



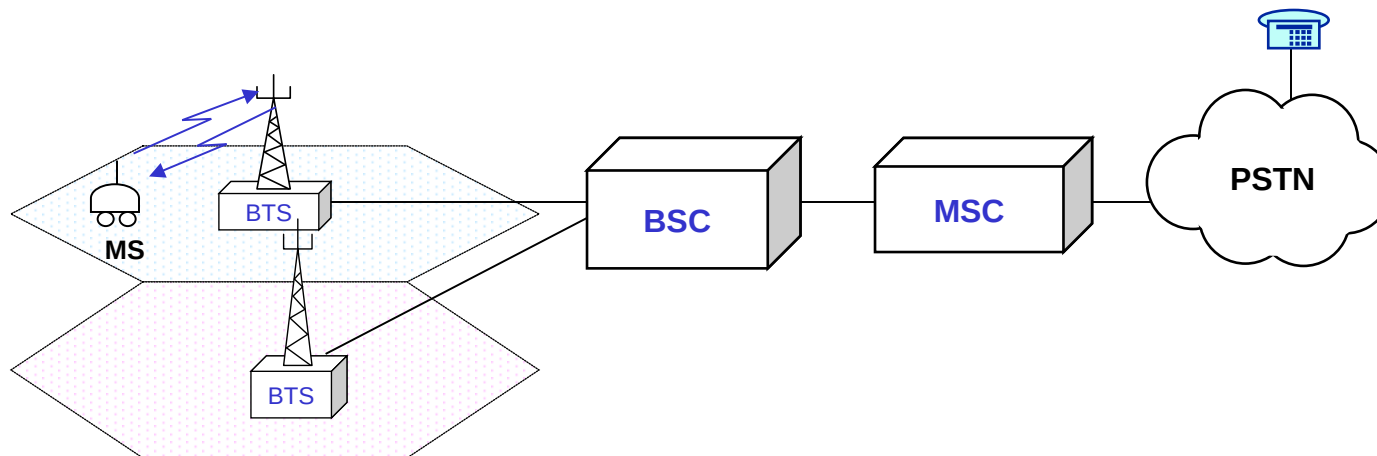
Next Generation Wireless Technologies

Jason Hillyard
New York City
July 14-16, 2000

Agenda

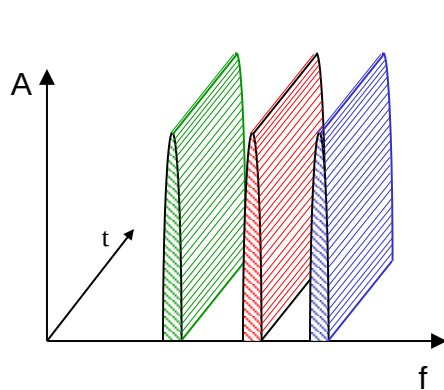
- Digital Cellular Concepts
- Current Technologies: GSM and CDMA
- GPRS and EDGE
- 3G: cdma2000 and W-CDMA
- Location Technologies

Cellular Network

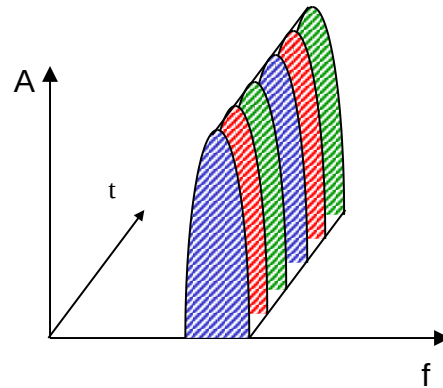


MS	Mobile Station
BTS	Base Tranceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center

