  - SEQN (1 bit): modulo-2 sequence number
  - HEC (8 bits): Header Error Correction (1/3 forward error correcting code)
- Payload
  - 0-343 bytes which include an additional 1- or 2-byte header and a 2-byte CRC

104

Packet types

- SCO packets
  - Data packets used in SCO connections
- ACL packets
  - Data packets used in ACL connections
- Poll packets
  - Control packets used by the master to poll slaves
- Acknowledgement packets
  - ACK and NACK
- Frequency Hopping Synchronization (FHS) packets
  - Control packets send by the master to a slave to enable it to synchronize to the clock of the master and its hopping sequence

Connection set-up



Service Discovery

- A BT device is able to provide services to other BT devices
- A BT device must monitor which service are currently available
  - The set of available service may be dynamic as BT devices join and leave the piconet
- The service discovery protocol (SDP) is used to
  - Find new service as soon as they become available
  - Deregister services that become unavailable

107

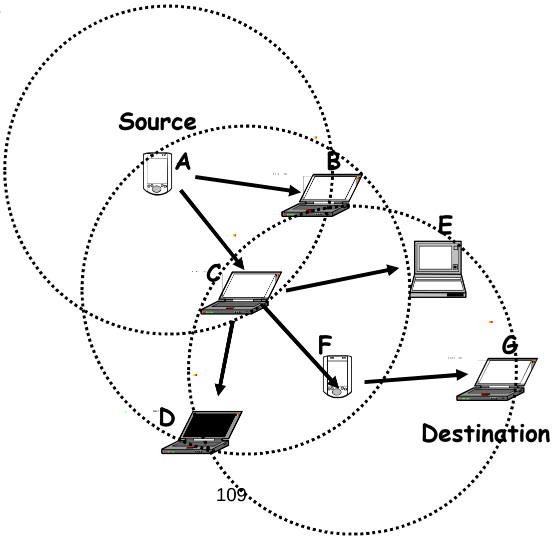
Scenario Steps

- Master device (e.g., BT phone) pages for nearby devices
- Receives responses from 0,1, or more devices
  - Slave device (e.g., headphone) responds to page
- establishes the BT connection
  - Assigning paging device to be master
  - The two devices synchronize their frequency hopping
- and negotiates connection parameters
  - Authentication is part of this phase
- Devices exchange profiles they both support
- Agree upon profile (e.g., audio streaming)
- Master sends audio data
  - Keep-alive packets used to maintain connection

108

Multi-hop Ad Hoc Networks (MANETs)

- **Multi-hop Communication**
  - Intermediate nodes act as routers
  - Appropriate routing protocols needed
- **Delivery may fail due to**
  - Node Movements/Failures
  - Selfish nodes
- **Peer-to-peer**
  - Nodes may be client and server at the same time



Routing Protocols

Ad Hoc Mobile Unicast Routing Protocol

Proactive (Table Driven)

si calcolano tutti i possibili percorsi indipendentemente dal loro uso effettivo e si memorizzano nelle tabelle di routing (e.g DSVD, OLSR, FSR, HSLS)

- Alto Overhead di controllo;
- No delay

Hybrid

racchiudono caratteristiche dei protocolli PROACTIVE e REACTIVE (e.g ZRP)

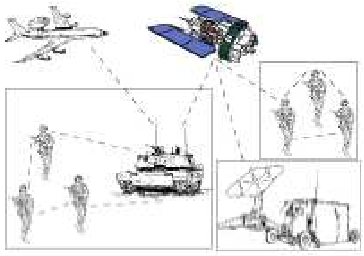
Reactive (On Demand)

si calcolano i percorsi soltanto quando è strettamente necessario, cioè al momento di una trasmissione (e.g DSR, AODV)

