CDMA System Analysis II

Authors: Timothy X Brown, Silvana Susi, Sukhjinder Singh
University Of Colorado, Boulder

Purpose
This experiment allows the student to gain a meaningful understanding of the IS-95 system specifications by observing the relationship between the different group categories of the PN Offset: Active Set, Candidate Set, and Neighbor Set, and the Layer 3 messages between the mobile and the base station while the terminal is active in the system.

Equipment
- RSAT-2000 CDMA/AMPS equipment
- A Portable Computer or desktop with OptimEyes Software

Introduction

IS-95
Interim Standard 95 (IS-95) is a U.S. digital cellular system based on CDMA that allows each user within a cell and in adjacent cells to use the same radio channel. Each IS-95 channel occupies 1.23MHz of spectrum in each one-way link, which corresponds to 41 30kHz AMPS channels.¹

The user data is spread to a channel chip rate of 1.2288MHz. IS-95 uses a different modulation and spreading technique for the forward and reverse links. On the forward link, the base station simultaneously transmits the user data for all mobiles in the cell by using different spreading sequence for each mobile. The user data is encoded, interleaved, and spread by one of sixty-four orthogonal spreading sequences (Walsh functions). To avoid interference, all signals in a particular cell are scrambled using a pseudorandom sequence of length $2^{15}$ chips.² CDMA base stations transmit information in four logical channel formats: pilot channels, sync channels, paging channels, and traffic channels.

On the reverse link, all mobiles respond in an asynchronous fashion. The user data is encoded, interleaved, and then blocks of 6 bits are mapped to one of the 64 orthogonal Walsh functions. Finally, the data is spread by a user specific code of 42 bits (channel identifier) and the base station pseudorandom sequence of length $2^{15}$ chips. The reverse channel is organized in access channels and traffic channels.³

² Ibid., 520.
³ Ibid., 520 – 521.
At both the base station and the terminal, Rake receivers are used to resolve and combine multipath components, in order to improve the link quality. In IS-95, a three-finger Rake receiver is used at the base station.\(^4\)

**IS-95 Logical Channels**

Pilot Channel: is used by the base station to provide a reference for all mobile stations. It provides a phase reference for coherent demodulation at the mobile receiver to enable coherent detection. It is assigned the Walsh code \(W_0\). The pilot signal level for all base stations is kept about 4 to 6 dB higher than the traffic channel with a constant signal power. The pilot is used for comparisons of signal strength between different base stations to decide when to perform handoff. The pilot signals from all base stations use the same PN sequences, but each base station is identified by a unique time offset. These offsets are in increments of 64 chips to provide 512 unique offsets.\(^5\) Each terminal segregates the set of PN Offset values (and implicitly the set of base stations) in a system into four categories:\(^6\)

- The **active list** contains base stations currently used for traffic channel transmissions. In a soft handoff condition, there is more than one base station in this list.
- The **candidate list** consists of base stations classified by the terminal, on the basis of measured signal quality, as available for traffic channel transmissions.
- The **neighbor list** is a set of nearby base stations that could soon be available for handoff.
- The **remaining list** contains the base stations that are not in any of the other categories.

Sync Channel: is assigned the Walsh function \(W_{32}\) and is used with the pilot channel to acquire initial time synchronization. The Sync channel message parameters are: System Identification (SID), Network Identification (NID), Pilot short PN sequence offset index, Long-code state, System time, Offset of local time, Daylight saving time indicator, and Paging Channel data rate (4.8 or 9.6kbps).\(^7\)

Paging Channel: there are up to seven paging channels that transmit control information to the terminals that do not have calls in progress. The paging

channels are assigned the Walsh functions $W_1$ to $W_7$. Some of the messages carried by the paging channel include:

- **System Parameter message**: such as base station identifier, the number of paging channels, and the page channel number.
- **Access Parameters message**: parameters required by the mobile to transmit on an access channel.
- **Neighbor List Message**: information about neighbor base station parameters, such as the PN Offset.
- **CDMA Channel List message**: provides a list of CDMA carriers.
- **Page message**: provides a page to the mobile station.
- **Channel Assignment message**: to inform the mobile station to tune to a new frequency.
- **Data Burst message**: data message sent by the base station to the mobile.
- **Authentication Challenge**: allows the base station to validate the mobile identity.