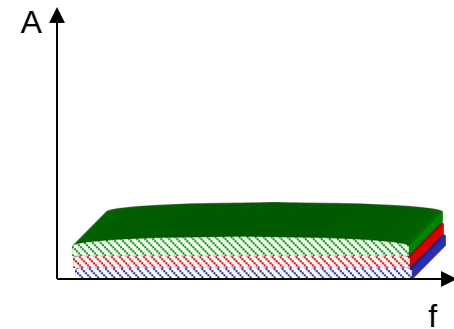
Multiple Access Methods



FDMA



TDMA



CDMA

Digital Communications: Data vs. Voice

- Voice Considerations
 - low bit-rate vocoder
 - transmission errors reduce voice quality
 - uses circuit-switched channel
- Data Considerations
 - transmission errors not acceptable
 - ARQ protocols used in link and transport layers
 - uses circuit or packet switched channel

Current Technology

- CDMA
- GSM

CDMA: Introduction

- Developed and first deployed in early 90's
- Mainly used in North America and Asia
- 57M subscribers worldwide
- Sprint PCS, Verizon (Airtouch, BAM, GTE), DDI (Japan)

CDMA: Features

- Voice at 13k, 8kbps
- Dial-up data and fax at 9.6k, 14.4kbps
- Packet data at 9.6k, 14.4kbps
- Higher speed packet data to 76kbps (Japan)
- SMS, etc...

CDMA: Technical Description

- 1.25 MHz channel
- Direct-sequence spread spectrum
- 800 MHz and 1900 MHz bands
- Communication protocols based on IS-54 TDMA and AMPS
- Designed to be compatible/coexist with AMPS

CDMA: Packet Data

- Actually uses a circuit-switched channel
- Radio Link Protocol (RLP) transmits data between phone and base station
- Standard protocols (PPP, IP, etc.) used at higher layers

CDMA: Security

- Complexity of airlink makes monitoring difficult/expensive
- Encryption on airlink
 - LFSR scrambling for voice
 - CMEA for signalling message encryption
 - ORYX for data
- Authentication
 - Shared secret data
 - Keyed one-way hash function (CAVE algorithm)

GSM: Introduction

- Developed in 80's, first system in 1992
- Worldwide coverage
- 300M subscribers in 150 countries

GSM: Features

- Voice at 13kbps
- Dial-up data and fax at 9.6kbps
- SIM card
- SMS, etc...

GSM: Technical Description

- TDMA system
- 200 kHz channel, 8 time slots per channel
- 900, 1800, 1900 MHz bands
- Communication protocols based on ISDN

GSM: Security

- Authentication and identity parameters stored in SIM
- Authentication
 - Shared secret (K_i)
 - Keyed one-way hash function (A3/A8)
- Airlink encryption
 - A5

GPRS and EDGE

- Real packet switched data system
- Overlays on GSM, other TDMA systems
- Adds new communications protocols, logical channels, and network equipment entities

GPRS: Features

- Same physical layer/RF channels as GSM
- Only uses network resources when data is sent or received
- Higher speed data throughput
- Enables packet data apps in phone: (Minibrowser, WAP, etc)

GPRS Data Throughput

- 171kbps only possible using all 8 times slots with no error correction coding
- 56k/9.6k asymmetrical downlink/uplink targeted for first systems
- May launch with 9.6k or 19.2kbps downlink
- Expect low rates at launch, 56k later, higher rates even later (if at all)

GPRS: When

- Trials and initial announcements now
- Leading European carriers: this year
- Elsewhere: next year

EDGE

- Increases throughput to 384kbps
 - Depends on radio transmission conditions
- Uses additional modulation
- When service will begin
 - AT&T: mid-to-late 2001?

3G: Background

- Initiated by the ITU in 1998
- Envisioned a single global standard
- Settled on embracing multiple standards
 - Currently five incompatible standards

Motivations for 3G

- Higher capacity
- High speed data
- Competition with 2G systems

3G Hype

- 2Mbps data rates
- Multimedia video phones
- High speed Internet phone in your pocket

3G Security: Lessons from 2G

- CDMA Security
 - CMEA cracked 3/97
 - ORYX cracked 8/98
 - LFSR scrambling: too weak to bother
 - Authentication still ok...
- GSM Security
 - A5 cracked 5/97, 12/99, 4/00
 - SIM cards cracked 4/98
 - Authentication generally still ok...

