International Journal of Research in Engineering, Science and Management
Volume-2, Issue-9, September-2019
www.ijresm.com | ISSN (Online): 2581-5792

CDMA: Encryption Modulation in Communication

Nishant Sharma[1], Ujwal Bang[2]
[1,2]*Student, Department of Electronics and Telecommunication Engineering, Thadomal Shahani Engineering College, Mumbai, India*

***Abstract*: Review of Code Division Multiple Access (CDMA) technology as modulation and encryption technique in communication and use of Discrete sequence spread spectrum (DSSS) implementation of CDMA IS-98 using 8051 to code data and establish encrypted sound communication, using QCELP coding technique of CDMA.**

***Keywords*: Code Division Multiple Access, Discrete Sequence Spread Spectrum, QCELP, I/O, Sampling.**

1. Introduction

Code Division Multiple Access, CDMA, is a communication technique originally developed for military communication due to its jam resistance. CDMA has also been used in satellite communication, and with some modification in commercial and civilian mobile communication. In CDMA multiple signals are sent over the same channel, encoded, in such a way that none of the signals interfere with each other, and the receiver can only decode and interpret desired signal. Which infers that CDMA modulation is basically encrypting the data which is though available to reception by multiple users, can only be interpreted by selected ones.

2. Coding in CDMA

A. *PN Sequence*

Multiple signals are sent on the same channel, each signal coded using signal spread. The message is coded using PN sequence even before transmission using the unique identification number of each node and DSSS is used to spread the signal into wideband.

PN sequences are deterministically generated sequences which seem like random noise generated in a circuit and is therefore used to generate random sequences of length of order 2n from a key of b bits [1]. It is not preferred in case of predicting algorithms because it can exploit and decode it completely or partially.

B. *Discrete Sequence Spread Sprectrum (DSSS)*

Discrete Sequence Spread Spectrum (DSSS) is a spread spectrum technique whereby the original data signal is multiplied with a pseudo random spreading code. DSSS significantly increases protection against interference. DSSS coverts a narrow band signal into a wideband signal. In CDMA, DSSS codes should have property of auto-correlation and orthogonality.

Auto-correlation: Multiplication of the code by the code itself results in a large value.

Orthogonality: Code multiplied by any other code than itself will result in zero.

A: Amplitude of the signal. *f*: Frequency.

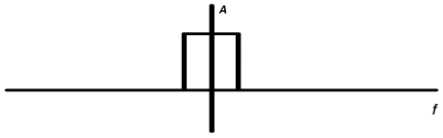

Fig. 1. Narrow band signal

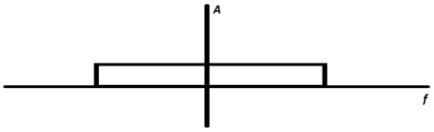

Fig. 2. Wide band signal: after multiplication of data with DSSS code

Walsh codes are used for DSSS. Walsh codes are linear code that codes n bit long binary data signal to 2^n bits long signal. Walsh codes are mutually orthogonal.

1) *Generation of Walsh code using Hadamar matrix [1]:*

$$H_1 = (1) \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H_{2N} = \begin{pmatrix} H_N & H_N \\ H_N & -H_N \end{pmatrix}$$

For correctness, we see that,

$$H_{2N}H_{2N}^T = \begin{pmatrix} H_N & H_N \\ H_N & -H_N \end{pmatrix} \begin{pmatrix} H_N^T & H_N^T \\ H_N^T & -H_N^T \end{pmatrix}$$

$$= \begin{pmatrix} H_N H_N^T + H_N H_N^T & H_N H_N^T - H_N H_N^T \\ H_N H_N^T - H_N H_N^T & H_N H_N^T + H_N H_N^T \end{pmatrix}$$

$$= \begin{pmatrix} 2I_N & 0 \\ 0 & 2I_N \end{pmatrix} = 2I_{2N}$$

Fig. 3. Generation of Walsh code using Hadamar matrix [1]

C. *Frequency Hopping CDMA*

Frequency hopping in CDMA is basic modulation technique used in spreads spectrum communication. In FH-CDMA, frequency of transmission is repetitively changed, in a pre-programmed manner, or pseudo-randomly. Frequency hopping

was innovated during the WWII to make wireless communication less prone to interception.

3. Significance of CDMA coding as encryption

According to Shannon's Theorem of Cryptography, perfect secrecy is achieved when the receiver has no clue about the data sent by the transmitter, that is, when data is random, with PN sequence we can generate pseudo random codes, hence granting high secrecy or good encryption. Since the code is nearly random, the entropy of transmitted signal is high.

