Smartphone Mobile Computing

CSEP590B/F Winter 2011 (first offering)

4th Lecture, 31 January 2011

Instructor:

Gaetano Borriello

Teaching Assistants:

Temitope Oluwafemi and Cary Anderson

Overview for Today

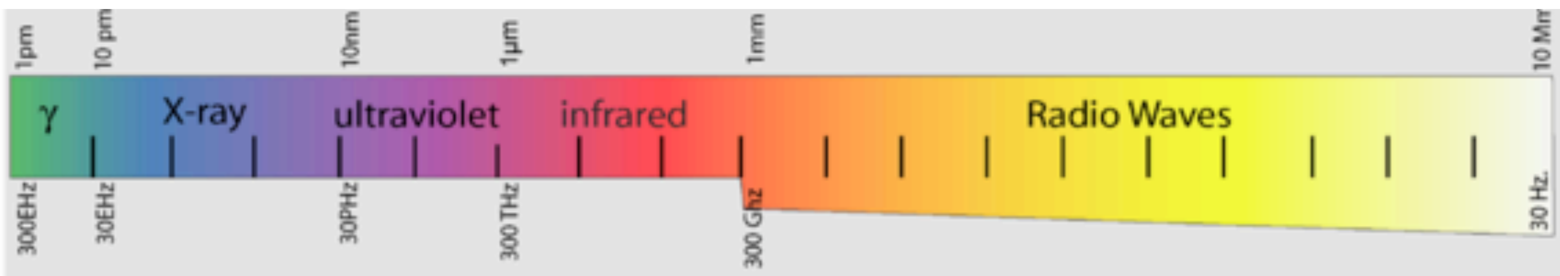
- Finish up on sensing from last week
- ML applied to sensor data for determining user context
- Q/A on sensing

- Group projects: questions on mid-term project report

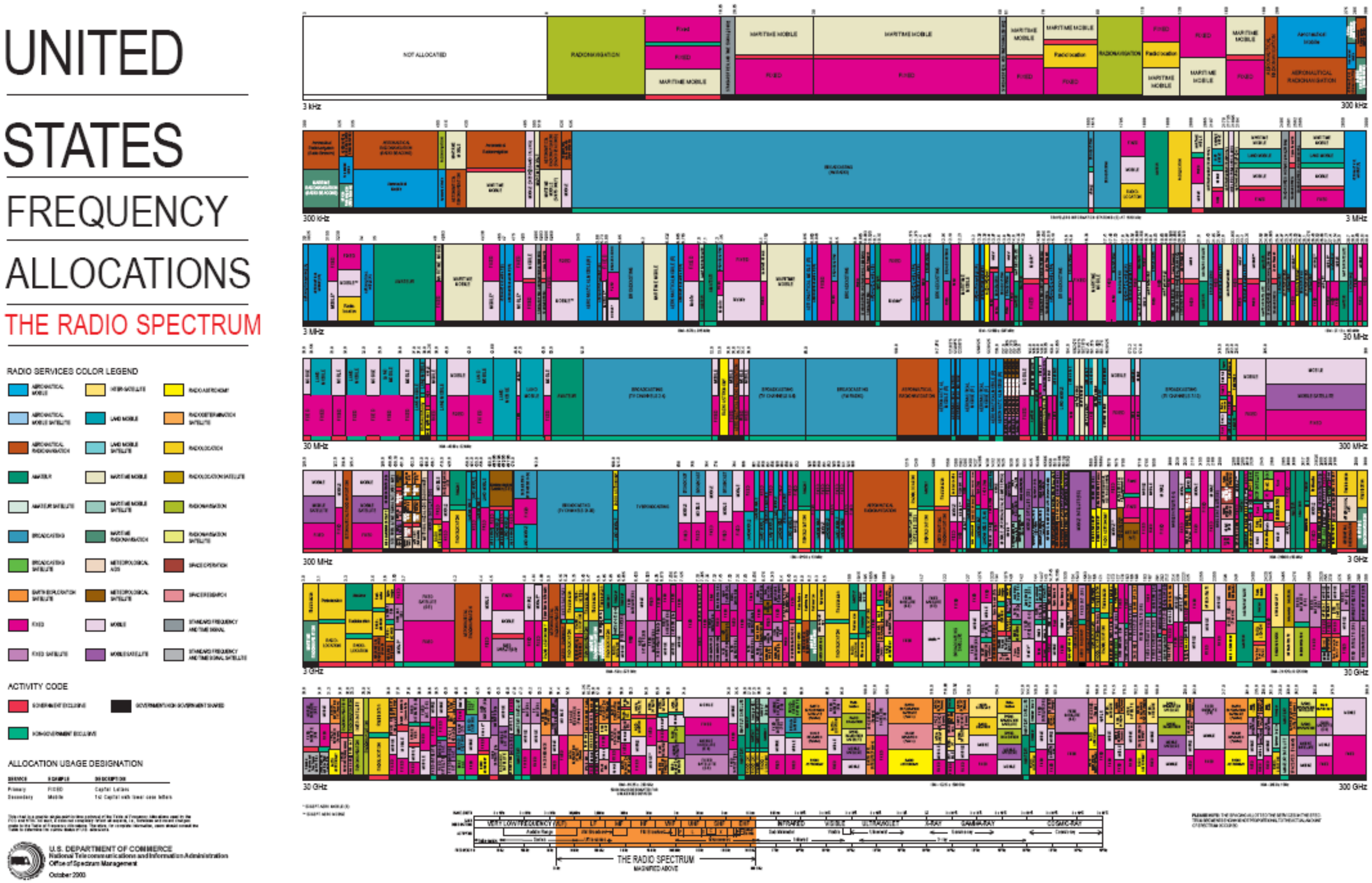
- Communication methods
- Smartphone and SMS, Bluetooth, WiFi, GPRS
- Future directions

Wireless Communication

- **Serial communication**
- **Allocated a frequency of operation**
  - Could be a range of frequencies
  - Regulated by FCC (Federal Communications Commission) in US
  - Unfortunately, allocations are not world-wide



Electromagnetic Spectrum (3kHz – 300GHz)



How wireless frequencies are allocated

- Garage door openers, alarm systems, etc. – 40MHz
- Cordless phones: 40-50MHz, 900MHz, 2.4GHz, 5.8GHz
- Baby monitors: 49MHz
- Radio controlled toys: 27-75MHz
- Wildlife tracking collars: 215-220MHz
- MIR space station: 145-437MHz
- Cell phones: 824-849MHz, 869-894MHz, 1850-1990MHz (850/1900 in US, 900/1800 in EU)
- Public safety (fire, police, ambulance): 849-869MHz
- Air traffic control radar: 960MHz-1.215GHz
- Global Positioning System: 1.227-1.575MHz
- Satellite radio: 2.3GHz
- WiFi/802.11b/g and Bluetooth: 2.4GHz
- Zigbee/802.15.4: 868MHz, 915MHz, 2.4GHz
- Microwave ovens: 2.4Ghz
- TV: 54-216 (VHF 2-13), 470-806MHz (UHF 14-69)
- Ultra-wide-band: 3.1-10.6GHz
- ISM (industrial, scientific, medical): 900MHz, 1.8GHz, 2.4GHz, 5.8GHz

Considerations in choosing a frequency

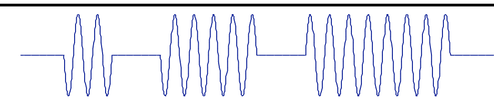
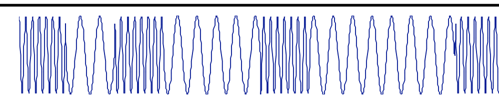
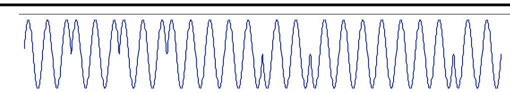
- **Carrier frequency**
  - Signal that is modulated to carry data
  - Frequency is not equal to bandwidth
- **Ability to carry data (modulation rate)**
- **Availability of devices to transmit and receive signals**
- **Interference from other devices in same band**
  - ISM bands limit power output
- **Interactions of radiation with environment**
  - absorption by water, metal, building materials, foliage
- **Reflection and multi-path properties**
  - constructive/destructive interference patterns (e.g., nulls)

Radio Protocols for Wireless Networks

- **Cellular (850-2100MHz)**
  - Voice, SMS, MMS, GPRS
- **WiFi (2.4GHz, 5GHz)**
  - Wireless LAN
- **Bluetooth (2.4GHz)**
  - Common in many consumer devices (headsets, cars, phones, etc.)
- **Zigbee (850-930MHz)**
  - Next generation radio for sensor networks and consumer devices

Communication methods

- **Modulation**

Modulation Technique	Waveform
No encoding (Baseband)	
On-Off Keying (OOK)	
Frequency Shift Keying (FSK)	
Binary Phase Shift Keying (BPSK)	
Complementary Code Keying (CCK)	

- **Multiplexing**
  - TDMA – time division - take turns talking
  - FDMA – frequency division - talk at different pitches
  - CDMA – code division - use different languages

Short Messaging Service (SMS)

