Code Division Multiple Access Technology

Mobile Device Investigations Program

Technical Operations Division
DHS - FLETC

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

Two problems exist with using conventional wireless i.e. radio communications.

1. Frequencies operating near on at the same narrowband will cause interference.

2. A constant frequency signal is easy to intercept.

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 intercept and spoof.

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

The is 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.

Remember tuning the dial and picking up a cell phone call?

CDMA – Frequency Hopping

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.

Done randomly it is nearly impossible for someone to eavesdrop or jam the signal.

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.

Other devices do not see a phone transmitting over spread-spectrum systems.

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 like 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

The desired information can be voice, data, video and so forth.

A spread-spectrum correlator is a very special matched filter that responds only to a PN code that matches its own.

A spread-spectrum correlator can be tuned to different codes by simply changing its local code.

It will respond only to identical PN codes matching its own.

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 – Direct Sequence

(b)(7)e

CDMA – Spread-Spectrum Operations

Spread-Spectrum signals use fast codes that run at a rate many times faster than the information bandwidth or data rate.

These special codes are called Pseudo Random Noise Codes or Walsh codes.

The uses of these special codes make signals appear wideband and noise like.

CDMA – Spread-Spectrum Operations

The spread-spectrum signals are hard to detect on narrow-band equipment.

The information bandwidth can be voice, data, video or image.

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

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 is an American Standard that was developed by Qualcomm.

It was originally developed for the battlefield because it is very hard if not impossible to intercept due to their spread spectrum nature.

CDMA is now defined by a number of standards, some of which are IS-95, J-STD-008 (PCS) and CDMA 2000.

CDMA Basics

A unique code is assigned to all digital speech bits and the signals spread across the broad spectrum of the RF.

Each CDMA base station can use the same 1.25 MHz carrier at the same time.

There are a maximum of 64 Walsh noise codes per 1.25MHz in a CDMAOne system.

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

CDMAOne and CDMA 2000

CDMA refers collectively to three CDMA standards that were the first formal specifications assigned to the technology;

1. IS-95A
2. IS-95B
3. J-STD-008

CDMAOne

CDMAOne standards have evolved in the complexity and effectiveness.

Earlier versions (IS-95A&B) had issues with voice quality, data throughput and were limited in the methods in which they transmitted data.

IS-95B and J-STD-008 allowed for Integrated Service Digital Network or ISDN to be used. More advanced calling features were accessible

CDMA 2000

CDMA 2000 falls under the specification known as IS-2000 as is backward compatible with earlier versions.

CDMA2000 is a 3G specification, which allows for multidata platform usage.

More on Both Later!!!!

CDMA Architecture

Personal Communication Services or PCS carriers such as Verizon Wireless and Sprint PCS has shown that CDMA systems can handle as much traffic as any other standard reliably

CDMA Architecture – Power Control

CDMA base stations control the power of all mobile devices within their coverage area.

All mobile signals must arrive at the base station at the exact power level.

Power Control is a required operational parameter of a CDMA System.

CDMA Architecture – Power Control

What happens if a mobile unit near the base has a higher power level than one far away? – Power Throttle

Power control is necessary to maintain system capacity.

A benefit is reduced cost at the base station and longer battery life for the mobile unit.

CDMA Architecture – Rake Receivers

Rake receivers exist in both the mobile unit and the BTS transceivers.

Rake receivers derive their name from the fact that they look like lawn rakes.

The signal from each is combined to generate a composite signal.

CDMA Architecture – Rake Receivers

There are four rakes in a transceiver and three rakes in a mobile unit.

The strongest signal is combined with the multipath (weaker) signal of the other rakes to form this composite signal.

The multipath signals are added to the direct signal to obtain the cleanest signal. This process is known as diversity combining.

CDMA Architecture – Soft Handoff

Hard Handoff are defined 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

CDMA systems requires a GPS receiver and antenna at every cell base.

The GPS antennas synchronize all the cells to one timing source, which is the GPS.

This is absolutely necessary for the soft handoff process.

This handoff is also known as mobile directed handoff.

"The daring Young Man On the Flying Trapeze"

CDMA Architecture – Soft Handoff

The sequence of events on a soft handoff are;

1. 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.

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

CDMA Architecture – Soft Handoff

3. 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.

4. 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

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

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

CDMA Architecture – Cell Breathing

CDMA is a noise-generated technology. As such the system must monitor its noise floor or ambient noise.

To much noise will cause interference leading to degraded service or dropped calls.

CDMA systems are equipment with a protocol that allows the system to adjust in these situations.

CDMA Architecture – Cell Breathing

When a CDMA base station determines that there is to much noise or interference it begins the process of powering down the cells and the mobile units under control down.

This lowers the noise level and shrinks the cells coverage area.

CDMA Architecture – Cell Breathing

If it is determined that the mobile unit is about to lose the signal it connects the mobile unit to another cell or drops the call if it is unable to do so.

When the MSC determines that the noise level has subsided it powers the entities back up increasing the coverage area.

This activity is what is described as the cell breathing process.

Benefits of CDMA

CDMA has increased capacity over the older systems such as TDMA and AMPS.

Simpler RF engineering because of the N=1 reuse pattern. This reduces the time and effort required to expand or modify a CDMA system.

Increased performance over the air interface which is the weakest link in wireless systems.

Benefits of CDMA

Lower transmitted power levels. Power adjustments are constantly being made to the system and mobile units. Costing less due to less power usage.

Greater security due to the encoding (spread-spectrum) of the signals.

Enhanced performance and voice quality due in part to the soft handoff capabilities.