**Access Channel**: is used by a terminal without a call in progress to send messages to the base station for three principal purposes: to originate a call, to respond to a paging message, and to register its location. Each base station operates with up to 32 access channels. The messages carried by the access channel include:

- **Registration Message**: sends to the base station information necessary to page the mobile, such as: location, status, and identification.
- **Order message**: to transmit information such as base station challenge, mobile station acknowledgement, local control response, and mobile station reject.
- **Data Burst message**: user-generated data message sent by the mobile station to the base station.
- **Origination message**: allows the mobile station to place a call—sending dialed digits.
- **Page Response message**: used to respond to a page.
- **Authentication Challenge Response message**: contains necessary information to validate the mobile station’s identity.

**Forward Traffic Channel**: channels not used for paging or sync can be used for traffic. Thus, the total number of traffic channels at the base station is 63.

---

minus the number of paging and sync channels in operation at the base station. Information on the forward traffic channel includes the primary traffic (voice or data), secondary traffic (data), and signaling.\textsuperscript{12} When the forward link is used as signaling, the following are some of the typical messages:\textsuperscript{13}

- Order message: similar to the order message in forward traffic channel.
- Authentication Challenge message: used to prove the identity of the mobile when the base station suspects its validity.
- Alert with Information message: allows the base station to validate the mobile identity.
- Data Burst message: data message sent by the base station to the mobile.
- Handoff Direction message: provides the mobile with information needed to begin the handoff process.
- Analog Handoff Direction message: tells the mobile to switch to the analog mode and begin the handoff process.
- In-Traffic System Parameters message: updates some of the parameters set by the System Parameters message in the paging channel.
- Neighbor List Update Message: updates the neighbor base station parameters set by the Neighbor List message in the paging channel.
- Power Control message: tells the mobile how long the period is or what threshold is to be used in measuring frame-error statistics that will be sent by the mobile.
- Mobile Registration message: informs the mobile that it is registered and supplies the necessary system parameters.
- Extended Handoff Direction message: one of several handoff messages sent by the base station.

Reverse Traffic Channels: this channel can multiplex primary (voice) and secondary (data) or signaling traffic. Some of the typical messages that the reverse traffic channel carries are:\textsuperscript{14}

- Order messages: include base station challenge, parameter update confirmation, mobile station acknowledgement, service option request and response, release, connect, DTMF tone, etc.
- Authentication Challenge Response message: information to validate the mobile station.

\textsuperscript{12} Vijay Garg, IS-95 CDMA and CDMA 2000: Cellular/PCS System Implementation (Prentice Hall, 1999), 123.
\textsuperscript{13} Ibid., 127.
\textsuperscript{14} Ibid., 131.
- Data Burst message: a user-generated data message sent by the mobile to the base station.
- Pilot Strength Measurement message: information about the strength of other pilot signals that are not associated with the serving base station.
- Handoff Completion message: is the mobile response to a Handoff Direction message.
- Parameter Response message: is the mobile response to the base station to a Retrieve Parameters message.

In Appendix 1 you will find a list of the messages carried on the CDMA paging and traffic channels.

For more detailed information refer to chapter 6 in Wireless Personal Communications Systems by David J. Goodman, and to chapter 7 in IS-95 CDMA and CDMA 2000 by Vijay Garg.

**IS-95 Call Processing**\(^{15}\)

In getting to a traffic channel, a mobile station goes through several states: system initialization, system idle state, system access, and traffic channel state.

In *system initialization* state the mobile acquires a pilot channel by searching all the PN Offsets possibilities and selecting the strongest pilot signal. Once the pilot is acquired, the sync channel is acquired using the \(W_{32}\) Walsh function and the detected pilot channel. Then the mobile obtains the system configuration and timing information.

Next the mobile enters the system *idle state* where it monitors the paging channel. If a call is being placed or received, the mobile enters the system *access state* where the necessary parameters are exchanged. The mobile transmits its response on the access channel and the base station transmits its response on the paging channel. When the access attempt is successful the mobile enters the *traffic state*.