- First "data" service for mobile phones
- Allows users to exchange brief text strings
- Addressing uses standard phone numbers
  - easy setup, supported by all tiers of phones, no separate accounts
- 160 characters: 1120 bits at 7bits/character
  - extensions for unicode halve this number
  - concatenated SMS for longer data
- 6 trillion SMS sent in 2010 – 35% in US and Philippines
- Cost is relatively high – more than data from Hubble telescope
  - 0.20USD/message leads to 1500USD per MB (US carriers)
  - 0.01USD/message is still 75USD per MB (India)
  - India: 3USD for 15000 SMS, US: 20USD for unlimited
  - incoming vs. outgoing message charges

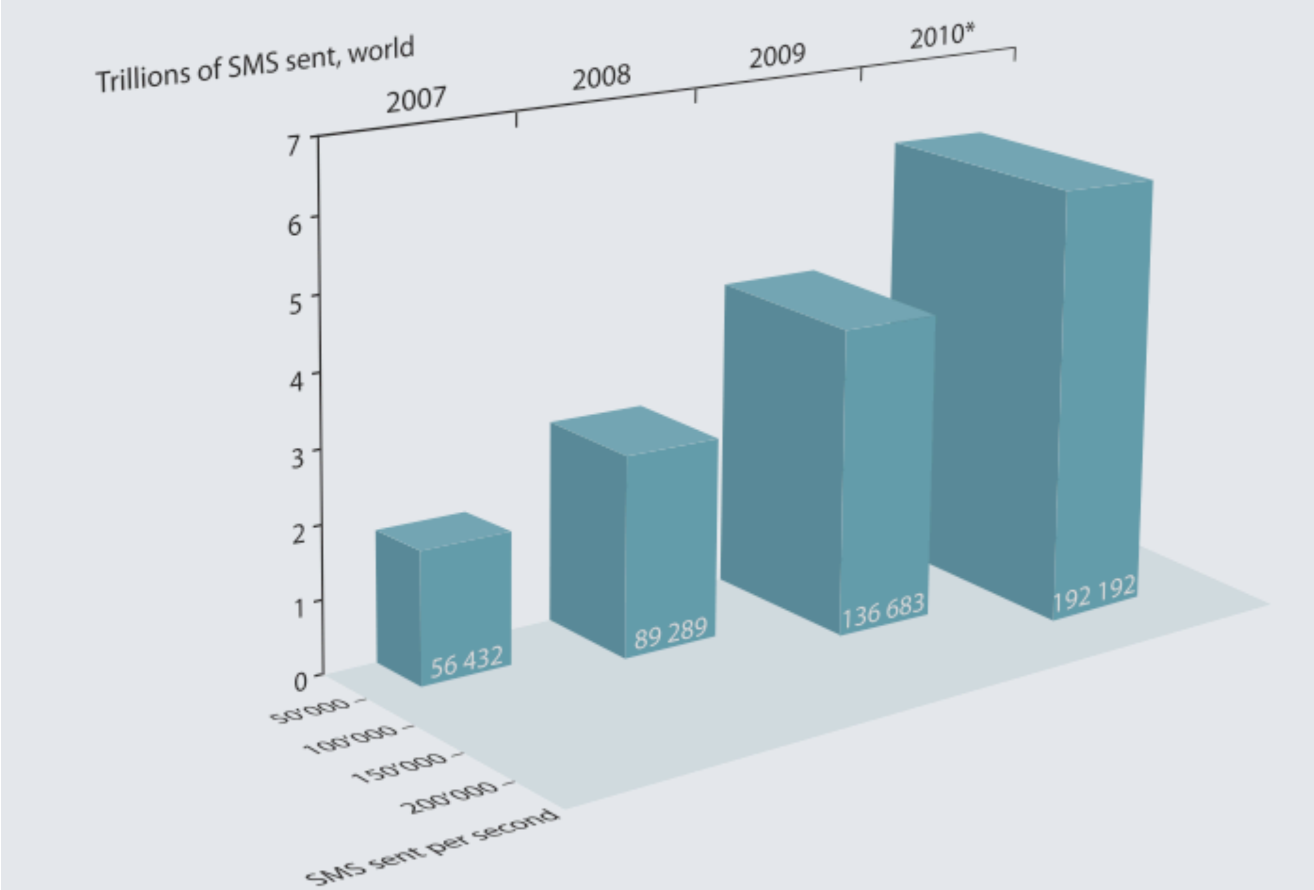
SMS history

- **Uses the control system of the GSM standard**
- **In 1993, Nokia realized they could sell unused bandwidth for an instant messaging service**
- **USSD is the still free variant of SMS**
  - carriers allocate USSD short codes for subsidized service
- **Input formats – focus on standard 12-key keyboard**
  - multi-tap is most popular (tap 3 times for “v” on 8-tuv)
  - T9 gained momentum until full-keyboard phones (predictive text)
  - auto-completion
- **Output formats**
  - single message queue
  - “conversations”

SMS services

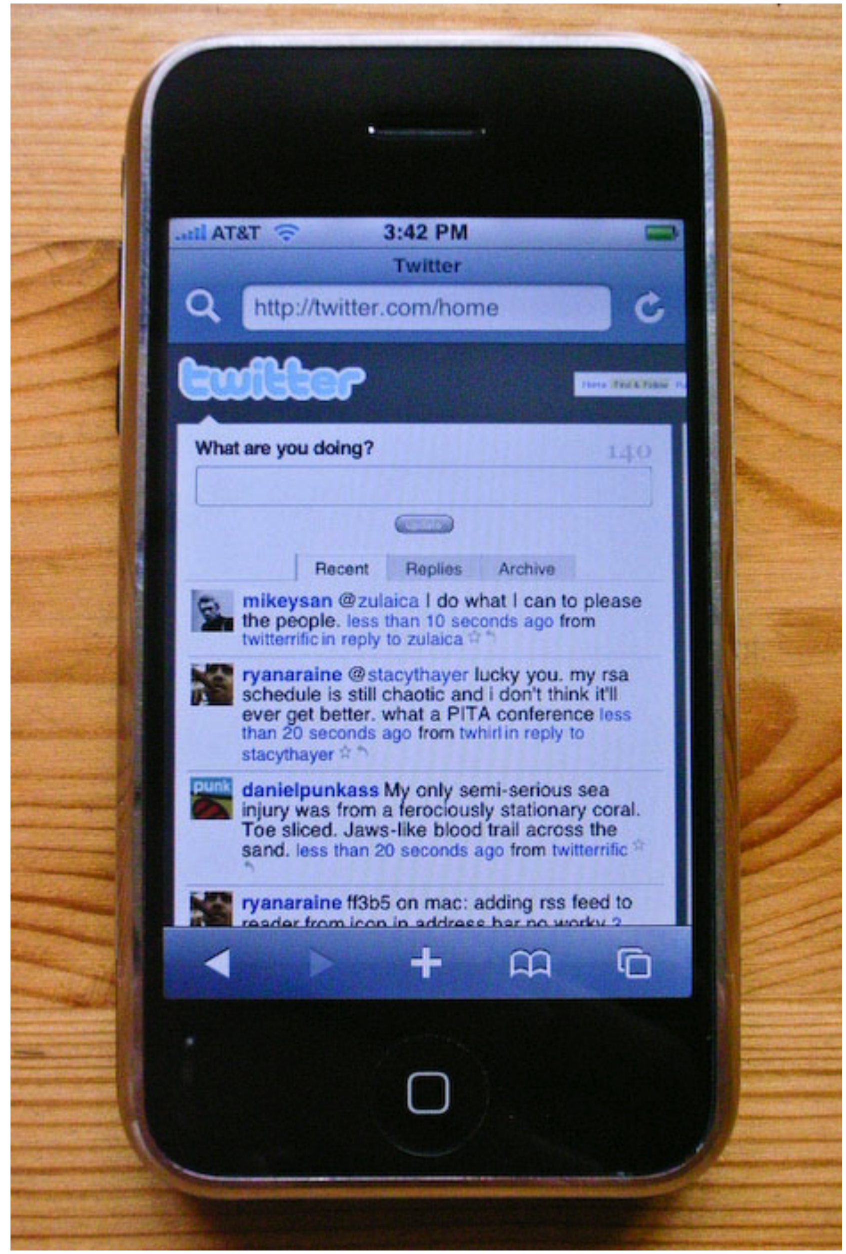
- **Short codes**
  - easier to remember shorter “phone numbers” for popular services
- **Payment**
  - transfer of payments associated with certain numbers (per msg)
- **Internet gateways**
  - allow arbitrary services
  - grab data from web and package it into SMS (e.g., OneBusAway)
  - require appropriate message formats (usability issue)

SMS growth over last 3 years



Note: *Estimate
Source: ITU World Telecommunication/ICT Indicators database

Grouptext, Twitter



Geochat

InSTEDD GeoChat 1.0 Disaster-ready Group Communications

Use SMS text messaging to coordinate with your team on the surface of a map!

