Cellular Technologies

Mobile Device Investigations Program

Technical Operations Division - DFB
DHS - FLETC

Homeland
Security

How it works

Cell phones operate within a given area called a cell.

An ongoing call is switched as the caller moves from cell to cell.

The cells are normally arranged, in a hexagon pattern, in groups of seven.

Basic Network Design

Hexagon Grid

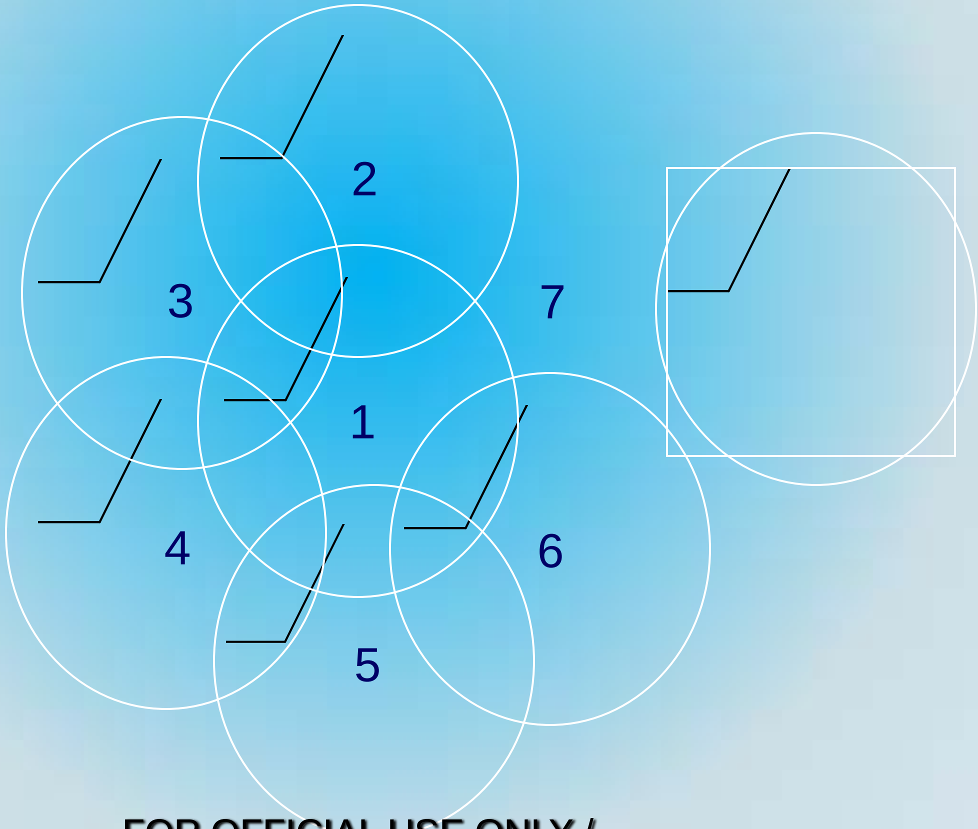
The hexagon grid design is the predominant engineering design tool in the wireless industry.

There are other design models configured in squares, circles, octagons, etc. depending on the number of cell towers in the design.

The hexagon is used because it best represents and simulates the seven tower overlapping of circles. Circles being the way radio frequencies are depicted.

Basic Network Design

Hexagon Grid



~~FOR OFFICIAL USE ONLY~~ /
LAW ENFORCEMENT
SENSITIVE

Basic Network Design

In viewing our hexagon grid we can see where frequencies overlap from one cell to the other.

It is at these points where the system determines is the best place to perform call handout.

Each tower would be 60 degrees from the other, therefore depending on which tower gives the best signal you can determine a number of things about the mobile unit.

Basic Network Design

You can estimate its distance from the tower based on power levels.

The direction in which the mobile unit is moving within the grid.

With the wireless systems GPS timing you determine the rate at which the handoffs are made.

By knowing the distance to reuse and the hand off rate you can determine the speed at which the mobile unit is traveling.

~~FOR OFFICIAL USE ONLY~~ /
LAW ENFORCEMENT
SENSITIVE

Frequency Reuse and Planning

The concept of **frequency reuse** is the central tenet to cellular design.

There are numerous seven cell frequency reuse groups in each cellular carriers Metropolitan Statistical Area (MSA) or Rural Service Areas (RSA).

Higher traffic cells will receive more radio channels according to customer usage or subscriber density.

~~FOR OFFICIAL USE ONLY~~ /
LAW ENFORCEMENT
SENSITIVE

Frequency Reuse and Planning

A frequency reuse plan is defined as how radio frequency (RF) engineers subdivide and assign the FCC allocated radio spectrum throughout the carriers market.

Frequency Coordination

Frequency Coordination is the effort by carrier RF Engineers to place base stations in a orderly fashion to minimize interference.

This is done by adhering to the Distance to Reuse ratio within their own system.

RF Engineers from the various carriers often coordinate with each other to comply with the FCC mandates.

RF Operation and Technology

Radio Frequency coverage from any base station is determined by three factors;

The height of the antenna

The type of antenna used

The Radio Frequency Power Level emitted.

This is true no matter where the antenna is placed

Basic Network Design

Fundamental Components of a Wireless System

There are five main components to a wireless network. They are:

The Mobile Unit

The Cell Base Station

The Backhaul or Fixed Network

The Mobile Switching Center

The interconnection to the Public Switched Telephone Network (PSTN)

Basic Network Design

There are two classifications of mobiles units in use today when we speak of cellular telephones and mobile devices.

The Mobile Unit

The Portable telephone or device – these are your small handsets, portable devices with network connection capabilities such as PDA's and GPS units.

