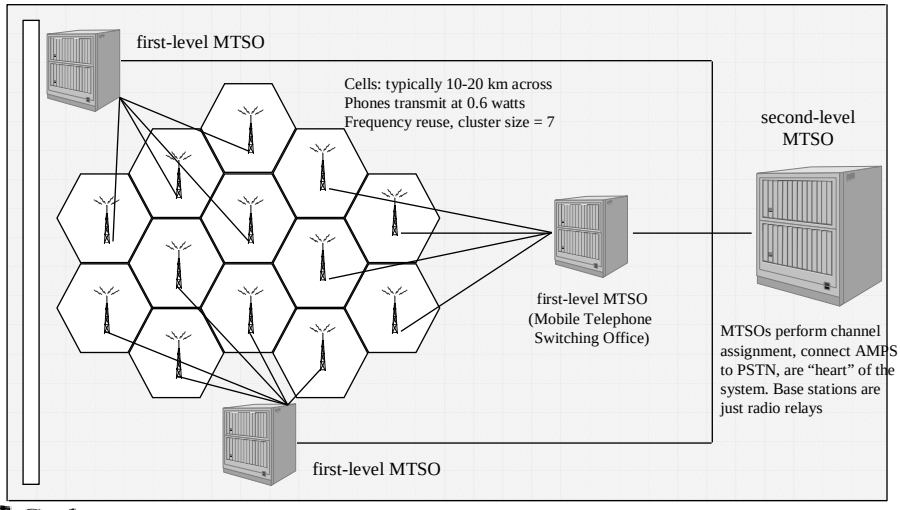
Course Overview

- Introduction and History
- Data in Wireless Cellular Systems: AMPS and CDPD
- Data in Wireless Local Area Networks
- Internet Protocols
- Routing and Ad-Hoc Networks
- TCP over Wireless Link
- Services and Service Discovery
- System Support for Mobile Applications

AMPS: History

- FCC allocated spectrum space in the 800 MHz spectrum and issued licenses for test systems in Chicago and Washington, D.C.
- first commercial systems available 1983, available in all major cities in US in a few years
- AMPS result of extensive research by Bell Labs in 1960s and 1970s
- 800 MHz band was compromise
  - lower frequencies occupied by FM and TV systems
  - higher frequencies were deemed too unreliable (information loss due to weather conditions, multipath fading, etc.) with existing technology

AMPS Architecture



AMPS Spectrum and Allocation

- A band set up for independent carriers
- B band set up for traditional wireline carriers, such as the Regional Bell Operating Companies (RBOC)
- idea was to ensure competition in all markets, while restrict potential proliferation of companies that would complicate spectrum allocation/management
- today, many independent carriers bought by RBOCs, so it is not uncommon to have one company operating in Band A in one market and Band B in another market
- channels always come in pairs, spaced 45 MHz apart

AMPS: Channel Numbers and Frequencies

System	Mhz	# of channels	boundary channel number	transmitter center frequency, mobile	transmitter center frequency, base
Not used		1	(990)	(824.010)	(869.010)
E-AMPS	1	33	991	824.040	869.040
			1023	825.000	870.000
A	10	333	1	825.030	870.30
			333	834.990	879.990
B	10	333	334	835.020	880.020
			666	844.980	889.980
A’	1.5	50	667	845.010	890.010
			717	846.480	891.480
B’	2.5	83	717	846.510	889.510
			799	848.970	883.970

E-AMPS, A’ and B’ added later, A’ and B’ may optionally use 5 MHz
Channels 313-333 and 334-354 are control channels, provider is free to use them in any manner deemed appropriate

AMPS Identification Numbers

- three identification numbers are used:
  - mobile station’s serial number (SN)
    - 32-bit binary number
    - uniquely identifies a cellular unit
    - established by manufacturer at the factory
      - 8-bit manufacturer code, assigned by FCC to manufacturer
      - 6 bit reserved (currently all 0)
      - 18 bits serial number, assigned by manufacturer
    - should not be easily alterable, burned into ROM
  - system identification number (SID)
    - 15-bit binary number, uniquely identifies cellular system
    - FCC assigns SID
    - mobile station in the cell must transmit the SID
  - mobile identification number (MIN)
    - digital representation of mobile’s 10-digit telephone number

AMPS: Call Initiation

- user enters number and presses SEND
- phone sends number to be called and own identity on access channel (random access channel), retry in case of collision
- MTSO looks for idle channel (if caller is customer of MTSO's company or one of its partners) and sends back channel number on the control channel
- mobile phone switches to the selected voice channel and waits until the called party picks up the phone