- Overhead di controllo contenuto
- Delay elevato per percorsi non disponibili

MANET Application Areas

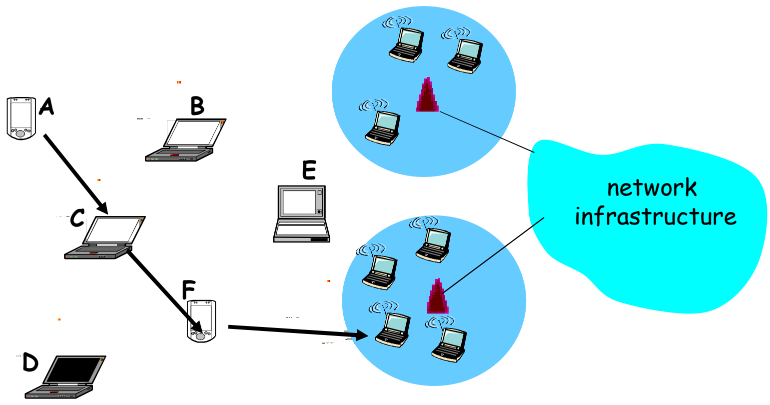
- Civil Protection
- Vehicular Ad Hoc Networks (VANETs)
- Robotic Networks
- Battlefield Communications



Roadmap

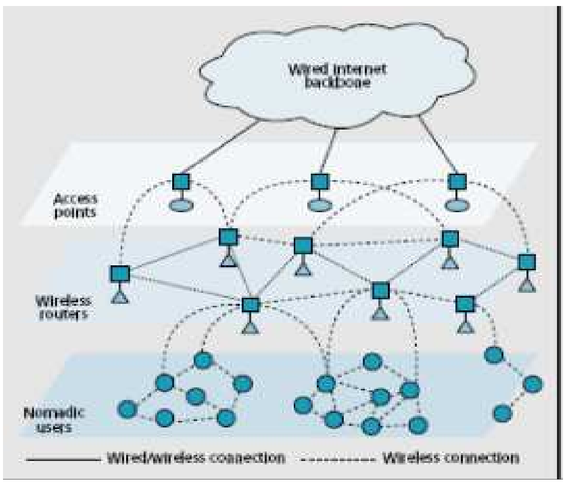
- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks

Hybrid Networks



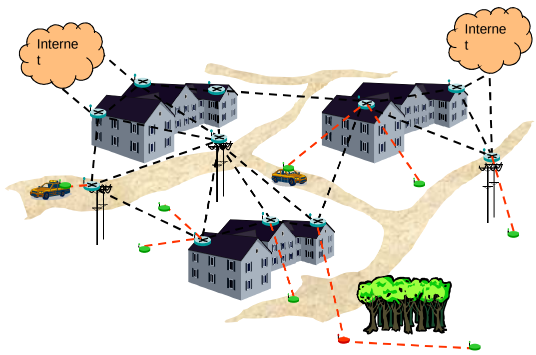
113

Mesh Networks



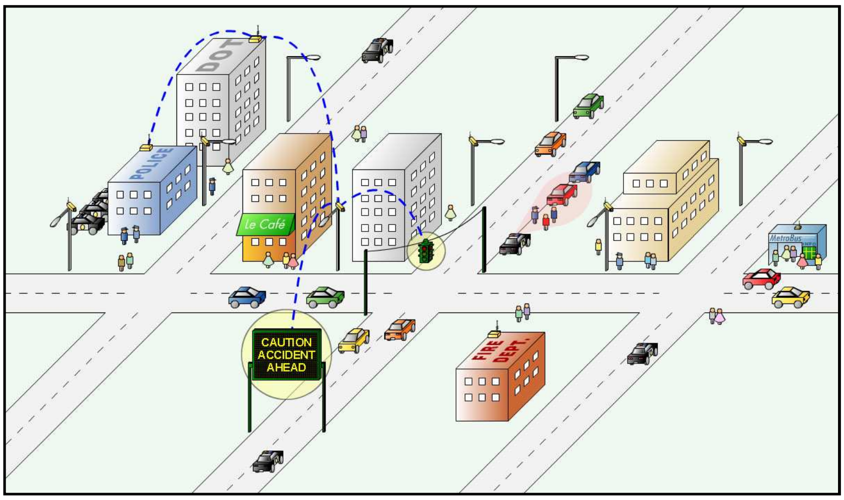
Mesh Networks: Applications

Residential Broadband Internet Access



Mesh Networks: Applications

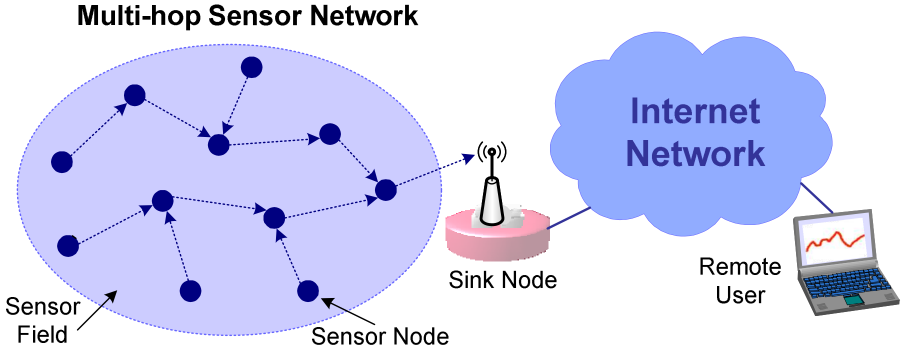
Intelligent Transportation System



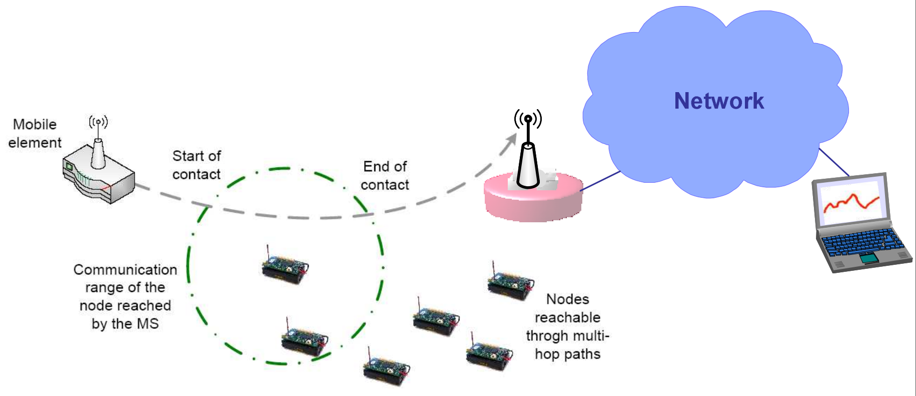
Summary

- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks

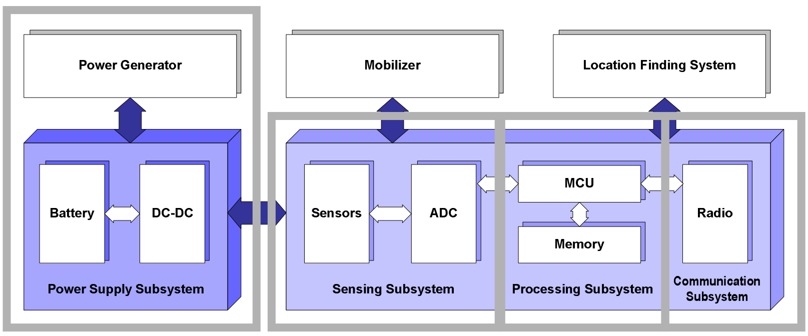
Wireless Sensor Networks



WSN with Mobile Elements



Sensor Node Architecture



Battery powered devices
Batteries cannot be changed nor recharged

Often negligible power consumption

Local data processing and data storage

Short range wireless communication
Radio is the most power hungry component

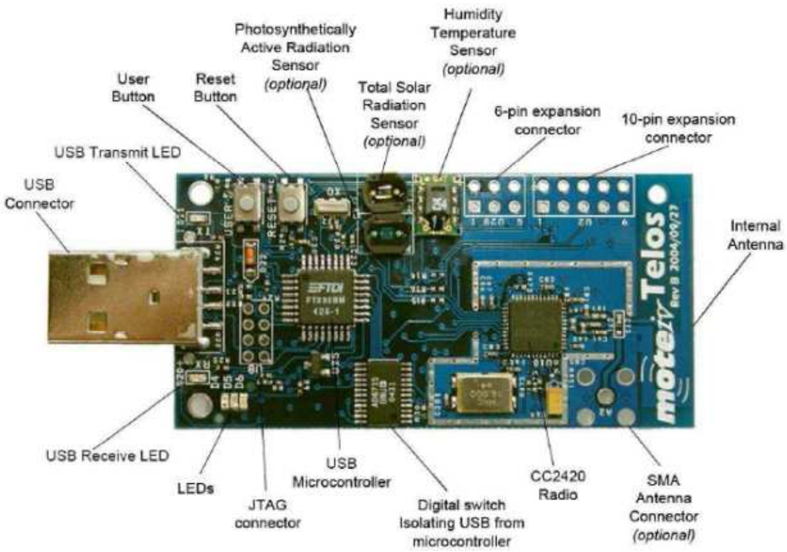
Sensors

- Sensor types
  - seismic
  - magnetic
  - thermal
  - visual
  - infrared
  - acoustic
  - radar…
- Sensor tasks
  - temperature
  - humidity
  - vehicular movement
  - lightning condition
  - pressure
  - soil makeup
  - noise levels
  - mechanical stress levels
  - current characteristics (speed, direction, size) of an object
  - …

Application Areas

- Military Applications
- Environmental Monitoring
- Precision Agriculture
- Health Monitoring
- Intelligent Home
- Info-mobility
- Industrial applications
- …

Telos Mote



The TinyOS Operating System

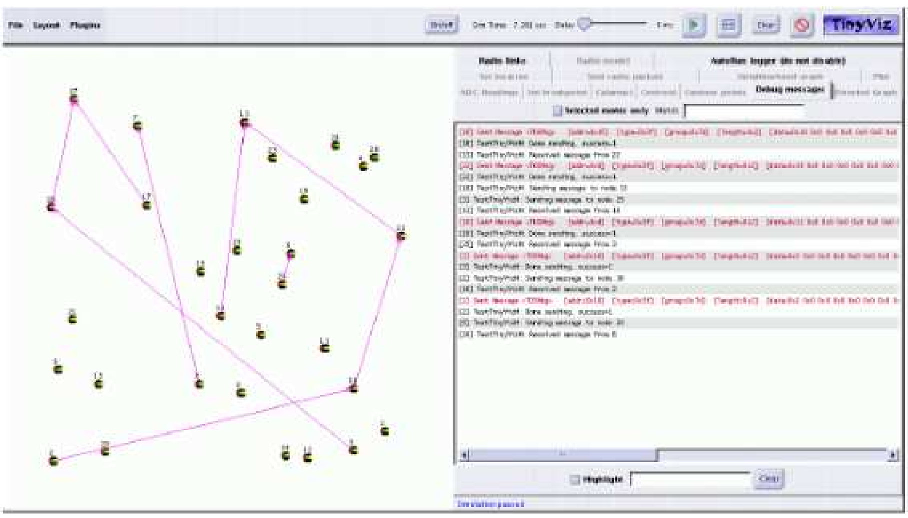
- Specifically targeted to wireless sensor networks