The Mobile telephone or device – devices that are mounted in the locomotion device, such as installed telephones and GPS units.

Basic Network Design

Each cell has its own antenna and low power Base Station to handle the traffic within it's area.

The Cell Base Station is the physical location of some of the equipment needed to operate the wireless network, such as antennas, GPS timing systems, cell towers etc.

The size of the base station is dependent upon it's location and system needs

Basic Network Design

Each Base Station is assigned different frequencies than its neighboring Base Stations.

Carriers then reassign these frequencies to non-adjacent Base Stations and cells.

Basic Network Design

The Cell Base Station

Raw Land Sites

Rooftop Sites

Water Tank Sites

Co-located Sites

Stealth Sites

Basic Network Design

Microcells – a outdoors network base station usually on rooftops, water tanks and the like. The Base Station range of a Microcell is generally 100 meters to 1000 meters.

Picocells – the smallest, usually used indoors and intended to provide coverage for a small area. The Base Station range of a Picocell is generally less than 100 meters. Typically found in airports, e.g.

Nanocells – mobile and easily installed. Nanocells can be mounted on walls, in vehicles or outdoor weatherproof enclosure. Coverage is dependant you configuration.

Basic Network Design

The Cell Base Station - Macrocells

Basic Network Design

The Cell Base Station - Microcells

Basic Network Design

The Cell Base Station - Picocells

Basic Network Design

The Mobile Switching Center

Often called the brains of a wireless network, the MSC is responsible for switching data packets from one network path to another.

This process is called call routing.

MSC provides subscriber service information such as user registration, authentication and location updating.

Basic Network Design

The MSC provides connection to:

the Public Switched Telephone Network (PSTN) and

the Integrated Services Digital Network (ISDN) using SS7 based interconnection.

Basic Network Design

The MSC provides subscriber management functions such as;

mobile registration

location updating,

authentication

call routing to roaming subscribers.

These functions are carried out by various databases, among which are the Home Location Registry, the Visitor Location Registry, Equipment Identity Register and the Authentication Center AuC in GSM

In-Building Coverage

Due to the nature of building construction and structure it is often difficult receive and maintain RF inside.

(b)(7)e

In-Building Coverage

This method is also used to provide WiFi Hotspots.

Making a call

The cell phone identifier is transmitted along with a "request for service" signal.

Information is transmitted on the strongest reverse control channel where the MTSO checks the information and assigns it to a voice channel.

The cell site opens a voice channel and transmits a SAT which is locked onto the mobile and transmitted back to the cell site.

The information is confirmed and a mobile message is returned as a busy signal or a ringback.

4 generations of mobile technology:

1G- Analog

2G- Digital

3G- Spread Spectrum

4G- IP Packet Switched

Analog System

The first generation of mobile technology

Increased number of available channels

The cell-phone carrier received about 800 frequencies to use across a city.

The carrier divided the city into cells, about 10 square miles each, across a giant hexagon grid.

2G Digital Transmission

Increased the number of available channels within a given bandwidth.

Converted analog signal to digital allowing 3-10 digital phones to occupy the space of one single analog call.

Frequency shift keying sends data back and forth over AMPS using 2 alternate frequencies, sending digital information between the cell tower and the phone.

~~FOR OFFICIAL USE ONLY~~ / LAW ENFORCEMENT SENSITIVE

3G

Intended for true multimedia use

Increased bandwidth and transfer rates to accommodate the internet usage

Contains many cellular technologies but the 3 most common are: Code Division Multiple Access, Wideband Code Division Multiple Access, and Time-division Synchronous Code-division Multiple Access.

4G

IP packet switched networks

Mobile ultra-broadband (gigabit speed) access

Multi-carrier transmission

Paired Channels

All wireless conversations require paired channels to function.

Mobile or portable phones conduct simultaneous two-way transmissions. This is known as Full Duplex.

One channel is used for transmitting and one channel is used to receive.

Depending on the technology, the frequency may be the same or they maybe different.

Paired Channels

When the frequency is the same, this is known as 'Time Division Duplexing'.

When the frequency is not the same it is known as 'Frequency Division Duplexing'.

The only time that duplexing will not take place is when there is one-way transmissions as in SMS or streaming media.

The channel from the base station to the mobile unit is known as the downlink or forward channel. The channel from the mobile unit to the base station is known as the uplink or reverse channel.

Channel Spacing

Channel Spacing refers to the actual bandwidth space that is allocated to every wireless channel allocated out of the total spectrum amount.

The following are the standard Channel Spacing for the listed air interfaces;