---

\(^{15}\) Vijay Garg, *IS-95 CDMA and CDMA 2000: Cellular/PCS System Implementation* (Prentice Hall, 1999), 133
RSAT- 2000 CDMA

Figure # 1 shows the system set up:

Figure # 1 – RSAT-2000 CDMA System Components

For the purposes of this lab we will use the Active Set (ACTV), Candidate Set (CAND), Neighbor Set (NBR) and Layer 3 (LYR3) modes.

Each operating mode will display the phone’s state (CALL, IDLE, NO SVC, SCAN and SETUP) and the RF mode (CDMA or AMPS) at the upper left corner of the screen. The type of handoff currently in progress will be displayed at the center top of the screen.

The Active Set Mode (ACTV) shows information when the phone is in CDMA mode. ACTV provides information about the current members of the Active Set. The parameters displayed for each active member are the PN offset, member’s Searcher Ec/lo, Pilot Signal Strength measured by the mobile, and Walsh Code channel number. An up-arrow (^) character next to the PN Offset indicates that the finger is locked to this cell for use in demodulation. The ACTV mode also shows the frequency channel number of the AMPS channel at the center of the CDMA channel currently being used, the Frame Error Rate, the transmit gain adjustment to the mobile station, the fingers’ PN
offsets, the delay from the reference finger, the sum of the fingers' values, and the mobile’s transmitted and received power.

The CAND Mode shows information when the phone is in a CDMA call. This operating mode provides information for the current members of the Candidate Set, which can have as many as five members. The parameters displayed for each candidate member are the PN offset, the Searcher Ec/Io, the Pilot Signal Strength measured by the mobile and sent to the base station to request a change in Active and Candidate Sets (usually prior to a handoff), and the Walsh Code channel number. In addition this mode presents some parameters that are also present in the ACTV mode: the AMPS frequency channel number, the FER, the transmit gain adjustment to the mobile station, the fingers’ PN offsets, the delay from the reference finger, the sum of the fingers’ values, and the mobile’s transmitted and received power.

The Neighbor (NBR) mode shows the PN Offsets and Pilot signal strength readings for up to 20 neighbor sites when the phone is in AMPS mode. An asterisk in front of one of the neighbors indicates the best neighbor site.

The Layer 3 (LRY3) mode will only show data when the phone is in CDMA mode. As the Layer 3 transactions take place, they will appear on the screen. By pressing the UP and DOWN keys you can access the 30 most recent messages that are store in a buffer. While you review these messages the RSAT-2000 will not accept new messages. Press ESC to exit the messages buffer and review new messages. The SETUP softkey allows you to select or deselect the Layer 3 messages for the different logical channels, and the type of information you would like to view for each channel: MIN/ESN Filter that enables or disables the messages from other phones and mainly affects the paging channel, Call Setup/Release, Registration, Handoffs, Authentication, and Release Cause. To modify these options you cannot have the OptimEyes running.

**OptimEyes**

To start the OptimEyes on the computer select Programs, LCC Field, and OptimEyes from the Start Menu. The alert message “Scanning for Hardware” appears followed by the message “Finished diagnostics...H/W status okay" if the hardware detection is completed successfully.

The Setup Window appears by default when OptimEyes is started. You can also display the Setup Window from the menu Hardware then Device Setup. Chose the Select/Create Setup radio button. You must have the RSAT-2000 completely setup and on to use the Select/Create Setup. A list of the setups available will appear in the left hand side. For this lab you will use the setup Lab14-CDMA. Select the setup as indicated throughout the lab procedures and press OK. To begin the collection of data press the button F2 and to stop it press ESC.
The Lab14-CDMA setup has eight different views:

- A line chart called ACTV that shows the power transmitted and received by the phone and the power adjustment to the mobile station.
- A text chart also shows these three signal levels together with the Frame Error Rate in percentage and the number of the AMPS channel.
- Another line chart called CDMA Handoff shows information relevant for the handoff process: the Ec/Io of each of the fingers, the handoff events and the mode events.
- Two related text charts show each finger’s PN Offset and Ec/Io, the handoff type, pilot PN offset, and active members PN Offsets.
- A text chart called Active Set shows the PN Offset, Search Ec/Io, Pilot Signal Strength measurements, and Walsh Code for each active member.
- The Candidate Set text chart will show the same information but for the candidate members.
- The Neighbor Set text chart shows the PN Offset and Pilot Signal Strength for the neighbor set.