  - a framework an application-specific operating system
  - static memory
  - low system overhead

http://www.tinyos.net/

TinyOS development environment

- nesC language
  - extension to the C language
  - definition of interfaces
  - abstraction between definition and composition of components
- nesC compiler and OS source
  - composition of the component graph (at compilation time)
  - TinyOS computational model (additional checks)
- TOSSIM simulator
  - same code runs in actual nodes and simulator
  - flexible models for radio and sensors
  - scripting (Tython), graphical interface (TinyViz)

TinyViz



Tutorials on Programming Environment

- TinyOS/TOSSIM Tutorial, http://docs.tinyos.net/index.php/TinyOS_Tutorials
- TinyOS Reference Manual, http://www.tinyos.net/tinyos-2.x/doc/pdf/tinyos-programming.pdf
- D. Gay et al., "The nesC Language: A Holistic Approach to Networked Embedded Systems", 2002.
- nesC Reference Manual, http://www.tinyos.net/dist-2.0.0/tinyos-2.0.0beta1/doc/nesc/ref.pdf

Networking Issues

- Application specific
  - protocols should adapt to the application behavior
- Environment interaction
  - The data traffic is expected to be different from human-driven traffic
- Scale
  - The number of sensor nodes can be several orders of magnitude higher than in traditional ad hoc networks
- Energy
  - Sensor nodes are limited in power, computational capabilities, and memory