Keep government agencies, first responders, and the local community ***in sync***

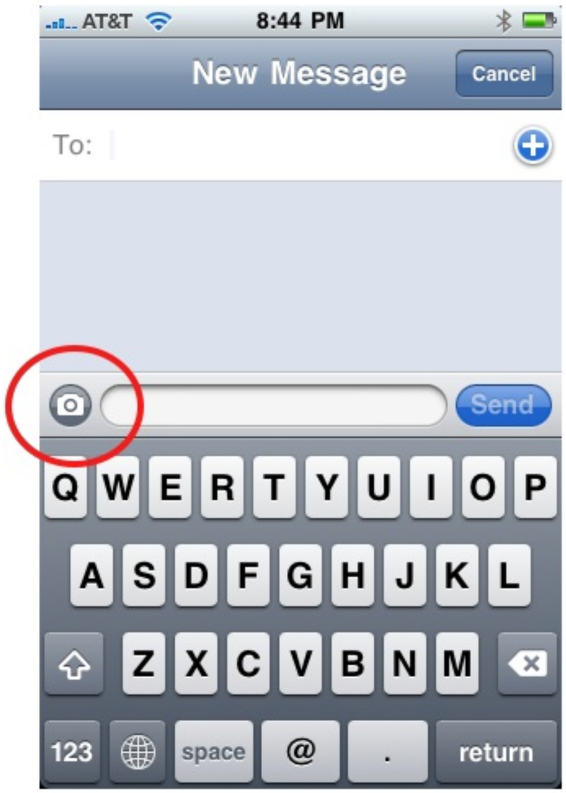
Broadcast alerts, form teams, and ***swarm*** *around critical events as they unfold*

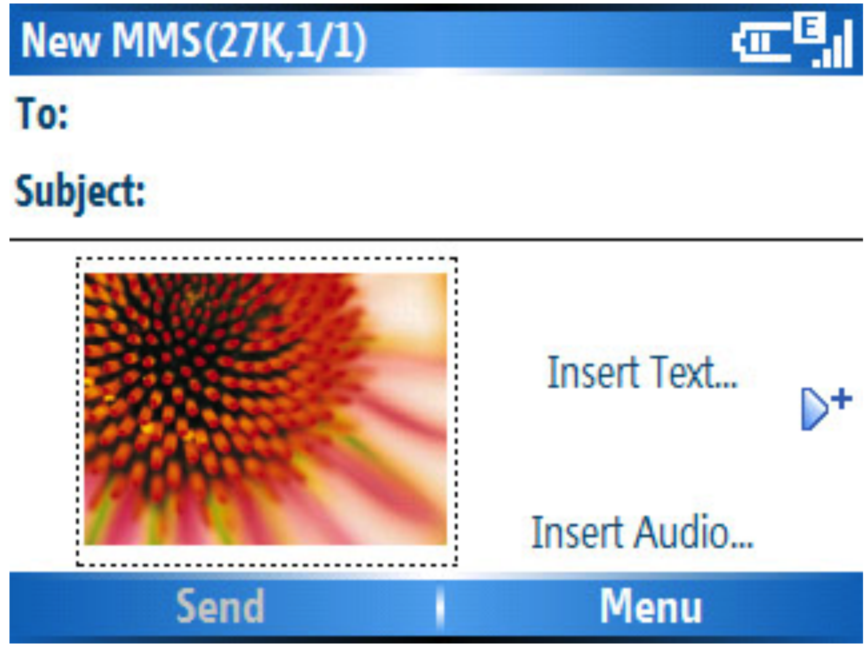
InSTEDD

Multi-media Messaging Service (MMS)

- **Similar to SMS, but no size limit**
  - began in 2002
  - really only practical on 3G networks (but works with some 2G as well)
  - 50 billion messages per year generating USD26B (2008)
  - Scandinavia is most advanced market
- **Mostly used by feature phones with cameras**
  - attach multi-media files to text message
  - if receiver isn't capable, then collected at web site, SMS with link sent
- **Pricing similar to SMS – by the message**
  - much cheaper by the bit
  - major issues are in encoding of data (currently, MIME-types) and codecs
  - no bulk messaging

MMS interface





MMS services expand connection to web

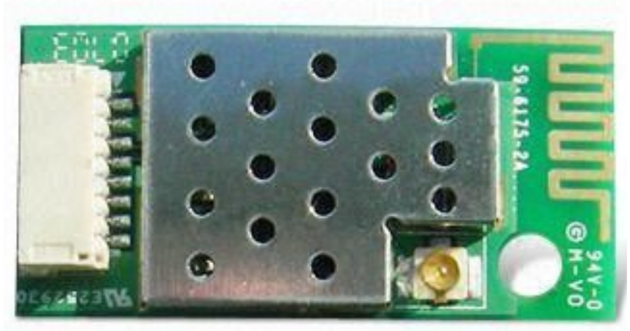
- Keyword to image-based search (possibly tied to location)
- Navigation instructions for non-smartphones
- Automatic translation services (e.g., Google Goggles)

Smartphones and SMS/MMS

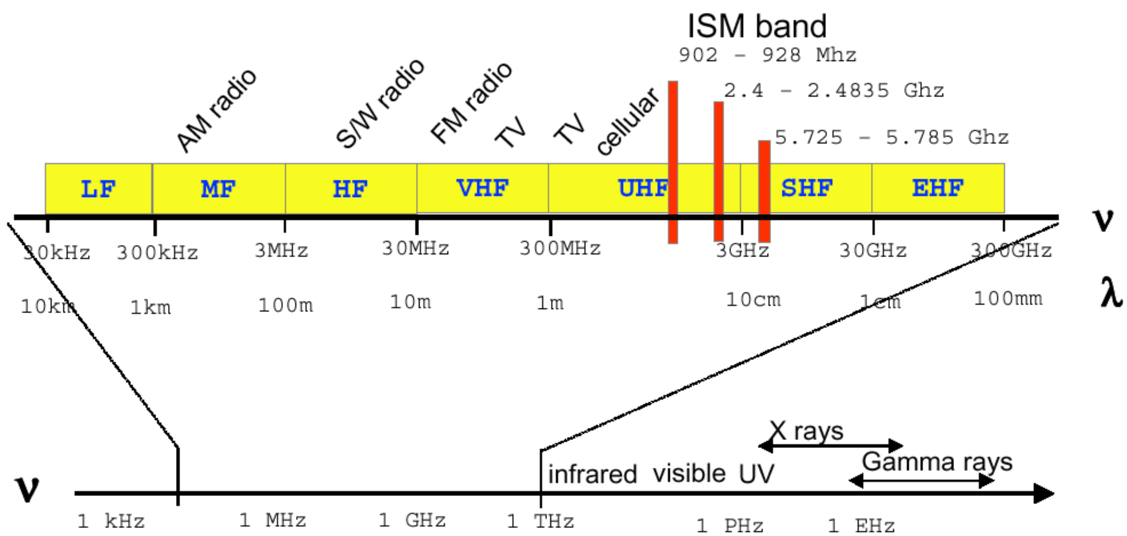
- **Legacy support for migration from feature phones**
- **Interplay with direct Internet access over GPRS**
- **Services/apps governed by**
  - pricing structure
  - familiar usage models and interfaces
- **Provide richer text entry and more media types**
  - Swype
  - video

Bluetooth

- **Short-range radio at 2.4GHz**
  - Available globally for unlicensed users
  - Low-power
  - Low-cost
  - Cable replacement
  - Devices within 10m can share up to 1Mb/sec – 700Kb/sec effective
  - Universal short-range wireless capability



Harald Blatand II unified Norway and Denmark in 10th century

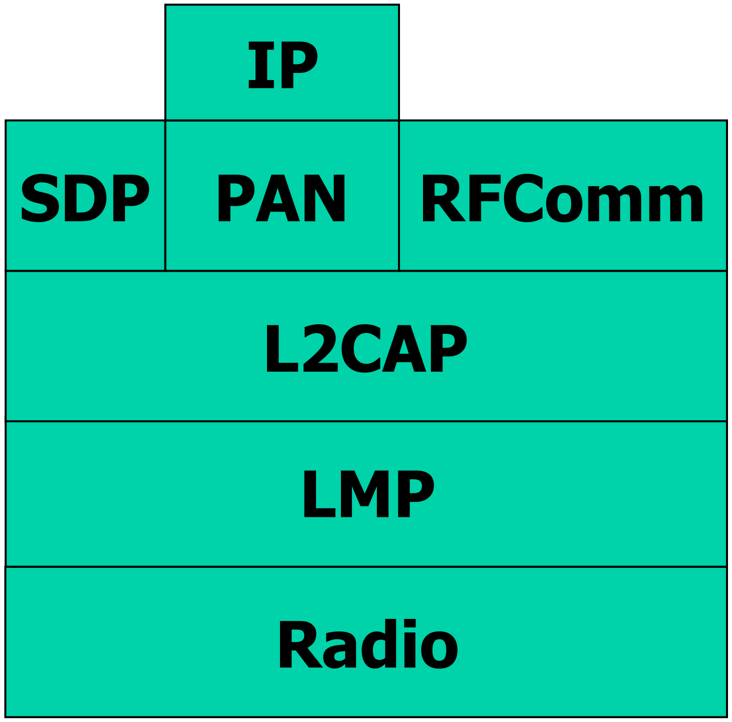


Bluetooth application areas

- **Data and voice access points**
  - Real-time voice and data transmissions
  - Cordless headsets
  - Three-in-one phones: cell, cordless, walkie-talkie
- **Cable replacement**
  - Eliminates need for numerous cable attachments for connection
  - Automatic synchronization when devices within range
- **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)

Protocol architecture

- **Bluetooth is a layered protocol architecture**
  - Core protocols
  - Cable replacement and telephony control protocols
  - Specialized protocols (profiles)
- **Core protocols**
  - Radio and baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)