PRE-STUDY

Read section 7.7 in IS-95 CDMA and CDMA 2000 by Vijay Garg, and sections 6.4 to 6.6 in Wireless Personal Communications Systems by David J. Goodman.

LAB PROCEDURES

Connect the equipment as indicated in Figure # 1. Make sure to have everything connected before turning on the power supply. To turn on the Display Unit press the power button in the phone. To turn on the phone press the power button again. Start the OptimEyes as indicated above. All phone calls will be to the phone number 611. This call lasts only 1.27 minutes.

Active, Candidate and Neighbor Sets

In this experiment you will observe the active, candidate and neighbor sets and measure the Signal Strength received at several locations in the Engineering Building (in the lab, hallway, lobby, and 5th floor). You can use both the RSAT-2000 Display and the OptimEyes. The advantage of using the OptimEyes is that you can view simultaneously the Active, Candidate and Neighbor Sets charts and observe how the PN Offsets move from one set to the other.
1. Select the Active Set, Candidate Set, Neighbor Set, and ACTV views in OptimEyes’ Lab14-CDMA setup. Press F2 to start recording.

2. Start a phone call. Repeat it as necessary.

3. Take note of the signal strength received. This is displayed in the ACTV view.

4. Observe the Active Set and Candidate Set views. Take note of the number active and candidates members you see, their PN Offsets, and the pilot signal strength (PSMM) at which a member moves from the one set to another. Repeat it for the neighbor and candidate sets.

5. Move the phone around and observe how these parameters change.

6. Repeat your observations and measurements at different locations in the Engineering Building.

**Layer 3 Messages**

In this experiment you will observe Layer 3 messages using the RSAT-2000 Display Unit. In order to modify the LYR3 setup you must close OptimEyes.

**Sync Channel:**

1. Select the LYR3/SETUP mode in the Display Unit.
2. Use the UP, DOWN and CHNG keys to set Access, Reverse, Paging, Forward, and MIN/ESN Filter to OFF and all other options to ON. Press ESC to return to LYR3 main screen.
3. Turn the phone off and then on again.
4. Identify and take note of the SYNC channel messages you observe.

**Paging Channel:**

1. Select the LYR3/SETUP mode in the Display Unit.
2. Use the UP, DOWN and CHNG keys to set Paging to ON and Sync to OFF. Press ESC to return to LYR3 main screen.
3. Turn on the phone.
4. In this screen you will see many paging messages that appear very fast. Use the UP and DOWN keys to view the buffered messages.
5. Identify and take note of the paging messages you observe.
6. Place a call and observe the Paging messages for this condition.

**Access Channel:**

1. Select the LYR3/SETUP mode in the Display Unit.
2. Use the UP, DOWN and CHNG keys to set Access to ON and Paging to OFF. Press ESC to return to LYR3 main screen.
3. Turn the phone off and then on again.
4. Identify and take note of the Access channel messages you observe.
5. Place a call and take note of your observations.

**Forward Channel:**
1. Select the LYR3/SETUP mode in the Display Unit.
2. Use the UP, DOWN and CHNG keys to set Forward to ON and Access to OFF. Press ESC to return to LYR3 main screen.
3. Place a call and take note of the messages you observe. Move the phone around to identify other forward channel messages. You might need to use the UP and DOWN keys to look at the buffered messages.

**Reverse Channel:**
1. Select the LYR3/SETUP mode in the Display Unit.
2. Use the UP, DOWN and CHNG keys to set Reverse to ON and Forward to OFF. Press ESC to return to LYR3 main screen.
3. Place a call and take note of the messages you observe. Move the phone around to identify other reverse channel messages. You might need to use the UP and DOWN keys to look at the buffered messages.

**Call Processing**

In this experiment you will observe the Layer 3 messages that take place during a call from the idle state to the traffic state (including call termination).