AMPS - 30 KHz or 60KHZ for downlink and uplink

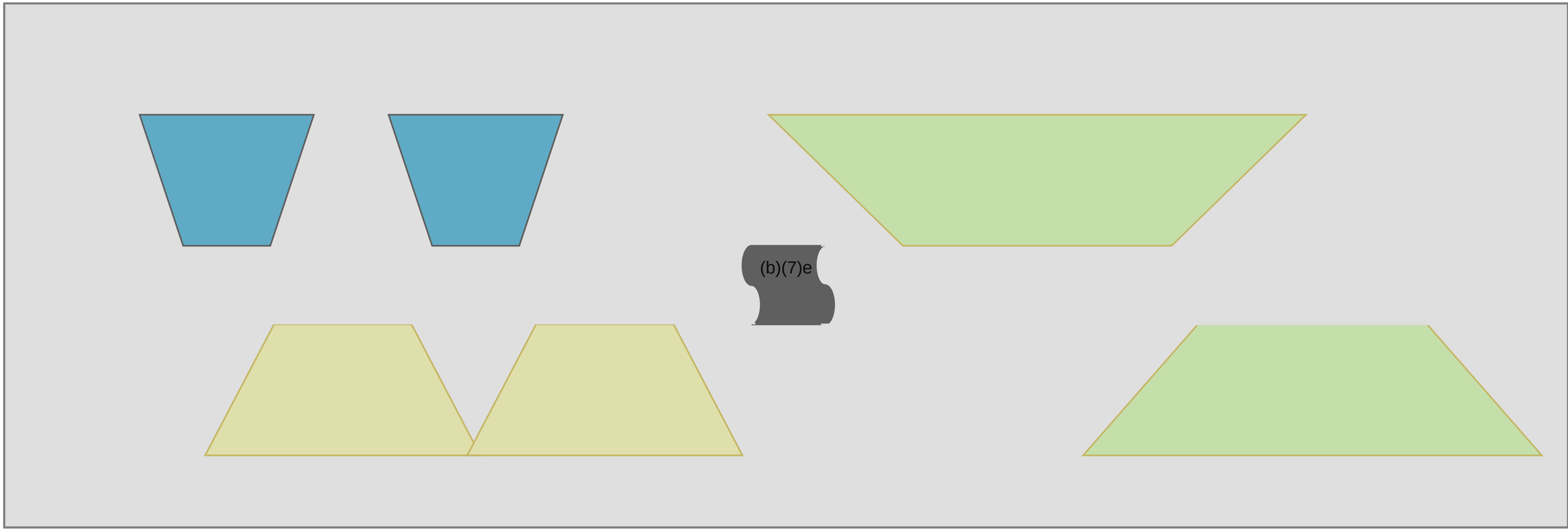
GSM - 25 KHz or 50 KHz for downlink and uplink

CDMA -Since CDMA uses spread spectrum technology it is assigned 1.25 MHz per channel. More Later!!!!

Page 34 redacted for the following reason:
- -
(b)(7)e

Three Wireless Services

Frequency Spectrum



(b)(7)e

Control Channels

The Control Channel performs numerous functions that leave evidence of a mobile user's activities.

The Control Channel handles the administrative functions and overhead of wireless systems.

Since the wireless carrier must know at all times if a subscriber is in their service area or not, constant contact with the Control Channel is necessary.

Control Channels

The Control Channel completes this task by having contact with the:

mobile unit

cell base stations

base station controllers

the mobile switching center

Some of the administrative task assigned the Control Channel are as follows:

Control Channels

Setup wireless calls, mobile originated or terminated (destined), locating mobile phones to make contact with them.

Collecting information for billing operations.

Collecting traffic measurements on base stations.

Control Channels

Autonomous mobile registration, registering the phones on the system (both home and roaming).

Initiating and assisting with call handoff.

RF Technologies

There are other technologies in use that are being incorporated into the wireless cellular and mobile device arena.

Bluetooth – The most well-known of the technologies. These devices are designed to offer wireless connectivity to devices with a wide range of capabilities.

Bluetooth enables any electrical device to wireless communicate with on the unlicensed 2.5MHz frequency. It is envisioned to replace cable connections using a single radio link.

Bluetooth is a medium to long range enabling technology.

RF Technologies

Bluetooth has a range of 10 – 100 meters and supports point to point data transfer. This data includes voice co-channels as well.

Bluetooth uses frequency hop schemes, which allows it to work in high interference areas.

(b)(7)e

Bluetooth Specs.

RF Technologies

Ultra-Wideband Wireless or UWB – UWB is a digital pulse technology designed to transmit large amounts of data over a wide spectrum of frequency bands.

UWB carries large amounts of data in distances up to 230 feet at very low power levels.

The digital pulses produced by UWB are timed precisely over the very wide spectrum at the same time.

RF Technologies

UWB can also be defined as wireless communications technology that can transmit data at speeds between 40 megabits and 60 megabits per second.

The two main difference between UWB and other narrowband or wideband systems;

The bandwidth of UWB is greater than any other current technology used for communication.

UWB is typically implemented in a carrier-less fashion, meaning it is not constricted by the RF allotment schemes.

RF Technologies

Current wireless carrier protest the use of UWB based on that argument that because they transmit on all frequencies, they may cause interference within their wireless networks.

UWB proponents argue because it transmit across such a wide spectrum and at such low power rates it will be impossible for it to interfere with current wireless networks

Access Technology

Advanced Mobile Phone System (AT&T and Verizon)

Time Division Multiple Access (AT&T, U.S. Cellular)

Global Systems Mobile (AT&T and T-Mobile)

Code Division Multiple Access (Verizon, Alltel, U.S. Cellular, & Cricket)

Universal Mobile Telecommunications Systems (AT&T - based on GSM and WCDMA)

Integrated Digital Enhanced Network (Boost & Sprint - based on GSM)

Code Division Multiple Access Technology

CDMA

Code Division Multiple Access or CDMA has it’s roots in WWII era *spread spectrum* technology.

CDMA can be implemented in several ways, two of which are *frequency hopping and direct sequencing.*

In 1985, the FCC allocated three frequency bands to spread spectrum communications.

CDMA

Conventional radio signals operate on a narrowband or a very narrow specific portion of the RF bandwidth.

Conventional radio signals are open to interference because of these narrowband widths.

A single interfering signal operating at or near its frequency can render a radio inoperable.

CDMA

CDMA uses spread-spectrum technology to minimize the problems.

Using spread-spectrum technology allows for the signals to be transmitted over a wide spectrum of the electromagnetic spectrum.

This is achieved by a specific but complex mathematical function.

The receiver must recognize the frequency-versus-time function employed by the transmitter.

CDMA

Spread-spectrum signals are distributed over a wide range of frequencies and then collected on their original frequency at the receiver.

This operation takes place inconspicuously and transparent.

Since spread-spectrum transmitter signals are so much wider they use less power.