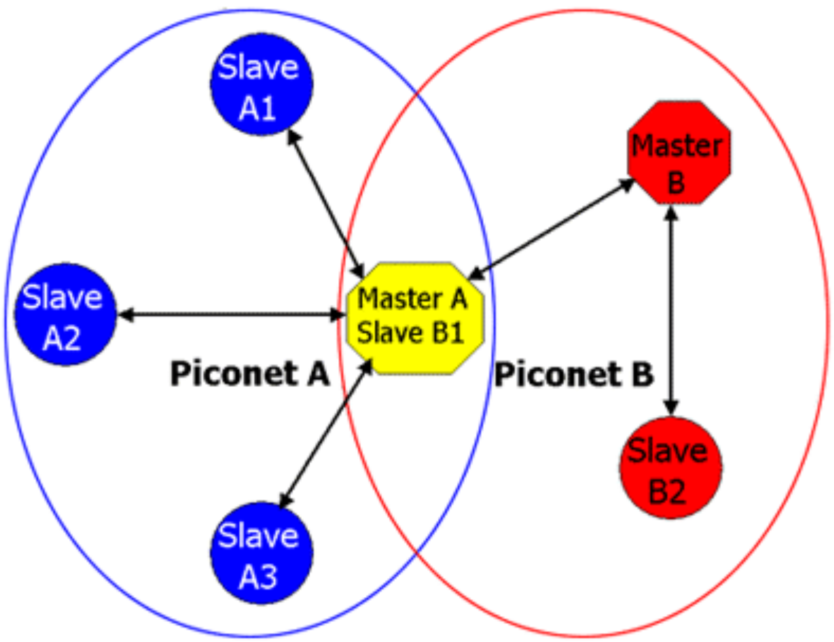


Protocol architecture

- **Cable replacement protocol**
  - RFCOMM
- **Telephony control protocol**
  - Telephony control specification – binary (TCS BIN)
- **Adopted protocols**
  - TCP/UDP/IP
  - OBEX
  - WAP
- **Profiles – vertical slide through the protocol stack**
  - Basis of interoperability
  - Each device supports at least one profile
  - Defined based on usage models
    - e.g., headset and phone, camera and TV, mp3player and car, etc.

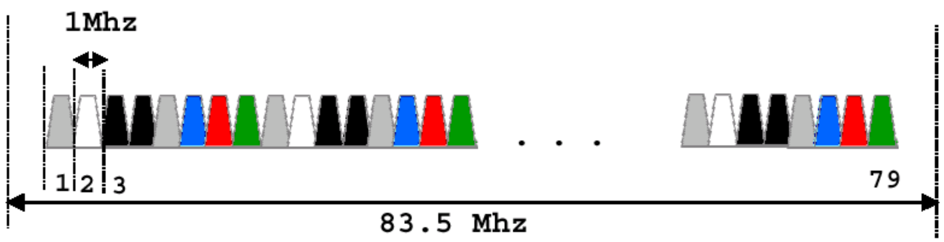
Piconets and scatternets

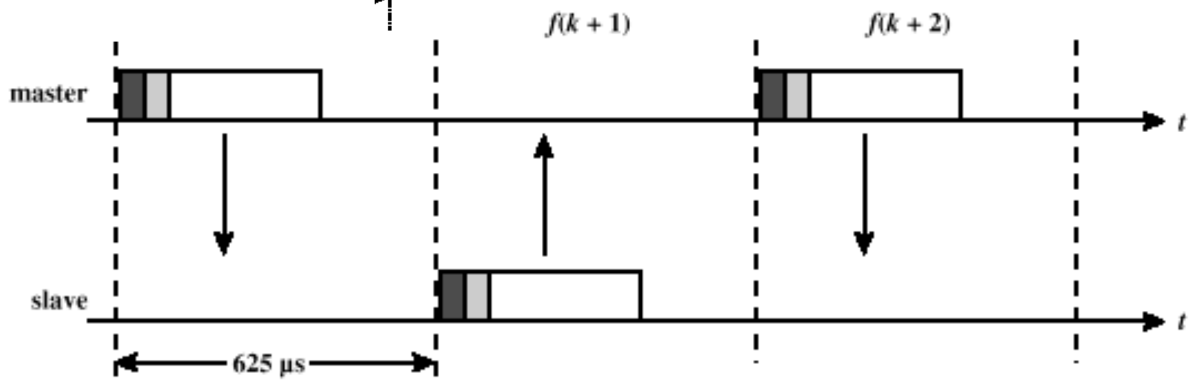
- **Piconet**
  - Basic unit of Bluetooth networking
  - Master and up to 7 slave devices
  - Master determines channel and phase
- **Scatternet**
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth



Frequency hopping

- Provides resistance to interference and multipath effects
- Total bandwidth divided into 1MHz physical channels
- Frequency hopping occurs by moving transmitter/receiver from one channel to another in a pseudo-random sequence
- Hopping sequence shared with all devices in the same piconet so that they can hop together and stay in communication





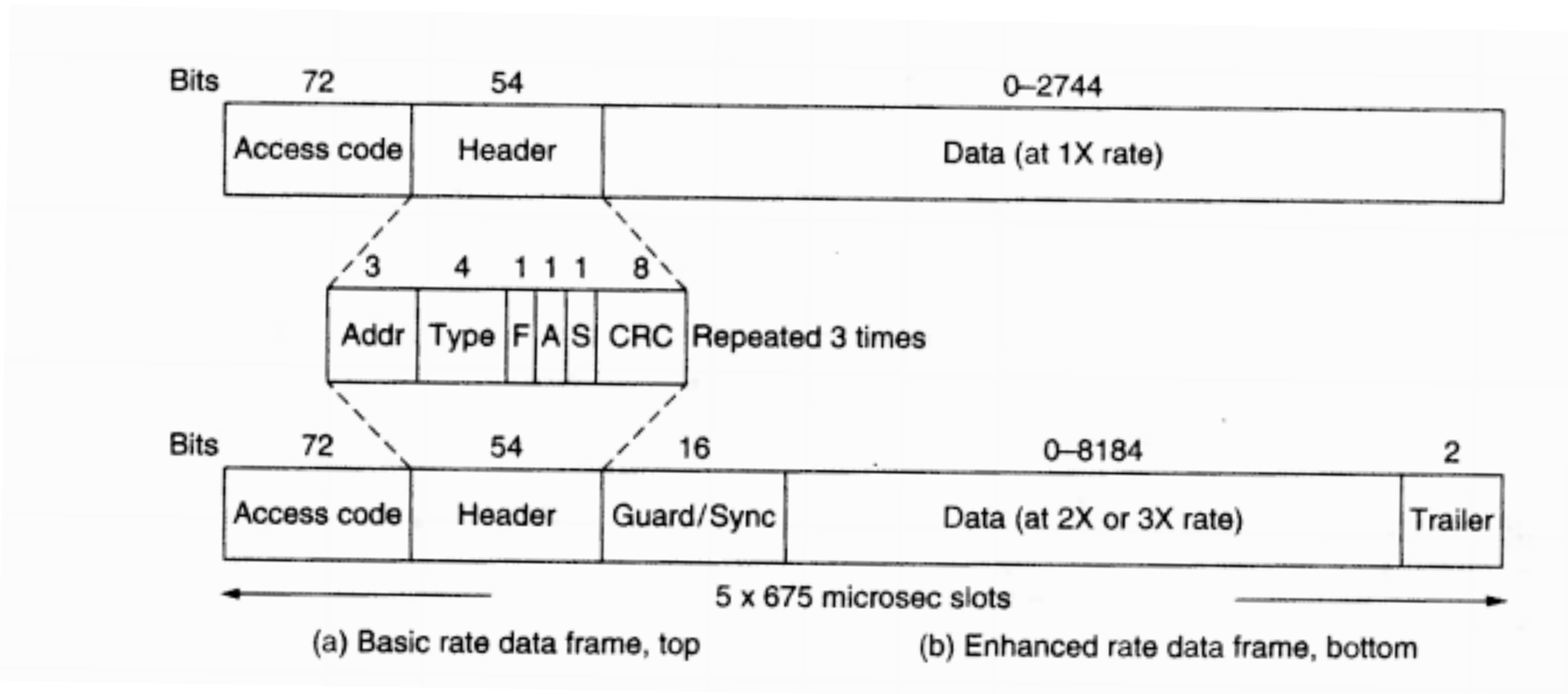
Links between master and slave

- **Synchronous connection-oriented (SCO)**
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
- **Asynchronous connection-less (ACL)**
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist

Pairing

- **Linking two devices via a shared PIN (old method)**
- **One device provides a pass-key to be entered on the other**
  - limited by I/O on some devices (e.g., head set)
- **Once paired, devices can re-discover each other and connect automatically**
- **De-pairing?**

Bluetooth packet format



Scenario steps

- **Master device (e.g., PDA) pages for nearby devices**
- **Receives response from 0, 1, or more devices**
  - Slave device (e.g., headphone) responds to page
- **Determines which it "knows" – established connections**
- **L2CAP establishes Bluetooth connection assigning paging device to be master**
- **Devices exchange profiles they both support**
- **Agree upon profile (e.g., audio streaming)**
- **Master sends audio data**
  - Two devices synchronize their frequency hopping
- **Keep-alive packets used to maintain connections**
- **Connections dropped if keep-alive packets are not ack'ed**

Limitations/Issues

- Discovery time on the order of 10sec for unknown devices
- Interaction with user required to connect to unknown devices or if multiple masters
- Can connect 8 devices at a time, more need to be multiplexed radically lowering throughput
- Doesn't support simple broadcast – need to be on same frequency hopping schedule
- Effective bandwidth closer to 500Kbps (within one scatternet, order of magnitude lower if between two)