1. Select the LYR3/SETUP mode in the Display Unit.
2. Use the UP, DOWN and CHNG keys to set all the options to ON but the MIN/ESN Filter that should be set to OFF. Press ESC to return to LYR3 main screen.
3. Start the OptimEyes and select Lab14-CDMA setup. For this experiment you will use the views CDMA Handoff (line and text charts), Active Set, Neighbor Set, and ACTV. Press F2 to start recording.
4. Place a call.
5. In order to take note of the messages observed you would need to use the messages buffer. But since the buffer can only save the 30 most recent messages you need to pay special attention in the following process.
6. After you place a call observe for a message that starts with `ACC:`; this is the origination message. Then wait until you start to see messages that begin with `FWD:` or `REV:`; these are the messages on the traffic channels. Wait few seconds and then press the END key in your phone to terminate the call. Few seconds later press the DOWN key on the Display Unit. This way you may get in the buffer all the messages that correspond to the call process. Use the UP and DOWN keys to identify and take note of the messages.
7. Stop your recordings in OptimEyes after you press the DOWN key in the Display Unit when the call is over. Play back the measurement and compare the messages obtained in the LYR3 screen with the actions presented by OptimEyes.

8. Compare the Layer 3 messages you observed with the call process diagrams in Appendix # 2.

POST-LAB (GROUP) EXERCISE

Exercise 1
What were the ranges of the received signal at the different locations in the Engineering Building? List the base station PN Offsets in each set and the corresponding PSMM you observed at each location. In which states of the call process did you observed members at the different sets? What events cause the mobile to move a base station from one set to another? Determine the threshold at which this transition occurs.

Exercise 2
Make a list of the messages you observed for each of the logical channels. What messages did you observed more often?
In the part when you observed just the paging channels, did you see any paging messages while the call is in progress? Why?

Exercise 3
For measurements performed in the Call Processing section of the lab procedures, what events in your OptimEyes measurements were you able to relate to the layer 3 messages observed in the RSAT’s Display Unit?
Make a flow chart similar to those in Appendix #2 with the messages you observed in this part. Compare your diagrams with the ones in Appendix #2

References:

Appendix # 1 : (From Goodman, pages 236 – 238)

**Table 6.6 Messages Carried on CDMA Paging and Access Channels**

<table>
<thead>
<tr>
<th>Access Channel</th>
<th>Paging Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Broadcast Messages</strong></td>
<td><strong>CHANNEL ASSIGNMENT</strong></td>
</tr>
<tr>
<td>SYSTEM PARAMETERS</td>
<td>PAGE</td>
</tr>
<tr>
<td>ACCESS PARAMETERS</td>
<td>SLOTTED PAGE</td>
</tr>
<tr>
<td>NEIGHBOR LIST</td>
<td>RELEASE*</td>
</tr>
<tr>
<td>CDMA CHANNEL LIST</td>
<td>FEATURE NOTIFICATION</td>
</tr>
<tr>
<td><strong>Call Management Messages</strong></td>
<td>DATA BURST</td>
</tr>
<tr>
<td>ORIGINATION</td>
<td>LOCAL CONTROL*</td>
</tr>
<tr>
<td>PAGE RESPONSE</td>
<td>REORDER*</td>
</tr>
<tr>
<td>DATA BURST</td>
<td>INTERCEPT*</td>
</tr>
<tr>
<td>LOCAL CONTROL RESPONSE*</td>
<td>ABBREVIATED ALERT*</td>
</tr>
<tr>
<td><strong>Authentication and Privacy Messages</strong></td>
<td><strong>AUTHENTICATION CHALLENGE</strong></td>
</tr>
<tr>
<td>AUTHENTICATION CHALLENGE RESPONSE</td>
<td>SSD UPDATE</td>
</tr>
<tr>
<td>SSD UPDATE CONFIRM/REJECT*</td>
<td>BASE STATION CHALLENGE</td>
</tr>
<tr>
<td>BASE STATION CHALLENGE*</td>
<td><strong>REGISTERATION</strong></td>
</tr>
<tr>
<td><strong>Mobility Management Messages</strong></td>
<td>✓ REGISTRATION ACCEPTED/REJECTED*</td>
</tr>
<tr>
<td>REGISTRATION</td>
<td>REGISTRATION REQUEST*</td>
</tr>
</tbody>
</table>

(continued)
### Table 6.6 Messages Carried on CDMA Paging and Access Channels (Continued)