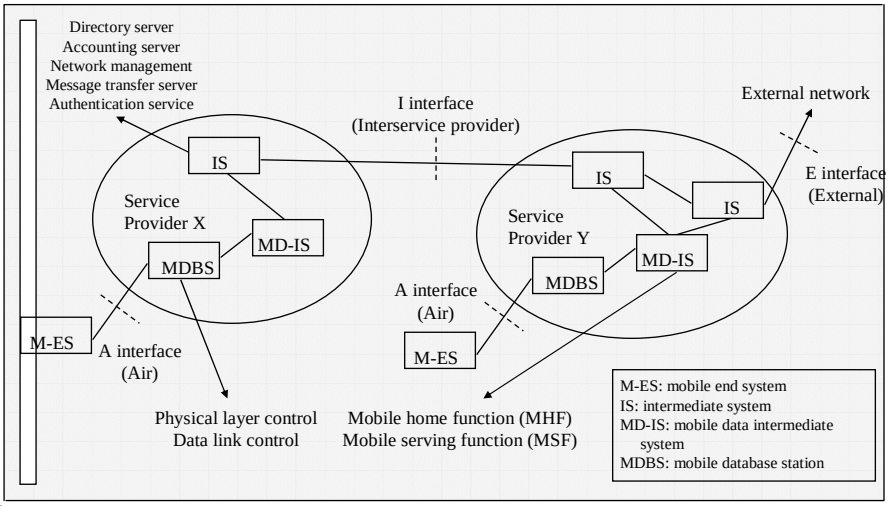
AMPS: Call Reception

- idle phones continuously listen to the paging channel to detect messages directed at them
- when someone initiates call to mobile, message is sent to home MTSO to find out where mobile currently is
- a packet is then sent to base station in current cell, which pages the mobile on the paging channel
- if mobile replies, base assigns channel number and sends it to mobile
- mobile switches to this channel and starts making ringing sound

AMPS: Security

- analog cellular phones are completely insecure
  - anyone with all-band radio receiver can tune in and listen, just ask the British Royal Family
  - also, combining all-band receiver with a computer, one can monitor the control channels and record all 32-bit serial numbers and 34-bit MINs (kind of like monitoring Ethernet for password in clear text, except that intrusion here is even easier)
  - once SN and MIN are known, use them to reprogram cheap phones and viola: all your calls will be charged to unsuspecting victim, who will only notice weeks later, when phone bill arrives (big scam in New York).
  - provisions to authenticate a device (shared secret, burned into hardware), but older phones do not support this and therefore device authentication not used
  - even with device authentication, communication over airlink not encrypted and therefore still unsafe
- also an issue of vandalism and damage to antennas and base stations (similar to damaged public phone booths)

CDPD: Architecture



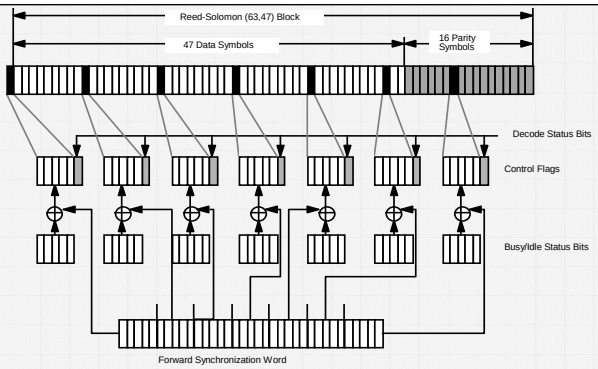
CDPD: Architecture

- M-ES: user device, mobile, identified by at least one globally unique Network Entity Identifier (NEI)
- IS: basically a router, might provide additional services
- MD-IS: only entity that has knowledge of mobility, runs MNLP (Mobile Network Location Protocol):
  - each M-ES belongs to a fixed home area, MHF keeps track of this information
  - MSF handles packet transfer services for visiting M-ES
  - requires that M-ES register with serving MD-IS when roaming
- MDBS: supports air interface to M-ES
  - resides at the AMPS cell
  - uses AMPS transmit and receive equipment

CDPD: Protocol Stack

- follows OSI stack
- CDPD basically specifies physical layer and data link layer protocols only
- nominal channel rate: 19.2 kbps, maximum throughput after coding & framing, ignoring contention, is 11.8 kbps on downlink (to mobile), 13.3 kbps on uplink
- standard specifies support for CLNP (ConnectionLess Network Protocol) and IP (Internet Protocol) at layer 3
- higher layers can be TCP or TP4
- CDPD also specifies a wide variety of upper-layer protocols (directory management, electronic messaging, etc.), based on OSI and Internet services