WiFi

- **Infrastructure-based**
  - most popular
  - access points (APs) act as wireless-to-wired Ethernet gateways
- **Ad hoc network**
  - not very popular – so far

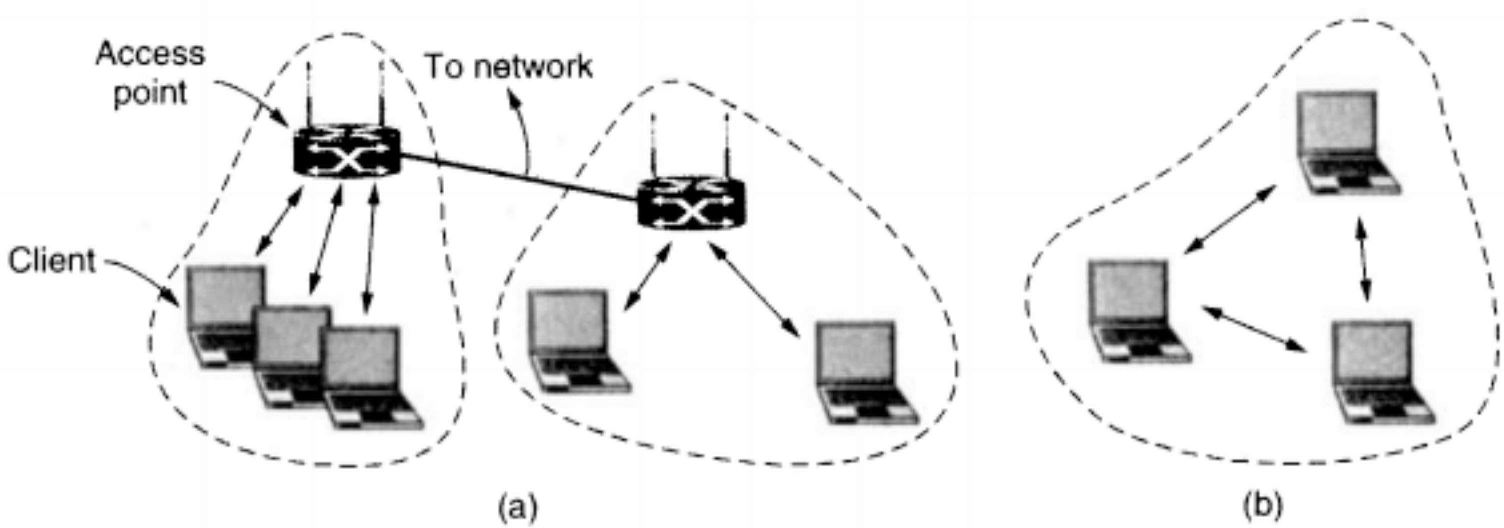


Figure 4-23. 802.11 architecture. (a) Infrastructure mode. (b) Ad-hoc mode.

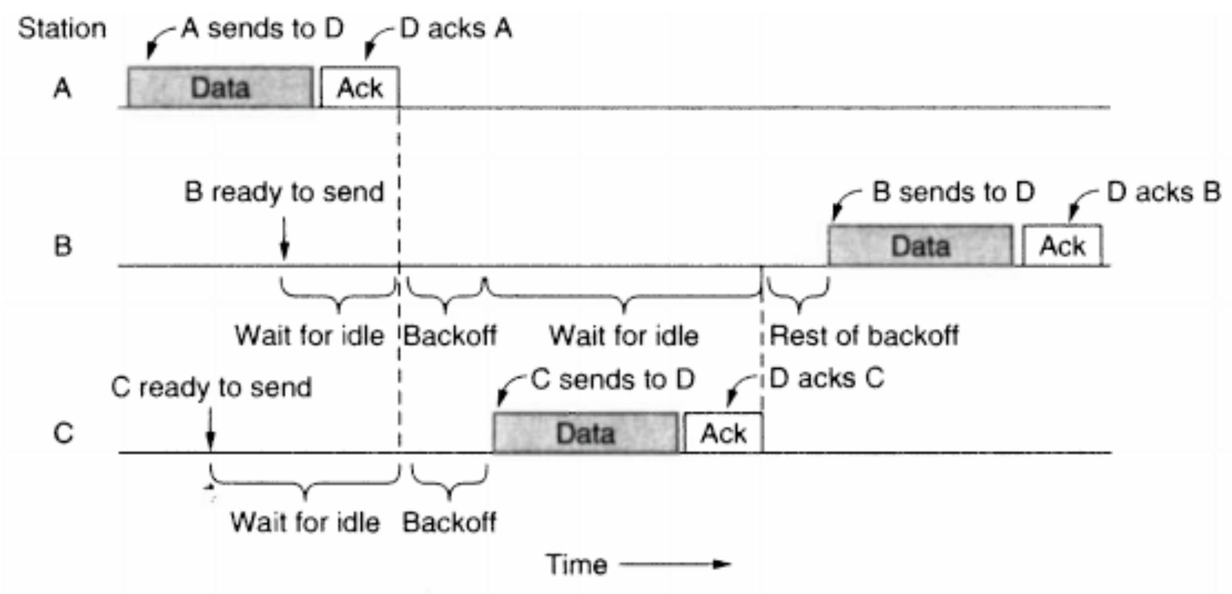
Types of WiFi (IEEE 802.11)

- **802.11b – spread spectrum – 1999**
  - 11 Mbps but also supports 5.5, 2, and 1 (2.4GHz)
- **802.11a – orthogonal frequency division multiplexing (OFDM)**
  - 54 Mbps (5GHz)
- **802.11g – OFDM with 802.11b compatibility – 2003**
  - 6 to 54 Mbps (2.4 GHz) – shorter range than 802.11b
- **802.11n – multiple antenna OFDM (MIMO/OFDM) – 2009**
  - 100 – 600 Mbps (2.4 GHz but wider band)

- **Most common today is b/g combination**

Major issues with WiFi

- **Can't transmit and receive simultaneously**
  - outgoing signal swamps any incoming signals
- **Difficult to detect collisions – DCF (distributed coord. function)**
  - collision at receiver may not be seen by sender
  - collision avoidance instead of collision detection
  - use of acks to determine if collision occurred



Hidden and exposed devices

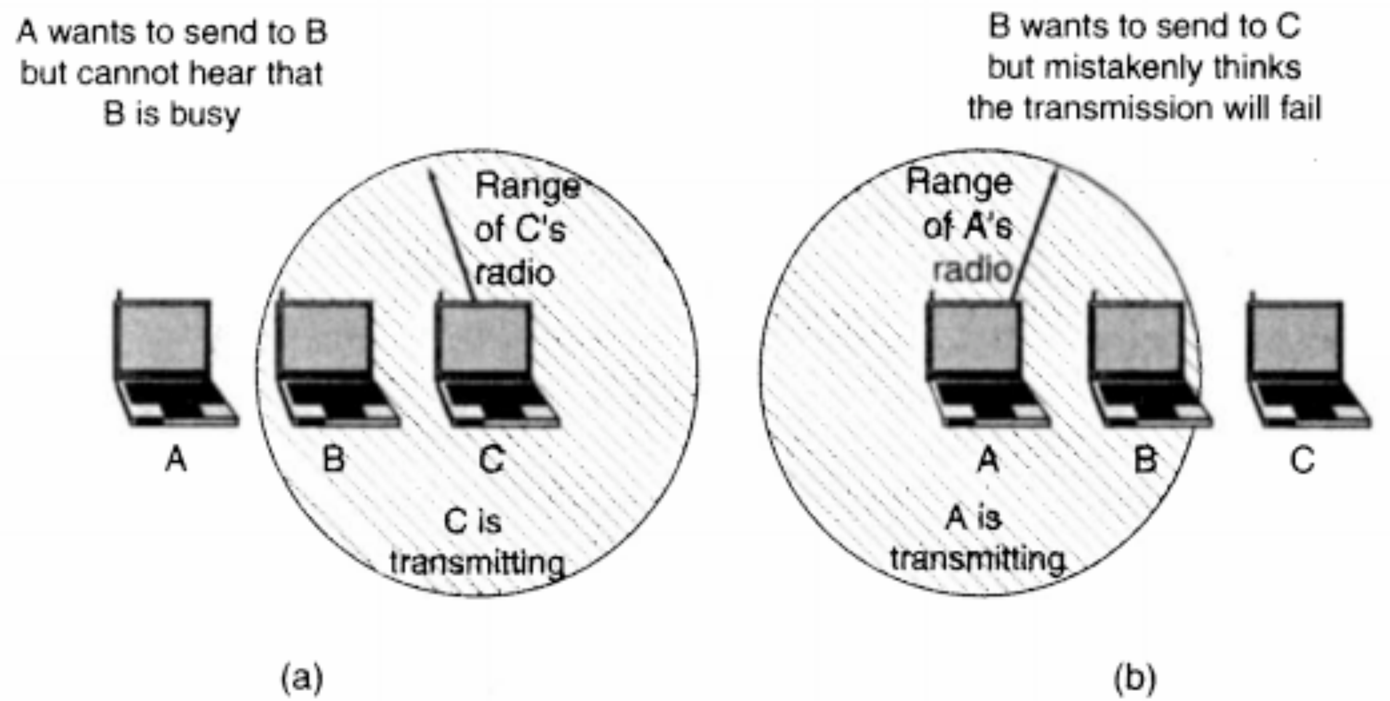


Figure 4-26. (a) The hidden terminal problem. (b) The exposed terminal problem.