This also allows for the use of both narrowband and spread spectrum on a single frequency.

CDMA

Spread-spectrum signals are hard to intercept and spoof.

Spoofing - falsely or maliciously introducing misleading or false traffic and messages.

This also known as Signal Exploitation.

CDMA

All spread-spectrum systems have a threshold or tolerance level of interference.

This threshold is directly related to the systems Processing Gain.

The processing gain is the ratio between the RF bandwidth and the information bandwidth.

There are two types of spread-spectrum technologies.

Frequency Hopping and Direct Sequencing.

CDMA – Frequency Hopping

Frequency hopping is the easiest spread-spectrum modulation to use.

Frequency hopping conversation requires the addition of pseudo-noise (PN) code generators.

If both receiver and transmitter know in advances what frequencies will be used this is not necessary.

CDMA – Frequency Hopping

De-hopping is achieved by a synchronized PN code generator in the local receivers frequency synthesizer.

The idea behind frequency hopping is to transmit across a broad spectrum, switching frequencies rapidly from one to another

CDMA – Frequency Hopping

The challenge is to keep both the transmitter and receiver synchronized.

An accurate clocking system and a pseudo-random generator makes this simple.

The phone creates the equivalent of a low powered noise pattern system.

CDMA – Direct Sequence

Direct Sequencing is the more practical and all digital form of spread-spectrum.

A Direct Sequence system uses a locally generated PN code to encode the data.

The local PN code runs faster and the encoded data is transmitted at the higher rate of speed.

CDMA – Direct Sequence

Carrier Modulations other than Binary Phases Shift Keying or BPSK is possible.

BSPK is the simplest and most commonly used spread-spectrum modulation.

A spread-spectrum receiver uses a locally generated replica PN code and a receiver correlator.

CDMA – Direct Sequence

Think of a conference room in the United Nations where no two people speak the same language.

All the attendees start to speak at once. This is the noise spread across the spectrum.

A person on the opposite end of the room understand you and blocks out all the other languages.

CDMA – Direct Sequence

Although the others can hear the noise they can not understand what is being said.

Now envision the same conversation being held but you have to move about the room at the right time to hear and understand what is being said.

You are only receiving little bits of information at a time that you must then decode.

CDMA – Spread Spectrum Advantages

Interference Immunity – Spread Spectrum radios are inherently more noise immune than conventional radios.

Multichannel Capability – Spread Spectrum radios offer the ability to have multiple channels, which can be changed dynamically through software

CDMA Basics

CDMA networks have pilot channels which carry no data but are used by the subscriber’s mobile unit to acquire the system and assist in the soft handoff process.

A separate pilot channel is transmitted for each sector of a cell site and is uniquely identified by it’s own PN code, just like other users

CDMA Architecture – Soft Handoff

Hard Handoff are defines as the milliseconds in which a mobile unit is passed from one cell to the other and there is no connection.

Soft Handoffs in CDMA systems work differently. When a unit is about to leave one cell area and travel to another it seeks out the strongest cell signal it can find.

This information is sent by the mobile unit to the MSC. The MSC verifies the information and connects to the unit to the cell while it is still connected to the previous cell.

CDMA Architecture – Soft Handoff

Once the connection is secure and complete the MSC disconnects the mobile unit from the old cell and the handoff is complete.

Hard Handoffs are known as break-before-make connections.

Soft Handoffs are known as make-before-break connects

CDMA Architecture – Soft Handoff

The sequence of events on a soft handoff are;

After a users completes a call the mobile unit continually scans to determine if it is in range of another cell that has a stronger signal.

When the mobile unit determines it has located a stronger signal it now knows that it is in another cell's coverage area.

The mobile unit transmits a control message to the MSC, stating it has entered another cell's coverage area. The mobile unit identifies the cell to the MSC.

The MSC initiates the handoff by establishing a link between the mobile unit and the new cell site. The MSC maintains a link between the old cell site and the mobile unit.

CDMA Architecture – Soft Handoff

While in the transition region between the two cells the mobile unit is serviced by both cell sites.

The original link will only be disconnected when the mobile unit is firmly connected to the new cell site.

CDMA – Spread-Spectrum Operations

Two criteria must be met to qualify as a Spread Spectrum Signal;

1. The signal bandwidth must be wider than the information bandwidth.

2. Some code or pattern, other than the data to be transmitted, determine the actual on air transmit bandwidth

Time Division Multiple Access Technology

TDMA

Time Division Multiple Access or TDMA is a digital transmission technology that allows a number of users to access a single radio frequency (RF) channel without interference by allocating unique times slots to each users within the channel.

TDMA multiplexes three signals (from multiple users) over a single channel.

TDMA

In 1989 the Telecommunications Industry Association and the Cellular Telecommunications & Internet Association chose TDMA over FDMA as the standard to use for 800 Mhz cellular market and the emerging 1.9Ghz markets.