Networking Issues

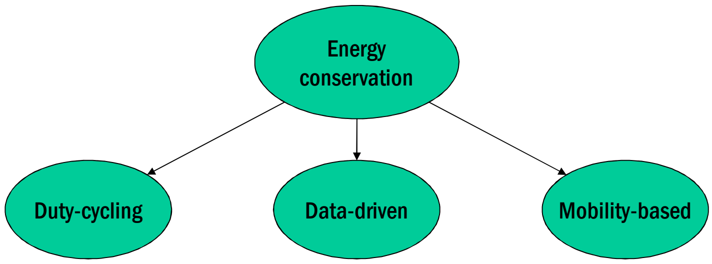
- Dependability
  - sensor nodes prone to failures
  - frequent topology changes (due to failures, energy limitations, mobility)
- Simplicity
  - limited computational resources
- Data-centric approach
  - the importance of a particular node is considerably reduced (due to redundancy)

The Energy Problem

- Energy is the key issue in the WSN design
  - Applications may require a network lifetime in the order of several months or even years
  - If always active, sensor nodes deplete their energy in less than a week
- Possible approaches
  - Low-power sensor nodes
  - Energy harvesting techniques
  - Energy conservation schemes
  - Energy efficient protocols
  - Energy-efficient application design
  - Cross-layering
  - …

Energy Conservation

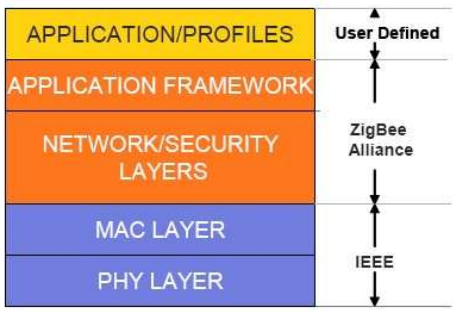
- Goal
  - Use the available energy very efficiently so as to extend the network lifetime to meet the application requirements
- Different approaches
  - targeted mostly to the radio subsystem
  - also solutions to reduce the number of data acquisitions (sensor's energy management)



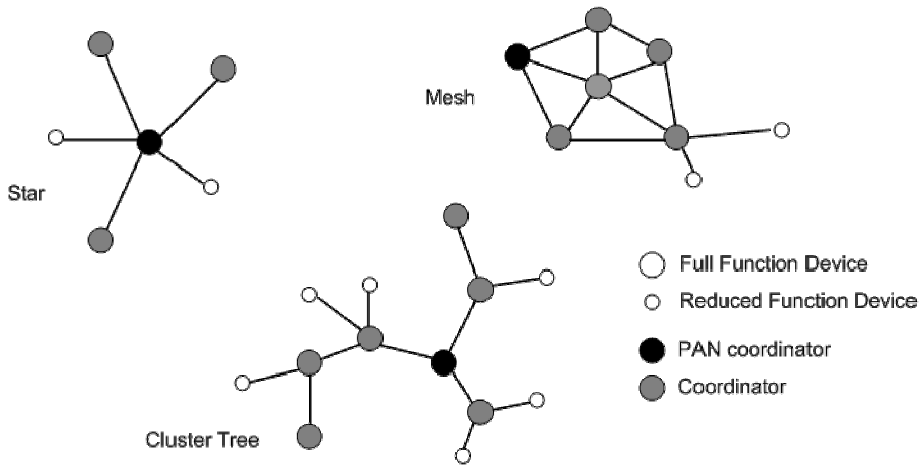
G. Anastasi, M. Conti, M. Di Francesco, A. Passarella, **Energy Conservation in Wireless Sensor Networks: A Survey**, *Ad Hoc Networks*, Vol. 7, N. 3, May 2009. Elsevier.