CDPD: Channel Coding



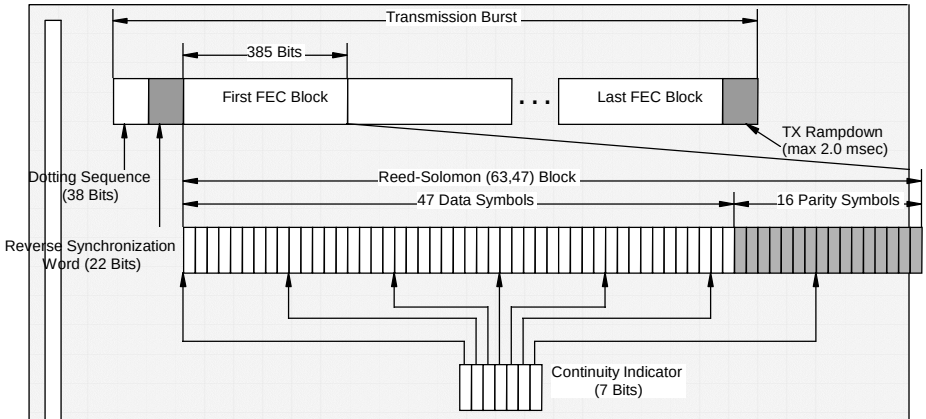
RF link-layer frame segmented into blocks of 282 data bits (6*47). Each 6-bit symbol participates in a (63, 47) Reed-Solomon block code: can correct up to 8 6-bit symbol errors. Total block length is 378 bits.

Every 10th 6-bit symbol is used to spread busy/idle flag and decode status flag, monitored by mobiles. Each flag is 5 bits, modified by forward synchronization word.

CDPD: Forward Channel

- forward channel is continuous, contiguous series of blocks, interleaved with sync. and control flags
- forward synchronization word
  - marker for FEC block boundaries and timing references
  - binary value: 11101 00001 11000 00100 11001 01010 01111
  - each group of five bits XOR-ed with one 5-bit busy/idle flag
- control flags
  - busy/idle status flag: signals status of reverse channel
    - channel busy = 00000, channel idle = 11111
  - block decode status flag: could received block be decoded (burst errors and collision both prevent successful decoding)
    - success = 00000, failure = 11111
    - transfer 6 or 7 bits, but ignore extra bits (flag is one 5-bit word)

CDPD: Channel Coding

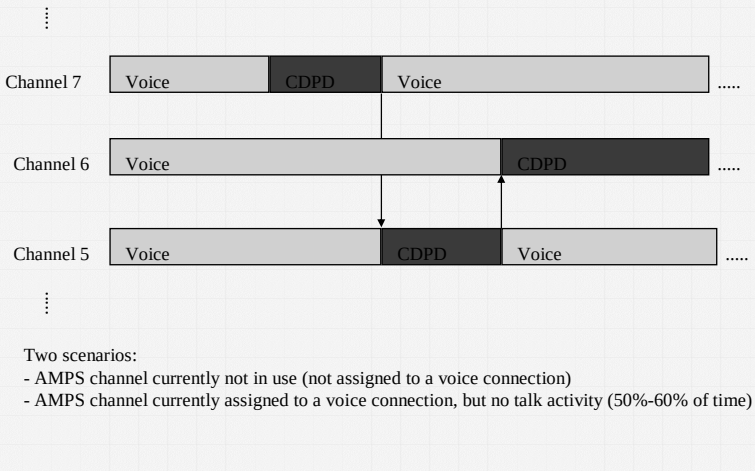


Contention on up-link: each 378-bit block followed by "continuity" or EOT indication requesting subsequent block reservation if necessary. Default maximum number of block: 64

CDPD: MAC Protocol

- downlink/forward channel: no contention, only one sender: the MDBS. All frames are broadcasted, each M-ES picks out the ones destined for it or for everyone
- uplink/reverse channel: contention is a problem
  - access to channel follows a DSMA/CD protocol:
    - uses time slots of 60 bit times (see structure of forward channel)
    - "digital sense": watch forward channel to determine whether reverse channel is busy or idle (busy/idle flags every 60 bits)
    - if busy, skip a random number of slots and try again. If still busy, wait for longer period (statistically twice as long) and retry
    - if idle, start transmitting
    - "collision detection": decode flag in forward channel indicates with delay whether there was a collision
    - keep sending until collision is detected or until maximum number of slots is set or until MDBS tells M-ES to shut down

CDPD: Sharing AMPS Channels



Two scenarios:
- AMPS channel currently not in use (not assigned to a voice connection)
- AMPS channel currently assigned to a voice connection, but no talk activity (50%-60% of time)

