CDMA2000 Simulation Project

Nikita Teplitskiy

February 2020

1 Introduction

This project is a limited implementation of the CDMA2000 wireless communications standard that focuses on the IS-95 compatible portion of the standard. The project simulates the forward pilot and and traffic channels when in Radio Configuration 1 using a 9600 baud non-flexible data rate. This implementation is based on the most recent 'E' revision of the standard with additional guidance provided by "Designing cdma2000 Systems" textbook.

2 Background

Code Division Multiple Access technology is based on the idea of encoding data using orthogonal codes that would allow the underlying data to be recovered from multiple overlapping data streams. This technique is very different from OFDM, which makes use of the orthogonality of sine waves to ensure data separation, and TDMA which separates signals in time. The orthogonality in CDMA is not implemented in the frequency domain, nor in the time domain, but rather on the level of transmitted data.

The benefit of using CDMA over other techniques is its flexibility and capacity. Because channel division occurs in the code domain, the number of available channels is linked to the number of available codes. Whereas GSM (a competing mobile standard) supports up to 8 users per frequency band through TDMA, IS-95 can support up to 55 users per frequency band. Though IS-95 bands are much wider than GSM bands, CDMA can handle more users over an entire bandwidth allocation. Additionally, because most of the complexity in CDMA systems lies in the encoding and decoding of data, existing IS-95 networks benefited from improvements in digital processing. When these 2G networks were made obsolete by cdma2000, many systems could be upgraded to the new standard while retaining some existing RF components.

3 Spread Spectrum

Spread spectrum techniques are means by which a baseband signal is modulated to a transmission bandwidth much larger than the bandwidth of the baseband signal. Though these techniques consume large amounts of bandwidth, spread spectrum channels can operate with much lower SNR than narrowband signals of comparable capacity. This is can be seen in the Hartley-Shannon theorem which states:

$$C = B \log_2(1 + \tfrac{S}{N})$$

Where C represents capacity, B is bandwidth, and $\frac{S}{N}$ is the SNR. The particular technique used by IS-95 and cdma2000 to modulate the data is direct sequence spreading. This technique works by combining baseband data with additional data and continuously occupies the entire allocated frequency space.

In IS-95, the additional data used to perform the spreading comes from two augmented pseudo noise generators which are defined in the "Physical Layer Standard for cdma2000 Spread Spectrum Systems." These generators create a repeating sequence of length 2^{15} chips which are used to modulate incoming data into in-phase and quadrature components at a rate of 1.2288 MCPS. All base stations use the same PN sequence and are synchronized in time, station differentiation is achieved by changing PN sequence

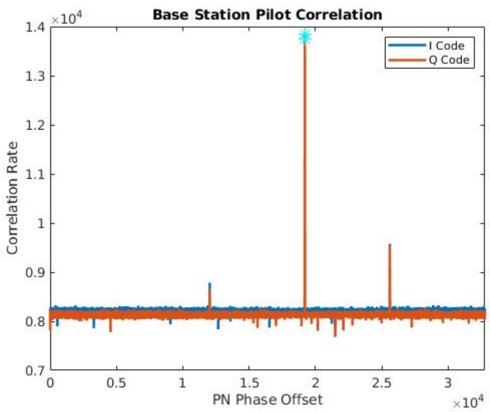

Figure 1: Correlation of 1 close BS and 2 distant BS

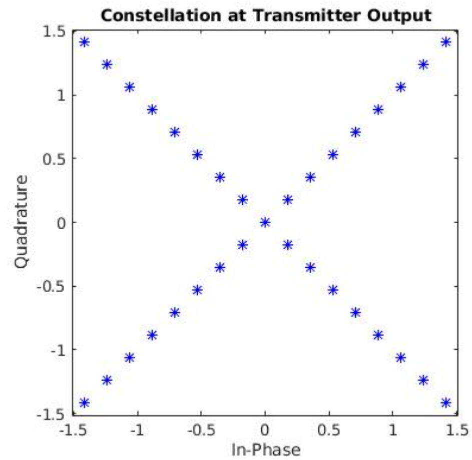

Figure 2: Correlation of 1 close BS and 2 distant BS

phase offset between stations. Whereas conventional cellular systems use a frequency reuse pattern to prevented intercell interference, CDMA stations use a phase offset reuse pattern instead. A total of 512 phase offsets are available.

Also involved in spread spectrum are Walsh-Hadamard codes and the long PN sequence. These additional data sources do, in some situations, increase the bandwidth of the signal, contributing to the spreading effect. The forward chanonels are first modulated up to 1.2288 MCPS using one of the 64 Walsh codes, so the short PN sequences do not perform any additional spreading. In the reverse link, the long PN code is used to encode transmissions from the mobile to the base station. While these codes are directly involved in spreading the signal, the primary reason for their inclusion is to identify and isolate individual channels.