IEEE 802.15.4 and ZigBee

- IEEE 802.15.4 standard
  - Low-rate, Low-power, Low-cost Personal Area Networks (PANs)
  - PHY and MAC layers
- ZigBee Specifications
  - Upper Layers

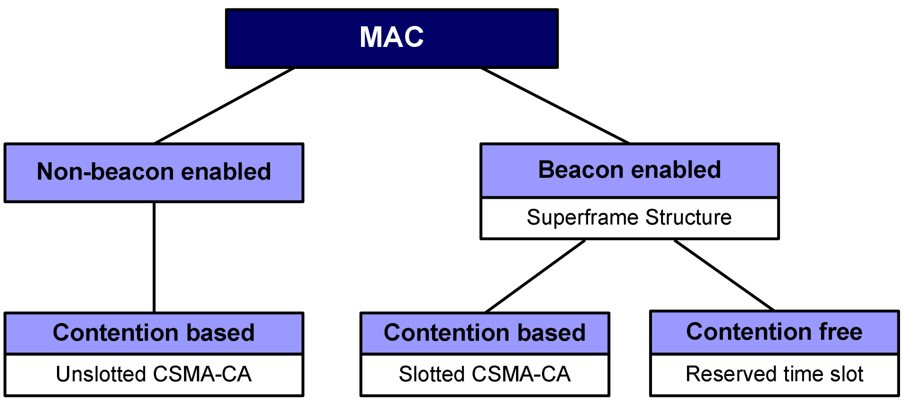


IEEE 802.15.4/ZigBee Network Topologies

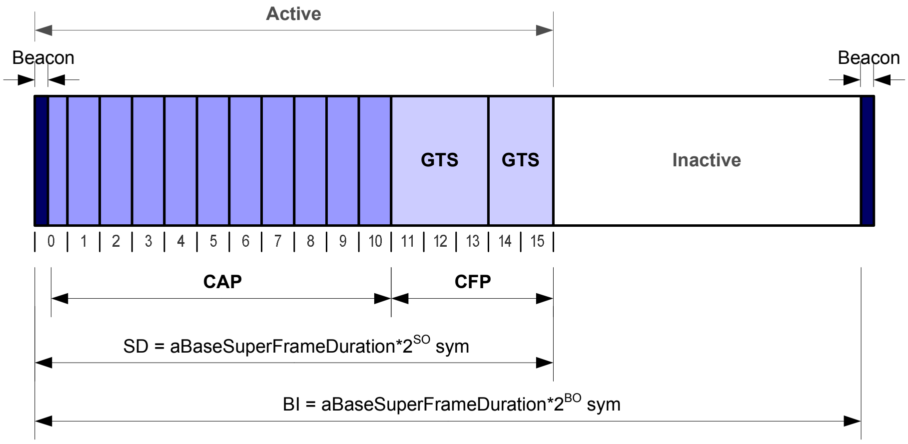


IEEE 802.15.4: MAC protocol

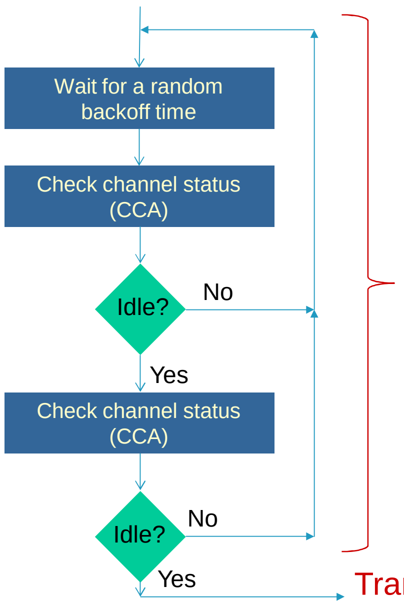
- Different operating conditions
  - duty-cycled beacon enabled mode
  - different channel access methods



IEEE 802.15.4: beacon enabled mode



CSMA/CA: Beacon-enabled mode



Transmission

At each trial the maximum backoff-window size is doubled

Only a limited number of attempts is permitted (***macMaxCSMABackoffs***)

Acknowledgement Mechanism

- Optional mechanism
- Destination Side
  - ACK sent upon successful reception of a data frame
- Sender side
  - Retransmission if ACK not (correctly) received within the timeout
  - At each retransmission attempt the maximum backoff window size is doubled
  - Only a maximum number of retransmissions allowed (*macMaxFrameRetries)*

Summary

- Introduction
- IEEE 802.11 wireless LANs (WiFi)
- Cellular Internet Access
- Addressing and routing to mobile users
- Mobile IP
- Mobility and higher-layer protocols
- Infrastructure-less networks
  - Bluetooth
- Hybrid Networks
  - Mesh Networks, Sensor Networks