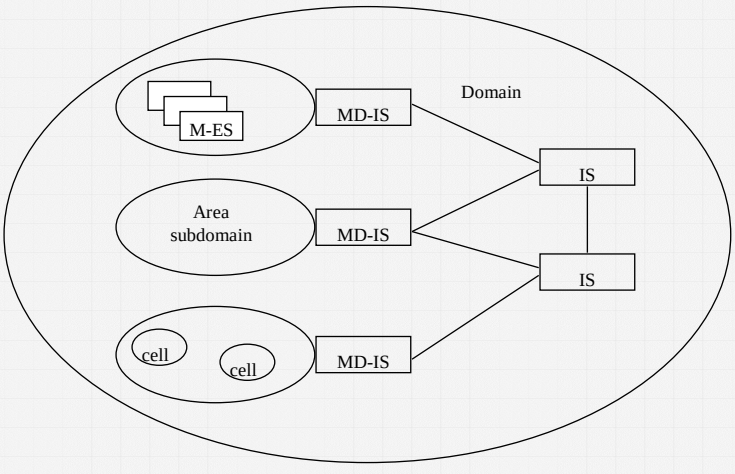
CDPD: Sharing AMPS Channels

- each cell can have multiple pairs of up- and downlink channels for data transmission (**channel streams**), each stream managed by one logical MDBS
- MDBS can find out what channels are currently not assigned by sniffing/monitoring control channels
  - before channel is used, connection setup through control channels
- MDBS monitors active voice channels by “sniffing” low-level radio frequencies (even if no voice activity, AMPS uses in-band signaling at low frequencies)
  - narrowband sniffing: scans each 30 kHz channel, one at a time
  - wideband sniffing: analyze all radio frequencies in the complete 12.5 MHz spectrum
- if voice channels become active, MDBS initiates hop
- timing is crucial to avoid interfering with AMPS system
  - MDBS has a ramp-up and ramp-down time of 10 ms
  - M-ES has ramp-up and ramp-down time of 2 ms

CDPD: Sharing AMPS Channels

- two types of channel hops:
  - forced channel hop is the one described before: get out of the way of voice channel that is about to be used
  - planned channel hop: initiated by MDBS periodically. Timer value typically set to a value less than an AMPS user's perception that the CDPD traffic is interference ("cross-channel interference"?)
- specifications are based on notion that CDPD users are second-class citizens. However, if CDPD becomes more popular, nothing prevents network providers from dedicating channels to CDPD (except that as is, voice is the big cash cow.....)

CDPD: Mobility Management



CDPD: Mobility Management Identifiers

- NEI (Network Entity Identifier): identifies mobile
- LCI (Local Cell Identifier): unique cell identifier for all cells controlled by the same MDBS
- CSI (Channel Stream Identifier): unique 6-bit identifier for all channel streams in a cell
- LCI and CSI together uniquely identify all channels on any given cell or its adjacent cells
- LSAI (Local Service Area Identifier): 16-bit unique number for all service areas in a CDPD network
- SPNI (Service Provider Network Identifier): 16-bit unique CDPD network identifier

CDPD: Mobility Management

- cell transfer decision: compare relevant parameters on previous RF channel and current RF channel (after channel hop):
  - no change in LCI, CSI, cell group color or area color: channel hop occurred within current cell
  - area color is the same, but LCI and CSI are different: intra-area cell transfer is performed
  - different area colors: inter-area cell transfer procedure is performed

CDPD: Intra-Area Cell Transfer

- intra-area cell transfer: controlled by same MD-IS
- M-ES initiates transfer if channel becomes bad (extended loss of channel synchronization and/or unacceptable error rate)
- to assist M-ES in locating CDPD channel, MDBS periodically broadcasts RF channel number in use or as candidates for use in adjacent cell
- after M-ES synchronized with new RF channel, sends link-layer receive ready to serving MD-IS
- MD-IS acknowledges frame and updates its information for M-ES (physical media association)

CDPD: Inter-Area Cell Transfer

- starts out identical to intra-area cell transfer
- once M-ES synchronized with new channel, mobile sends “end system hello” (ESH) to new serving MD-IS
- ESH informs MD-IS of presence of M-ES, register its address (NEI)
- new serving MD-IS sends message to home MD-IS to tell it where data for M-ES should be redirected
- home MD-IS acknowledges if registration is successful
- new serving MD-IS confirms successful registration to M-ES
- home MD-IS “flushes” previous serving MD-IS, telling it that messages are no longer forwarded for this M-ES

CDPD: Evaluation

- based on widespread system, AMPS
- provides reasonable data rate at variable cost (12 to 19 cents/US per kilobyte of data)
- Available (at end of 1997) in US (166 “regions”, Canada (30 sites in Alberta, 2 in BC), Ecuador (4 cities), Indonesia (trial in Jakarta), Mexico (2 cities), and New Zealand (trial in 4 cities)
- What does the future hold?
  - Andrew Tanenbaum: “use is growing rapidly”
  - Ulysses Black: whether CDPD will be the technology of choice for wireless data remains to be seen
  - Bob Egan, DEC: CDPD will become competitor to packet radio systems such as ARDIS or MOBITEX in short term, but will be only interim solution until digital cellular radio is available