With growing competition between CDMA, GSM and TDMA the CITA decided to let the carriers make their own technology selection

TDMA – How It Works

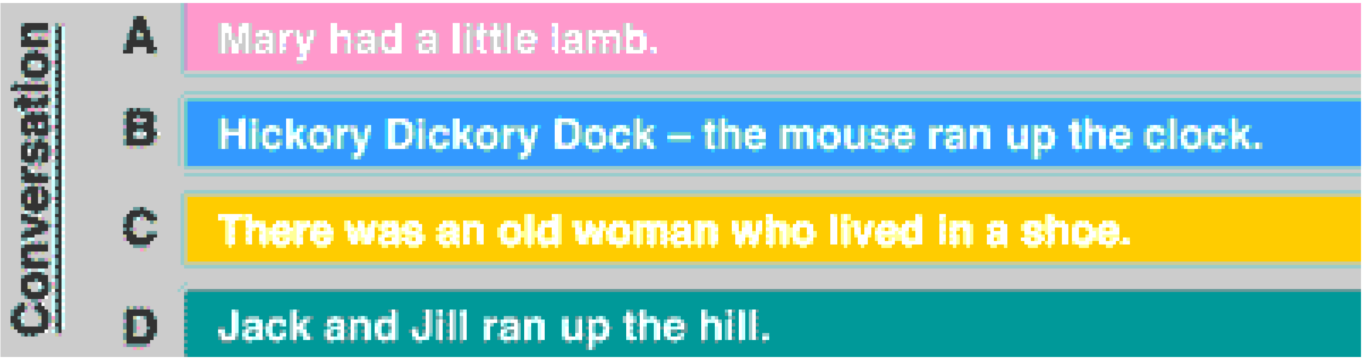
TDMA takes the digitized audio signal and transmits them on a RF in very short bursts, no longer than milliseconds typically 10 msec.

Audio packets are assigned a time slot on RF with audio burst portions of other communications.

It allocates a channel frequency for a short time and then moves to another channel.

TDMA – How It Works

Consider having four conversations going on at one time on four different channels.



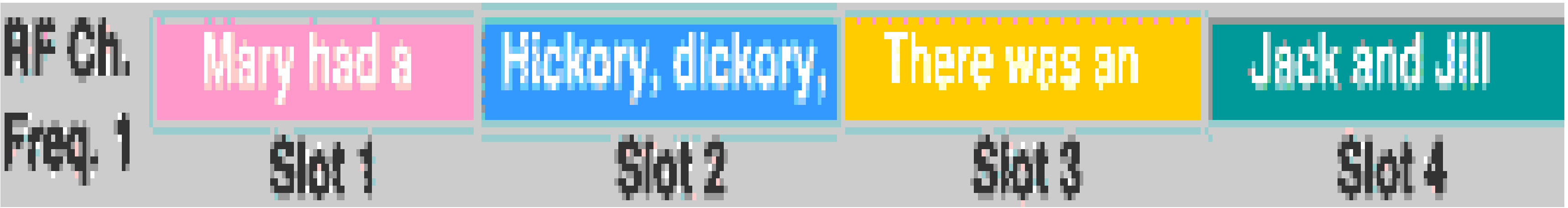
A Mary had a little lamb.

B Hickory Dickory Dock – the mouse ran up the clock.

C There was an old woman who lived in a shoe.

D Jack and Jill ran up the hill.

TDMA – How It Works



RF Ch. Freq. 1	Mary had a	Hickory, dickory,	There was an	Jack and Jill
	Slot 1	Slot 2	Slot 3	Slot 4

TDMA – How It Works

The IS-54 and IS-136 in effect tripled the capacity of cellular frequencies by dividing the 30 Khz channel, allowing more users per channel.

Today TDMA and other standards allow for more slotting giving rise to more users on the systems.

Proponents of TDMA such as AT & T Cingular state they will have the ability to carry 40 or more conversations on a single channel in the near future.

Extended TDMA or ETDMA

The weakness in TDMA is the waste of bandwidth, which in effect is a waste of possible on air time.

ETDMA uses a control channel to detect and assign a channel dynamically when voice activity is detected.

When ETDMA determines there is no conversation or there is a pause it reassigns the channel to a party having a conversation

Extended TDMA or ETDMA

Consider the pace in which this presentation is being given.

ETDMA uses these natural pauses to transmit the short millisecond burst of information.

TDMA – Digital Advantages

Digital technology is now the standard for public telephone systems.

Analog calls are converted into digital form for transport across the telephone systems back bone.

There are a number of advantages that digital has over analog transmissions. They are;

TDMA – Digital Advantages

It economizes on bandwidth.

It allows easy integration with personal communication systems (PCS) devices.

It maintains superior quality of voice transmissions over a distance.

It’s difficult to decode.

It can use lower average transmitter power.

It enables smaller and less expensive individual receivers and transmitters.

It offers voice privacy.

TDMA – Disadvantages

In TDMA systems each user has a predefined time slot.

If the user enters into a cell area in which all the time slots are allocated he/she may not be able to complete a call.

However, most phones and services today are multi-spectrum. If the TDMA is overcrowded, the carrier will flip to another spectrum seamlessly.

Check your own phone. You will probably find it is multi-spectrum.

Global System for Mobile Communication Technology

GSM Technology

Global System for Mobile Communication or Groupe Special Mobile

To standardize cellular communication thoughout Europe

Prior to it’s development there were a number of incompatible systems served Europe

GSM Technology

With GSM European companies agreed to a set of standards

GSM is an open source system

Allows access to code

All operate based on these standards

GSM Technology

GSM operates on the 900 MHz, 1800 MHz and 1900 MHz

GSM uses Digital Communication System or DCS 1800 and is the worlds main 2G standard

When the FCC issued 1900 MHz to PCS in the United States it was based on GSM

DCS 1900 is considered the GSM standard for North America and is called North American GSM.

GSM Technology

GSM is now a worldwide standard

GSM uses Time Division Multiple Access or TDMA technology as their air interface standard

TDMA has limited capabilities

GSM is strictly controlled by a Memorandum of Understanding (MOU)

GSM Architecture and Subsystems

Open architecture according to the Open Systems Interconnect or OSI model for layers 1,2, and 3.