3G Security: What to expect

- 3G security initially will use 2G algorithms
 - Short keys
 - Weak, “secret” algorithms
- No motivation to secure airlink
- Real security may happen with end-to-end solutions at higher layers
 - Like current generation Internet applications

3G Standards

- cdma2000
- W-CDMA

cdma2000: Introduction

- Designed for backward compatibility with existing CDMA systems
- Supports multi-mode (2G + 3G) systems in the standards
- Easier/cheaper for existing carriers to upgrade

cdma2000: Features

- Voice
- 153-307kbps packet data
- 2x capacity of existing CDMA systems
- Better standby time

cdma2000: Technical Description

- Uses same 1.25 MHz channel and spread spectrum techniques as current CDMA
- More advanced way of dividing channel capacity for high speed data
- Supports multiple 1.25 MHz carriers on forward link for higher speed data
- Communication protocols derivative from current CDMA

cdma2000: Data Rates

- Carriers want to launch with 153kbps
- Probably use asymmetrical links
 - 153kbps/14.4kbps downlink/uplink
- Single carrier cdma2000 capable of 307kbps bidirectional
- Multi-carrier cdma2000 capable of 2Mbps downlink

cdma2000: When

- End of 2000 in Korea
- Mid 2001 in North America and Japan
- Next phase (multi-carrier) a few years after that...?
- Expect multi-mode/multi-band phones
 - 2G CDMA + cdma2000
 - 2G CDMA + cdma2000 + AMPS

W-CDMA: Introduction

- Totally new system, deployed in new radio spectrum
- Next evolution of GSM
- Based on some GSM technology and concepts

W-CDMA: Features

- Voice
- 2x capacity of existing networks
- 384kbps and above packet data
- True packet switched data

W-CDMA: Technical Description

- CDMA direct sequence spread spectrum
- 2 GHz frequency band
- 5 MHz channel
- Certain similarities to cdma2000
- Protocols somewhat based on GSM
- Packet data system based on GPRS

W-CDMA: Data Rates

- Carriers targeting 384kbps
- Probably do asymmetrical 384/64kbps downlink/uplink at first
- Capable of 2Mbps downlink in future

W-CDMA: When

- Japan (NTT DoCoMo) mid 2001
- Europe mid 2002...?
- Single-mode phones for Japan
- GSM W-CDMA dual mode phones in Europe

Wireless Location Technologies

- Current technology
- FCC mandate
- New technologies
- New applications

Location: Current Technology

- Carriers supply cell site, sector and call back number for 911 calls
- Specialized equipment (wireless modem + GPS) used in specific applications
 - vehicle tracking

Location: FCC Mandate

- Carriers must:
 - Begin selling location-capable handsets by March 2001
 - Ensure at least 95% of all new digital handsets are location-capable by October 2002
- Accuracy requirements for 911 calls
 - Network-based: 100m on 67%, 300m on 95%
 - Handset-based: 50m on 67%, 150m on 95%

Location: New Technologies

- Network-based approach
 - Uses base stations to “triangulate” handset
 - Requires some new infrastructure equipment but no handset modifications
 - Accuracy: 50-200m
- Handset-based approach
 - GPS receiver in phone
 - Assisted by timing/location information from base
 - Accuracy: 5-50m

Location: New Applications

- Not just for 911: Carriers want to make money from new services
- Traffic information, navigational assistance
- Enhanced directory assistance
- Personal location
- Smart phone and Internet applications

Location: When

- US carriers need to decide on systems by October 2000
- US carriers need to start implementing service by March 2001
- European carriers also interested

Questions?