Access points

- **Gateways between wireless and wired networks**
- **Devices associate with an access point**
  - security managed at association with passcode or registration (WPA2)
- **Orchestrate their associated clients**
  - beacon frames (provide way to fingerprint WiFi environment and used for indoor location)
  - reservations and buffer status
  - fairness among clients

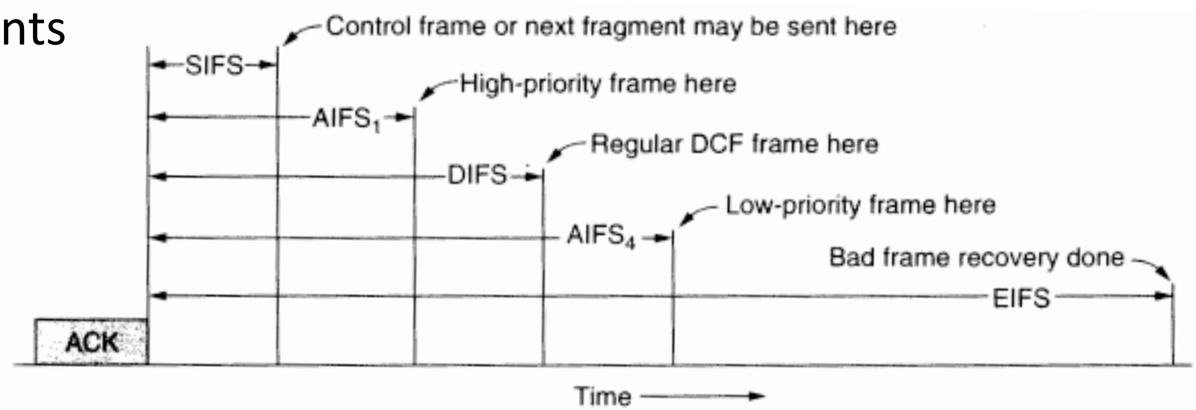


Figure 4-28. Interframe spacing in 802.11.

WiFi packet format

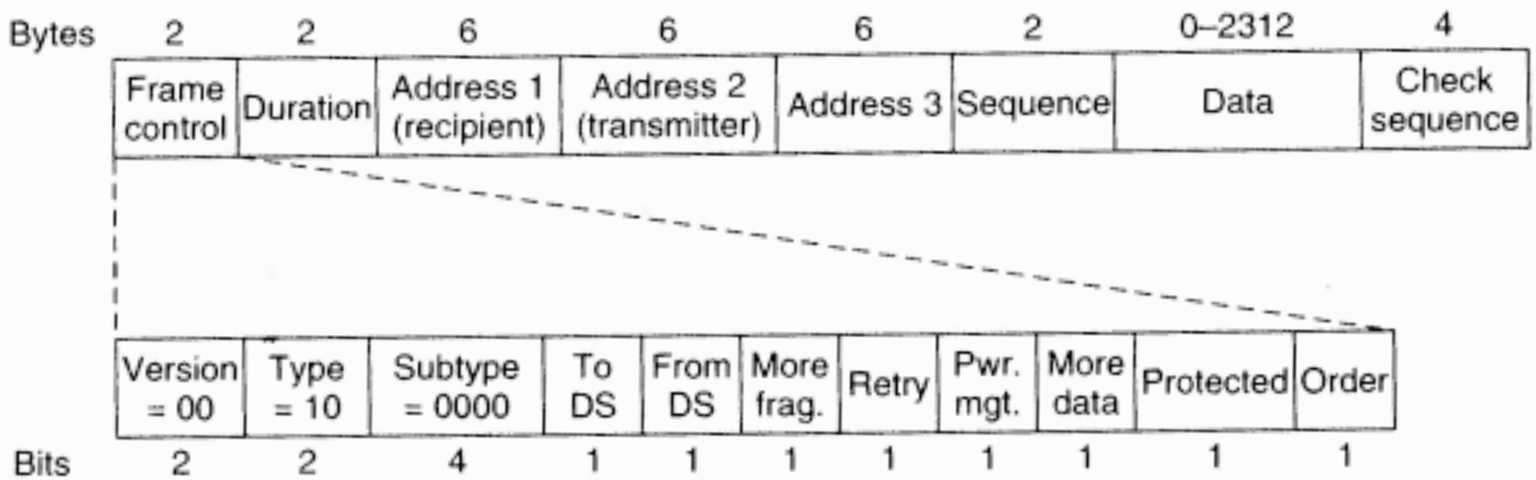


Figure 4-29. Format of the 802.11 data frame.