Layer 1 – Physical Layer
Layer 2 – Data Link Layer
Layer 3 – Network Layer

GSM carriers can go to any GSM manufacturer

GSM Architecture and Subsystems

GSM uses voice coders/decoders or vocoders

Vocoders are firmware and chips sets that digitize the human voices

Voice that is sampled and channelized is housed in the vocoder

GSM Architecture and Subsystems

Vocoders packetize the sample of the human speech and transmits it through the handset to the base station

Distant-end vocoders decode the pulses and routes the call to the MSC

A full-rate vocoder allows for eight (8) conversations over a channel

Half-rate vocoders samples at half the rate of speed and allows for more effective use

GSM Architecture and Subsystems

By standard the GSM network is divided into four (4) subsystems

- The Base-Station Subsystem
- The Network Subsystem
- The Operation and Support Subsystem
- The Mobile Station Subsystem (The Mobile Unit)

GSM Subsystems – Base Station Subsystem

The Base-Station Subsystem is comprised of:

The Base-Station Controller[1] (BSC) -part of the wireless system's infrastructure that controls one or multiple cell sites' radio signals

Performs radio signal management functions for base transceiver stations, managing functions such as frequency assignment and handoff.

The BSC acts as a front-end processor for the MSC.

[1] http://www.mobiledia.com/glossary/35.html

GSM Subsystems - Base Station Subsystem

Base Transceiver Station[2] (BTS) - The name for the antenna and radio equipment necessary to provide wireless service in an area.

Also called a base station or cell site.

Defines a cell coverage area

Controls the radio link protocols with the mobile station.

[2] http://www.mobiledia.com/glossary/37.html

GSM Subsystems - Base Station Subsystem

The Air Interface[3] - operating system of a wireless network.

Radio-frequency portion of the circuit between the cellular phone set and the active base station.

As a subscriber moves from one cell to another the active base station controller changes periodically

Each changeover is the same as a handoff.

[3] http://www.mobiledia.com/glossary/17.html

GSM Subsystems - Network Subsystem

The Network Subsystem is in affect the Mobile Switching Center

The central part of the network.

The MSC provides connection to the Public Switched Telephone Network (PSTN) and the Integrated Services Digital Network (ISDN) using SS7 based interconnection.

GSM Subsystems - Network Subsystem

The MSC provides subscriber management functions such as;

mobile registration
location updating,
authentication
call routing to roaming subscribers.

The Home Location Register (HLR) and the Visitor Location Register (VLR) are located within the MSC.

Basic Network Design

Home Location Registry – HLR

HLR is a database that contains records of all subscribers.

HLR is used to identify and verify a subscriber on network

The record of what services the subscriber has is kept here

GSM Subsystems - Network Subsystem

The HLRs database contains different types of information;

Every Subscriber Identity Module (SIM) card issued by the Mobile Phone Operator.

The SIM has a unique identifier called the International Mobile Subscriber Identifier or IMSI.

IMSI is a primary key to each HLR.

GSM Subsystems - Network Subsystem

The SIM card keeps track of all Mobile Subscriber Integrated Services Digital Network Number or MSISDNs.

These are the telephone numbers that have called the mobile unit.

It is used for making and receiving voice calls and SMS.

The MSISDN can have a second number for receiving data and fax.

Each MSISDN is also a primary key in the rational database.

GSM Subsystems - Network Subsystem

Examples of other data stored in the HLR in a SIM record;

GSM services the subscriber has requested or been given

General Packet Radio Service or GPRS settings allow the subscriber access to packet services

Current location of the subscriber; providing a Serving GPRS Support Node (SGSN- packet roaming)

Call Divert or Call Forwarding settings

GSM Subsystems - Network Subsystem

In theory the HLR data is stored for as long as the subscriber is with the mobile phone operator.

The HLR is a systems that directly receives and processes Mobile Application Part (MAP) transactions and messages.

If the HLR fails the system fails. The HLR manages the Location updates as mobile phones roam.

The HLR is now a powerful server more so than telephone switch hardware

GSM Subsystems - Network Subsystem

HLR connects and interacts with a number of other components on the system

- The Gateway MSC for handling incoming calls
- The VLR for handling request from mobile phones to attach to the network
- The SMSC for handling incoming SMS
- The voice system for delivering notification to the mobile phone that a message is waiting

GSM Subsystems - Network Subsystem

The main function of the HLR is to manage the movement of SIMs and mobile phones by;

Managing and updating the position through location areas identified with a LCA. Updates the users location

Send subscriber information to the VLR when the users roams

Act as a go between for the GMSC or SMSC with the VLR - receive text or voice messages

Remove the user of the VLR when he/she has left that roaming area

GSM Subsystems - Network Subsystem

Visitor Location Register (VLR) Database - stores information about all the mobiles that are currently under the jurisdiction of the MSC. Some of this information include;

The most important is the current Location Area Identity or LAI.

LAI identifies under which BSC the Mobile Station is currently

This information is vital in the call setup process.

GSM Subsystems - Network Subsystem

Visitor Location Register (VLR) Database - stores information about all the mobiles that are currently under the jurisdiction of the MSC. Some of this information include

Whenever an MSC detects a new MS in its network, it creates a new record in the VLR,

Updates the HLR of the mobile subscriber, apprising it of the new location of that MS.

GSM Subsystems - Network Subsystem

VLR is a temporary database of the subscribers that have roamed into the area

Each base Station is served by only one VLR

No one subscriber can be on more that one VLR at any given time.

VLR are either linked directly to the V-MSC or are integrated with a special software interface.