<table>
<thead>
<tr>
<th>Operations, Administration, and Maintenance Messages</th>
<th>LOCK UNTIL POWER CYCLED*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UNLOCK*</td>
</tr>
<tr>
<td></td>
<td>MAINTENANCE REQUIRED*</td>
</tr>
<tr>
<td></td>
<td>AUDIT*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOBILE STATION REJECT*</td>
</tr>
<tr>
<td>MOBILE STATION ACKNOWLEDGMENT</td>
</tr>
<tr>
<td>BASE STATION ACKNOWLEDGMENT</td>
</tr>
</tbody>
</table>

* Message classified as an “order” (see Section 6.5.1).

### Table 6.7 Messages Carried on CDMA Traffic Channels

<table>
<thead>
<tr>
<th>Reverse Traffic Channel</th>
<th>Forward Traffic Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Management Messages</td>
<td></td>
</tr>
<tr>
<td>CONNECT*</td>
<td>ALERT WITH INFORMATION*</td>
</tr>
<tr>
<td>ORIGINATION CONTINUATION</td>
<td></td>
</tr>
<tr>
<td>FLASH WITH INFO</td>
<td>FLASH WITH INFO</td>
</tr>
<tr>
<td>RELEASE*</td>
<td>RELEASE*</td>
</tr>
<tr>
<td>DATA BURST</td>
<td>DATA BURST</td>
</tr>
<tr>
<td>SEND BURST DTMF*</td>
<td>SEND BURST DTMF*</td>
</tr>
<tr>
<td>CONTINUOUS DTMF TONE*</td>
<td>CONTINUOUS DTMF TONE*</td>
</tr>
<tr>
<td>LOCAL CONTROL*</td>
<td>LOCAL CONTROL*</td>
</tr>
<tr>
<td>LOCAL CONTROL RESPONSE*</td>
<td>SERVICE OPTION REQUEST*</td>
</tr>
<tr>
<td>SERVICE OPTION REQUEST*</td>
<td>SERVICE OPTION RESPONSE*</td>
</tr>
<tr>
<td>SERVICE OPTION RESPONSE*</td>
<td>SERVICE OPTION CONTROL*</td>
</tr>
</tbody>
</table>

(continued)
| Table 6.7 Messages Carried on CDMA Traffic Channels (Continued) |
|----------------------------------|----------------------------------|
| **Authentication and Privacy Messages** | **Radio Resources Management Messages** |
| AUTHENTICATION CHALLENGE RESPONSE | HANDOFF COMPLETION |
| SSU UPDATE CONFIRM/REJECT* | REQUEST ANALOG SERVICE* |
| BASE STATION CHALLENGE* | POWER MEASUREMENT REPORT |
| PARAMETER UPDATE CONFIRM* | PILOT STRENGTH MEASUREMENT |
| LONG CODE TRANSITION REQUEST* | **Mobility Management Message** |
| LONG CODE TRANSITION RESPONSE* | MOBILE STATION REGISTERED |
| AUTHENTICATION CHALLENGE | **Operations, Administration, and Maintenance Messages** |
| SSU UPDATE | STATUS |
| BASE STATION CHALLENGE CONFIRM* | STATUS REQUEST* |
| PARAMETER UPDATE* | AUDIT* |
| MESSAGE ENCRYPTION NODE* | MAINTENANCE* |
| LONG CODE TRANSITION REQUEST* | LOCK UNTIL POWER CYCLED* |
| LONG CODE TRANSITION RESPONSE* | MAINTENANCE REQUIRED* |
| **Other Messages** | **BASE STATION ACKNOWLEDGMENT** |
| MOBILE STATION REJECT* | |
| MOBILE STATION ACKNOWLEDGMENT | |
| BASE STATION ACKNOWLEDGMENT | |

* Message classified as an “order” (see Section 6.5.1).
Appendix #2: (From Vijay, pages 145, 147, 173)

Figure 8-10 Flow Diagram for CDMA Call Origination

(A) Channel element assigned to call
(B) Walsh code assigned to call
(C) Speech handler assigned to call
Figure 8-12  Flow Diagram for CDMA Call Termination
Figure 9-12  CDMA Soft Handoff—Beginning