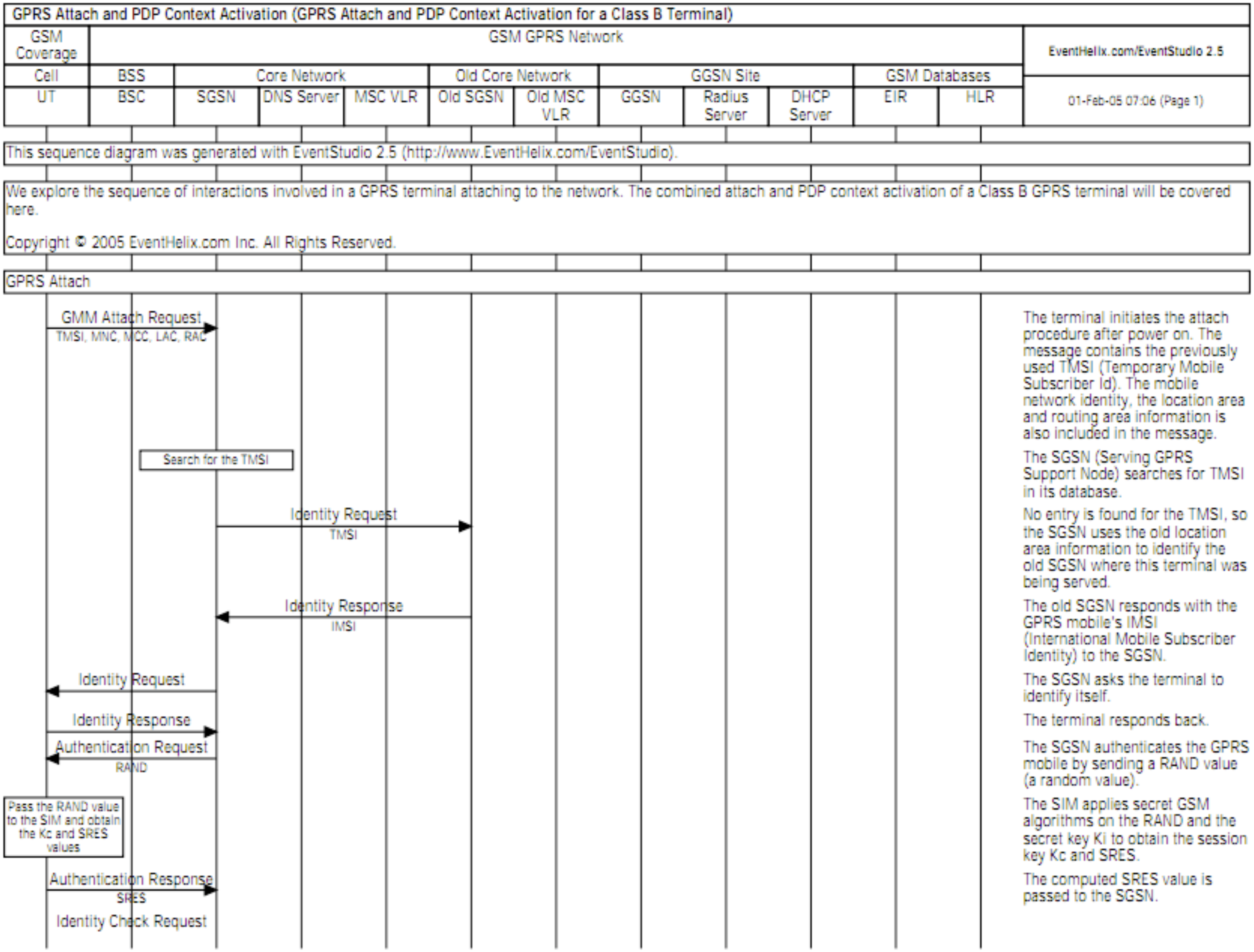
Hotspot and peer-to-peer

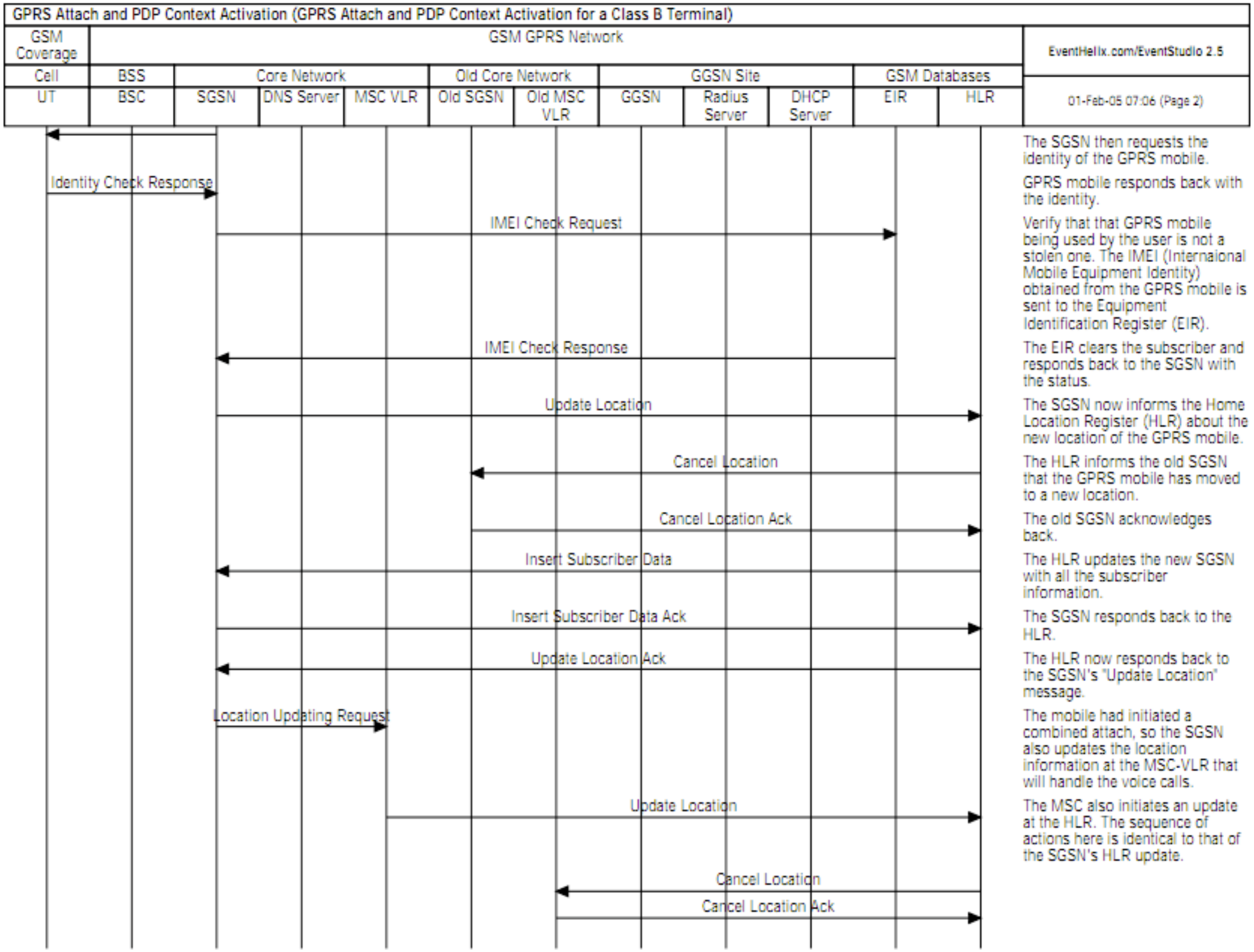
- **WiFi devices can act as hotspots (APs) for others**
  - must allocate IP addresses just like an AP
  - tethering of laptop through smartphone via WiFi to access web
- **Ad hoc networks of peers**
  - must decide on scope of network (temporary SSID)
  - allocate IP addresses to participants (distributed/centralized)

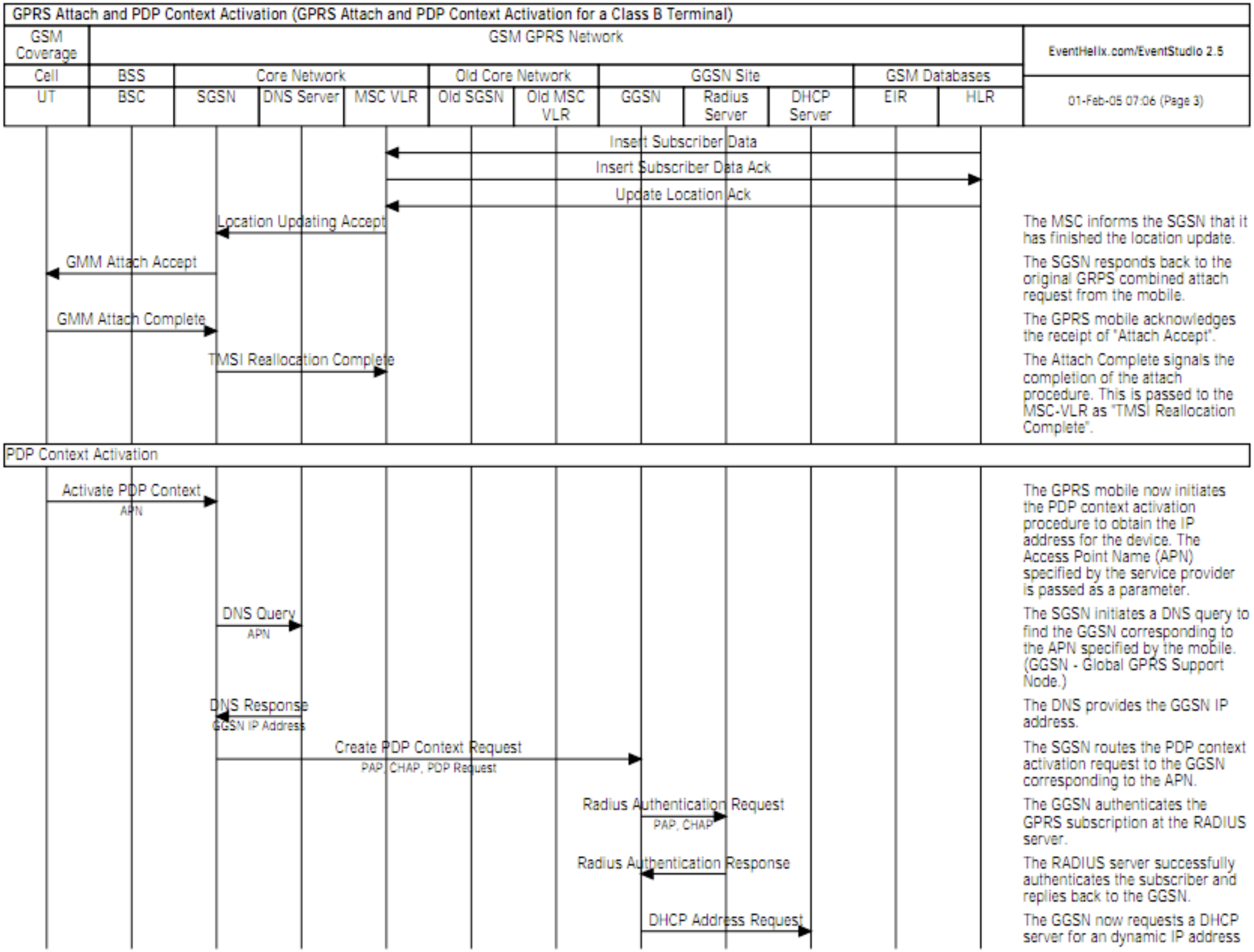
GPRS

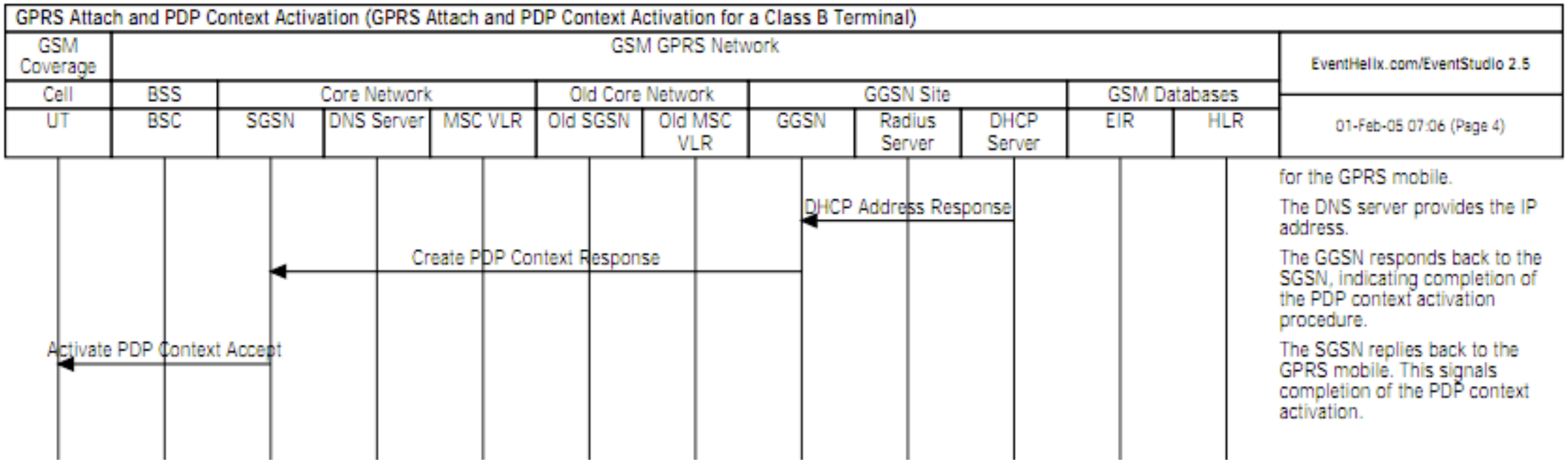
- **2G/3G data connection standard - 200 Kbits/sec**
- **High-speed download packet access (HSDPA/3.5G) can go up 14.4Mbps**
- **HSPA+ w/ MIMO at 42Mbps (2010) and can go up to 84Mbps**