GSM Subsystems - Network Subsystem

Relevant data stored there are;

IMSI – the subscriber's identity number

Authentication Data

MSISDN – the subscriber's phone number

GSM services the subscriber has access to

Access Points (GPRS) that are subscribed to, and

The HLR address of the subscriber

GSM Subsystems - Network Subsystem

The VLR also connects to;

The Visited MSC (V-MSC), to pass data needed for certain procedures i.e., authentication and call setup

The HLR to request data for the mobile phones attached to it’s service area

Other VLR to transfer data as the MS roams from one area to the next accessing new VLRs

GSM Subsystems - Network Subsystem

The VLR primary functions are

To inform the HLR that a MS has arrived in the particular area covered by the VLR

To track where the subscriber is within a VLR area when it is not active

To validate (allow/disallow) which services the subscriber may use

GSM Subsystems - Network Subsystem

The VLR primary functions are:

To allocate roaming numbers during the process of incoming calls

To purge the subscribers record if he/she becomes inactive while in its area

To delete the subscribers record when the subscriber moves into another VLRs area based on the rules of the HLR. The VLR is reset daily

GSM Subsystems - Network Subsystem

Other functions associated with the Network Substation are:

The Authentication Center - provides authentication of the MS and encryption of services

The Equipment Identity Register (EIR) – Using the IMSI, the EIR keeps track of valid MS. If one is lost, stolen or service discontinued it is blacklisted on the EIR

GSM Subsystems - Network Subsystem

Other functions associated with the Network Substation are: (CONT.)

Billing Center (BC) – produces the tolls Generated by the VLR and HLR for each subscriber and the roaming data

Short Message Service Center (SMSC) – the sending and receiving of short messages

GSM Subsystems - Network Subsystem

Multimedia Messaging Center – the sending and receiving of images, video, audio or any combination of them

Voicemail System (VS) – records and stores voice messages

(b)(7)e

This systems works with conference calling feature

GSM Subsystems Operations and Support Subsystem

The Operations and Support Subsystem – the command and control center used to monitor the GSM system.

If there is a particular failure in the OSS can identify the problem and determine what course of action is needed

GSM Subsystems - Mobile Station Subsystem

The Mobile Station (Mobile Phone) Subsystem – also known as the User Equipment. GSM phones are segmented for a number of reasons.

The MS has four main components:

The Mobile Terminal

The Terminal Equipment

Terminal Adapter

Subscriber Identity Module or SIM

GSM Subsystems - Mobile Station Subsystem

The Mobile Terminal or Handset – identification information is held on the SIM card

The handset's main functions are to transmit, receive, encode and decode voice transmissions.

The SIM card contains the GSM operating program, customer and carrier specific data.

GSM Subsystems - Mobile Station Subsystem

Programmed at the sales office, the SIM card provides authentication, information storage, subscriber account information and data encryption.

SIM cards and handsets are interchangeable.

SIM card will recall all information stored on it, including programmed numbers, SMS saved, ring tones, Contact list and the like.

GSM Subsystems - Mobile Station Subsystem

Some of the Network Specific items used to authenticate and identify subscribers on the Network are;

Integrated Circuit Card ID or ICCID – International ID, stored in the SIM card and stamp of the card

International Mobile Subscriber Identity or IMSI- Mobile operators connect mobile phone calls and communicate with their market through SIM cards

Local Area Identity or LAI – Networks are divided into local areas with a unique number. When you travel from one area to another the unique number is logged in the SIM.

GSM Subsystems - Mobile Station Subsystem

Operator Specific Emergency Number – like “112” or E911 these numbers (5) are programmed into the SIM

Short Message System Center Number or SMSC number – the number used to sent text messages

Service Providers Name or SPN – the telecommunications service providers name and ID

Service Dialing Numbers or SDN – numbers associated with the service provider

GSM Subsystems - Mobile Station Subsystem

Advice of Charges – what are the parameters in which the account will charged?

Value Added Services or VAS – what type of service (i.e. Internet access) is associated with the account?

Depending on storage capacity any type of data may be stored.

In Europe some subscribers store their medical records on their SIM card.

Any data!!!!!!!

GSM Subsystems - Mobile Station Subsystem

Authentication Key or Ki – a 128-bit value used to authenticate the SIM to the mobile network. Assigned by the operator the Ki is contained on the service providers HLR.

GSM was designed from the start with security in mind. The SIM card aids in this security, making fraud on a GSM network unlikely.

Using a series of secret keys and algorithms thwarted cloning of GSM devices.

GSM Subsystems - Mobile Station Subsystem

In GSM Call Handoff, or Call Handover is different in that it is mobile device assisted.

The mobile phone continually monitors base stations in vicinity measuring the strength in the MSC.

The six best prospects are sent back to the MSC who then determines when the handoff will be conducted.

GSM

Often described as a true Intelligence Network, GSM is called the first true wireless network because;

It has an open, distributed architecture

The separation of switching and service control functions

Full use of SS7 as the signaling infrastructure

Its clearly defined and specified interfaces

The nature of its IN structure

General Packet Radio Service (GPRS) and Enhanced Data Rates for Global Evolution (EDGE - CDMA), are 3G GSM based standards

GSM Adjunct Systems

GSM standards define that certain Adjunct or Secondary Systems work with GSM technology. Some of note are;

The Gateway MSC or GMSC – The purpose of which is to query the HLR and determine the location of the subscriber. Calls from another network i.e. PSTN will first go through the GMSC.

Short Message Service Center or SMSC – The node that stores and forwards short messages to and from the mobile station.

GSM Adjunct Systems

The Equipment Identity Register or EIR – identifies what equipment i.e. handsets are acceptable in a GSM Network

The Interworking Function or IWF – used for circuit switched data and fax services and is basically a modem bank

GSM v CDMA

There is a debate as to how long TDMA or IS-136 cell phones will be in existence. GSM and CDMA system now dominate the market.

Both work well on their own as well as with each other.

Some CDMA mobile units use a Removable – User Identity Module or R-UIM which is similar to a SIM. There are Dual R-UIM that allow for use in both GSM and CDMA units.

Both seem positioned to be in place for a period of time.