Though adequate when IS-95 was developed, only having 64 different Walsh codes meant that a large amount of clients or clients using multiple channels could exhaust the code pool causing users to be dropped or rejected. cdma2000 addressed this issue by sometimes replacing fixed length Walsh codes with variable length quasi orthogonal functions, which behave like Walsh codes but are not truly orthogonal. This feature is not compatible with IS-95 devices and was not implemented due to its complexity.

4 Data Format

Data transmission over the forward traffic channel usually consists of symbol frames transmitted at a rate of 19,200 SPS. This transmission rate applies to most radio configurations (RC), except that RCs added by cdma2000 tend to occupy multiple channels meaning that their overall symbol rate consists of some multiple of 19,200. Other RCs such as RC 5 can have a much higher data rate which is intended for high-speed data transmission.

This project focuses on RC 1 with a voice data rate of 9,600 BPS using a non-flexible data rate. In general RC 1 uses 20 ms frames each of which contains 384 encoded bits of data. The amount of bits remains constant regardless of the vocoder bit rate so padding, repetition, and, additional error correction are used to fill up the frame. At 9600 baud, no repetition is used but a rate 1/2 convolutional code is used to expand the input sequence. The particular convolutional encoder is described in section 3.1.3.1.5 of the physical layer standard. Both the mobile and base stations make use of the same convolutional codes.

The data protocol also makes use of an interleaver to scramble bits within each frame after the convolutional encoder. The purpose of this is to help mitigate burst errors which may wipe out a significant chunk of contiguous data. Since bits are scrambled throughout the packet, burst errors are transformed into spread out bit errors, which are more likely to be corrected. The particular interleaver used by RC 1 is a bit-reversal interleaver which is defined by the formula:

$$A_i = 2^m(i \bmod J) + BRO_m(\lfloor i/J \rfloor)$$

Factors m and J are tunable, depending on the amount of data one wishes to interleave. These factors as well as other types of interleavers are specified in 3.1.3.1.8 of the physical layer standard.

Of the 384 bits present in the frame, only 192 are left after removing the convolutional encoding. Of these, the last 8 are all 0 as specified in 3.1.3.15.2. Furthermore, at 9600 baud, each frame contains a 12 bit frame quality indicator that is generated by a CRC generator specified in 3.1.3.1.4.1.2. This leaves 172 bits free for voice data. This works out to a data rate of 8600 baud, so 9600 baud is only a nominal data rate. A peculiarity of my implementation is that due to a lack of vocoder, I am passing 64 kbps audio from the base station to the mobile receiver. So that the audio appears at the receiver in "real time" I have enlisted the use of 8 separate channels to carry my voice data to the receiver. While this is not representative of IS-95 or cdma2000, this deviation from the spec demonstrates the functionality of multiple channels operating simultaneously in the same frequency space. It is also not an entirely unreasonable deviation since cdma2000 often makes use of multiple channels to transmit data to a single receiver.

5 Long Sequence Pseudo Noise Generator

The long PN generator consists of a 42 stage long generator that operates at rate of 1.2288 MCPS. While the short PN generator code repeats multiple times per second, the long code only repeats approximately once every 42 days which makes it more suitable for identifying and securing both base stations and mobiles.

On the base station side, the long PN code is decimated by 64 before being applied to the 19,200 SPS frames mentioned in the previous section. The phase offset of the long code is specially configured based on the Electronic Serial Number of the target mobile to provide a rudimentary form of security and target identification. The generation of the phase offset is covered in 2.3.6.1 of "Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems."

On the mobile side, the long PN code is the main spreading code and a specific offset mask is used for each device. Since the public offset mask is generated from a SHA1 hash of the phones ESN, it is only useful against basic signal interception. For more secure applications it is possible to generate a private offset mask that should prevent an unauthorized user from snooping or impersonating a mobile.

6 Conclusion

The project as presented is a reasonably faithful implementation of the most basic of of pilot and traffic channels specified by the cdma2000 standard. The only notable omissions from the traffic channel are the vocoder, and power control bits which may be optional in some configurations. Unfortunately the reverse pilot and traffic channels have not been modeled. It should be noted that the script contains some audio components to provide the user with a rich multimedia experience.

7 Resources

Korowajczuk, L. Designing CDMA 2000 systems; John Wiley Sons Inc.: Hoboken, NJ, 2004.

Physical Layer Standard for cdma2000 Spread Spectrum Systems Revision E; 3GPP2: 2005

Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems Release D; 3GPP2: 2005