- **Similar architecture to infrastructure-based WiFi**
  - cell towers as access points
  - more emphasis on billing and “roaming”


GPRS Attach and PDP Context Activation (GPRS Attach and PDP Context Activation for a Class B Terminal)
GSM Coverage
GSM GPRS Network
EventHelix.com/EventStudio 2.5
Cell
BSS
Core Network
Old Core Network
GGSN Site
GSM Databases
UT
BSC
SGSN
DNS Server
MSC VLR
Old SGSN
Old MSC VLR
GGSN
Radius Server
DHCP Server
EIR
HLR
01-Feb-05 07:06 (Page 1)
This sequence diagram was generated with EventStudio 2.5 (http://www.EventHelix.com/EventStudio).
We explore the sequence of interactions involved in a GPRS terminal attaching to the network. The combined attach and PDP context activation of a Class B GPRS terminal will be covered here.
Copyright © 2005 EventHelix.com Inc. All Rights Reserved.
GPRS Attach
GMM Attach Request
TMSI, MNC, MCC, LAC, RAC
The terminal initiates the attach procedure after power on. The message contains the previously used TMSI (Temporary Mobile Subscriber Id). The mobile network identity, the location area and routing area information is also included in the message.
Search for the TMSI
The SGSN (Serving GPRS Support Node) searches for TMSI in its database.
Identity Request
TMSI
No entry is found for the TMSI, so the SGSN uses the old location area information to identify the old SGSN where this terminal was being served.
Identity Response
IMSI
The old SGSN responds with the GPRS mobile's IMSI (International Mobile Subscriber Identity) to the SGSN.
Identity Request
The SGSN asks the terminal to identify itself.
Identity Response
The terminal responds back.
Authentication Request
RAND
The SGSN authenticates the GPRS mobile by sending a RAND value (a random value).
Pass the RAND value to the SIM and obtain the Kc and SRES values
The SIM applies secret GSM algorithms on the RAND and the secret key Ki to obtain the session key Kc and SRES.
Authentication Response
SRES
The computed SRES value is passed to the SGSN.
Identity Check Request


GPRS Attach and PDP Context Activation (GPRS Attach and PDP Context Activation for a Class B Terminal)
GSM Coverage
GSM GPRS Network
EventHelix.com/EventStudio 2.5
Cell
BSS
Core Network
Old Core Network
GGSN Site
GSM Databases
UT
BSC
SGSN
DNS Server
MSC VLR
Old SGSN
Old MSC VLR
GGSN
Radius Server
DHCP Server
EIR
HLR
01-Feb-05 07:06 (Page 2)
The SGSN then requests the identity of the GPRS mobile.
Identity Check Response
GPRS mobile responds back with the identity.
IMEI Check Request
Verify that that GPRS mobile being used by the user is not a stolen one. The IMEI (Internaional Mobile Equipment Identity) obtained from the GPRS mobile is sent to the Equipment Identification Register (EIR).
IMEI Check Response
The EIR clears the subscriber and responds back to the SGSN with the status.
Update Location
The SGSN now informs the Home Location Register (HLR) about the new location of the GPRS mobile.
Cancel Location
The HLR informs the old SGSN that the GPRS mobile has moved to a new location.
Cancel Location Ack
The old SGSN acknowledges back.
Insert Subscriber Data
The HLR updates the new SGSN with all the subscriber information.
Insert Subscriber Data Ack
The SGSN responds back to the HLR.
Update Location Ack
The HLR now responds back to the SGSN's "Update Location" message.
Location Updating Request
The mobile had initiated a combined attach, so the SGSN also updates the location information at the MSC-VLR that will handle the voice calls.
Update Location
The MSC also initiates an update at the HLR. The sequence of actions here is identical to that of the SGSN's HLR update.
Cancel Location
Cancel Location Ack


GPRS Attach and PDP Context Activation (GPRS Attach and PDP Context Activation for a Class B Terminal)
GSM Coverage
GSM GPRS Network
EventHelix.com/EventStudio 2.5
Cell
BSS
Core Network
Old Core Network
GGSN Site
GSM Databases
UT
BSC
SGSN
DNS Server
MSC VLR
Old SGSN
Old MSC VLR
GGSN
Radius Server
DHCP Server
EIR
HLR
01-Feb-05 07:06 (Page 3)
Insert Subscriber Data
Insert Subscriber Data Ack
Update Location Ack
Location Updating Accept
The MSC informs the SGSN that it has finished the location update.
GMM Attach Accept
The SGSN responds back to the original GRPS combined attach request from the mobile.
GMM Attach Complete
The GPRS mobile acknowledges the receipt of "Attach Accept".
TMSI Reallocation Complete
The Attach Complete signals the completion of the attach procedure. This is passed to the MSC-VLR as "TMSI Reallocation Complete".
PDP Context Activation
Activate PDP Context
APN
The GPRS mobile now initiates the PDP context activation procedure to obtain the IP address for the device. The Access Point Name (APN) specified by the service provider is passed as a parameter.
DNS Query
APN
The SGSN initiates a DNS query to find the GGSN corresponding to the APN specified by the mobile. (GGSN - Global GPRS Support Node.)
DNS Response
GGSN IP Address
The DNS provides the GGSN IP address.
Create PDP Context Request
PAP, CHAP, PDP Request
The SGSN routes the PDP context activation request to the GGSN corresponding to the APN.
Radius Authentication Request
PAP, CHAP
The GGSN authenticates the GPRS subscription at the RADIUS server.
Radius Authentication Response
The RADIUS server successfully authenticates the subscriber and replies back to the GGSN.
DHCP Address Request
The GGSN now requests a DHCP server for an dynamic IP address


GPRS Attach and PDP Context Activation (GPRS Attach and PDP Context Activation for a Class B Terminal)
GSM Coverage
GSM GPRS Network
EventHelix.com/EventStudio 2.5
Cell
BSS
Core Network
Old Core Network
GGSN Site
GSM Databases
UT
BSC
SGSN
DNS Server
MSC VLR
Old SGSN
Old MSC VLR
GGSN
Radius Server
DHCP Server
EIR
HLR
01-Feb-05 07:06 (Page 4)
DHCP Address Response
Create PDP Context Response
Activate PDP Context Accept
for the GPRS mobile.
The DNS server provides the IP address.
The GGSN responds back to the SGSN, indicating completion of the PDP context activation procedure.
The SGSN replies back to the GPRS mobile. This signals completion of the PDP context activation.

4G

- **WiMax and LTE (steps toward 4G) now at 50Mbps**
- **4G will be 100Mbps (high mobility) to 1Gbps (low mobility)**
  - data is primary target (voice as another type of data)
  - will all use OFDM and MIMO

WiMax

- **Worldwide Interoperability for Microwave Access**
  - first developed in 2001 as IEEE 802.16
  - 10x range of 802.11b at 2.5GHz (licensed spectrum)
  - careful control by base station of all traffic
  - security built-in from start

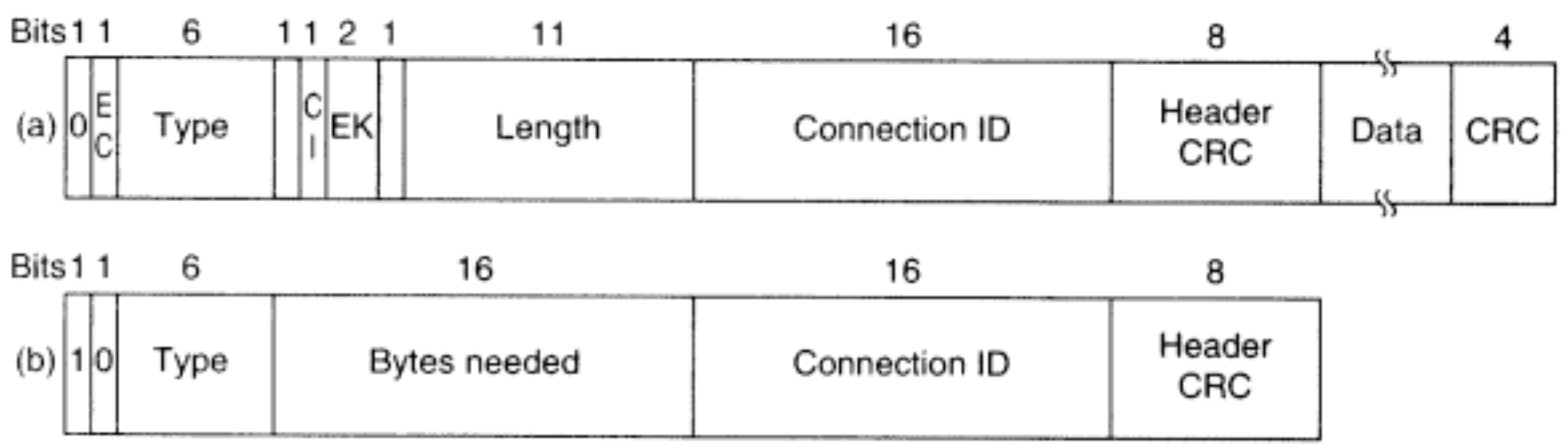


Figure 4-33. (a) A generic frame. (b) A bandwidth request frame.

NFC/RFID

- RFID read/write – 100Kbps