Integrated Digital Enhanced Network

*i*DEN

Integrated Digital Enhanced Network Technology or *i*DEN

In 1987 Nextel was formed and began to change the Specialized Mobile Radio (SMR) market.

Originally called Fleet Call, Nextel purchased SMR licenses around the country to form a national network.

*i*DEN

The technology was developed by Motorola who provided trunked radio and cellular telephone.

In 1990 Nextel applied for and received permission from the FCC to create Enhanced Specialized Radio Service (ESMR) in six major markets.

Nextel chose as its air interface TDMA technology.

*i*DEN

Introduced in 1994, *i*DEN combined two-way radio, digital cellular, messages services with acknowledgment and wireless data into a single system.

*i*DEN uses Vector Summed Excited Linear Prediction (VSELP) vocoders, which compresses large segments of voice into smaller packets.

VSELP uses Forward Error Correction so packets do not become corrupted.

The use of VSELP and FEC allows for six audio paths on one RF channel.

*i*DEN

One of the unique feature is the Push-to-Talk or Direct Connect feature.

As of 2003 Direct Connect has been offered nationwide with no roaming.

This dispatch feature is managed by separating talk groups into fleets.

Each subscriber has an ID called the Fleet Member Identifier and identifies a user within a fleet.

*i*DEN

*i*DEN network work in much the same way and has the same equipment as other cellular networks, but are often identified differently.

The basic structure of an *i*DEN network is as follows:

*i*DEN

Enhanced Base Transceiver System – provides the radio frequency link between the network and the landline (PSTN).

Mobile Data Gateway – the interface between the Internet (WWW) during Data Packet activity.

Dispatch Application Processors – the call managers within the network.

*i*DEN

Metro packet Switch – a subsystem that connects the Enhanced Base Transceiver System to the Dispatch Application Processor and packet Duplicators.

Mobile Switching Center – GSM based mobile phone system that provides interconnect service.

*i*DEN

Digital Access Cross Connect Switch – connect point for T1/E1 lines between *i*DEN equipment and the external transport facilities.

Base Site Controller – manages the inter-connect between the Enhanced Base Transceiver System and other network devices

*i*DEN

Operations and Maintenance Center

Establishes, maintains and collects information about the network for presentation to the system operator.

*i*DEN

*i*DEN has another distinct feature in its service system. The existence of two sets of Home Location Register and Visitor Location Register.

One set operates and maintains information on the digital services provided as in authentication, services allowed, timing and the like.

*i*DEN

The second, referred to as the *i*-HLR and the *i*-VLR. This system keeps track of the Dispatch Call function or Push-to-Talk..

It should be importantly noted that when requesting information about activity conducted on the Call Dispatch side of the network you must be specific and request the proper data.

Page 135 redacted for the following reason:
- -
(b)(7)e

*i*DEN

In 2004 Sprint and Nextel merged to form Sprint/Nextel.

On 2 November 2005, U.S. telecom carrier Sprint Nextel and four cable companies — Advanced/Newhouse Communications, Comcast, Cox Communications and Time Warner Cable — announced plans for a joint venture.

The partners will conduct joint marketing and work on integrating with each other's back-office systems to enable a "quadruple play" of voice, video, data and high-speed Internet services over cable and wireless devices.

*i*DEN

There is considerable discussions and speculation in the telecom community about the future of *i*DEN.

Because of its network nature Sprint/Nextel agreed to work with cities and others using the radio broadcast frequencies to address interference and other issues.

As of this date these concerns are being addressed and the outcome unclear.

Personal Communication Service

Personal Communication Service

Personal Communication Service or PCS is referred to as 2G wireless service.

The FCC has defined PCS as radio communication that encompasses mobile and fixed communication to individuals and businesses that can be integrated with a variety of competing networks.

Personal Communication Service

PCS refers to integrated networks as the ability to connect to PSTN, WiFi and Worldwide Interoperability for Microwave Access (WiMax) systems.

This can be anything from point to point to full cellular access.

Personal Communication Service

Some other ways to define the mobility of PCS networks;

Personal Mobility - the ability of users to access any telecom service at any terminal based on personal identifiers, the networks ability and users profile

Terminal Mobility – the wireless subscriber units ability to access services from different locations while in motions

Personal Communication Service

Service Mobility – the use of vertical features provided by landlines, users at remote locations or while in motion.

PCS refers to services that are user specific as opposed to location specific.

PCS is referred to as follow me services.

Personal Communication Service

PCS was the first wireless network from its inception. Upon obtaining licenses PCS carriers were allowed to choose their air interface, thus we have TDMA, CDMA and GSM carriers.

PCS uses the same type of equipment that cellular services use with the difference being that more PCS base stations are need to cover the same geographic area.

Personal Communication Service

There are two types of PCS services; Narrowband and Broadband PCS.

Narrowband, using the 3MHz radio spectrum was used primarily for data transmissions.

These services were paging an short message systems.

Personal Communication Service

Broadband PCS is used for multimedia transmissions such as voice, data. Internet, SMS, image and in the future full motion video.

This obviously requires more channel capacity and is set aside on the 140 MHz radio spectrum.

Personal Communication Service

The major carriers include AT & T/Cingular, Verizon Wireless, T-Mobile, Sprint PCS (Nextel), Alltel Mobile and U.S. Cellular.

There are hundreds of regional PCS Carriers that can be found at

http://www.wirelessadvisor.com/resources/wireless-carriers-a-b

Personal Communication Service

Only Sprint uses PCS as the primary technology

All other major carriers provide PCS as a secondary service.

- For example, if an Alltel user can not find a CDMA tower (or, all channels are taken), the system will automatically and seamlessly interface with a PCS tower.

QUESTIONS