Orthogonal property of Walsh codes is very important to CDMA, CDMA uses single channel to transmit multiple signals from different node, hence, at receiver, when the mixed signal is multiplied by an orthogonal code, the unwanted data results to zero and only the data coded with desired orthogonal code.

For instance, consider a user with Walsh code a receives a message encoded with b then [1],

$$a \,.\, (m \,.\, b \,.PN) = (a \,.\, b) \,.\, m \,.PN = 0 \,.\, m \,.PN = 0.$$

4. CDMA based communication using 8051 microcontroller

Establishing coded asynchronous serial communication over multiple microcontroller to simulate a communication system:

Here, to achieve voice communication, voice needs to be coded into digital samples, CDMA codes voice using QCELP in cellular communication, Qualcomm code-excited linear prediction, also known as Qualcomm Pure Voice. This is achieved using Qualcomm's own DSP chip solution MSM6275.

Data stream of voice coded as bits are given as the input at a port of the microcontroller used, intel's 8051. Which then codes the input bit stream and establishes a communication between multiple processor using single channel using UART protocol.

A. QCELP

QCELP uses adaptive algorithm to code voice into digital data bits. It dynamically selects sampling rate depending upon the speech activity. QCELP have four sampling rates to actively choose from, 8kbps, 4kbps, 2kbps, and 1kbps. QCELP is based on code excitation linear prediction [8].

B. MSM6275

MSM6275 is Qualcomm's digital signal processing chipset solution, it integrates many communication and powerful application processors. It has provisions for CDMA technologies.

C. 8051

8051 is Intel's 8-bit microcontroller, that is it has an 8-bit ALU, 2 data lines, one of 8 bits and another of 16 bits. It has 4 I/O ports.

D. Set-up

Set up consist of three 8051 microcontrollers ready for serial communication in mode 2 using UART protocols. The set up consist of one master controller and other two being slave controllers. Let master controller be called MC1 and slave controllers be MC2 and MC3. Slaves have master key and their own key saved in their ROM. MSM6275 is interfaced all 8051. Audio peripherals are connected to MSM6275.

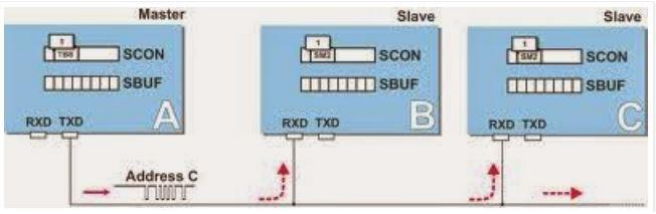

Fig. 4. 8051 serial communication mode 2 master slave [11]

E. Working

Voice is being coded to digital signal using QCELP algorithm in the MSM6275 chipset, these data bits are sent to 8051 to be coded using their corresponding orthogonal key.

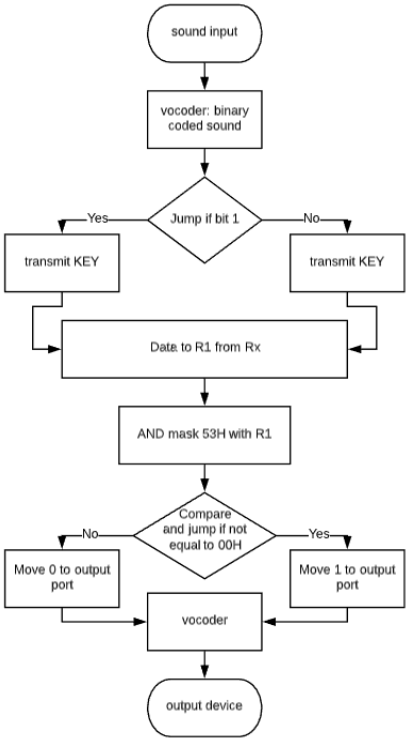

Fig. 5. Flowchart

The master controller signals the slave it wants to communicate to using TB8. This address is received by all the slaves. Slaves initially have their SM2 bit set to '1'. All slaves check this address and the slave who is being addressed, responds by clearing its SM2 bit to '0' so that the data bytes can be received. After slaves check for their address and the corresponding slave change the SM2 bit to '0'. Once the communication is established, DSSS is sent to the receiver, the

receiving microcontroller decodes the DSSS by multiplying it with the orthogonal key and adding the elements of the resultant product array. Bits 1 and 0 are stored in bit addressable area of RAM as a routine in every microcontroller, depending on the sum being positive or negative, 1 or 0 is received respectively and sent to DAC to convert it back to speech.

Here, even if the message was broadcasted, only the slave with the information of valid key could decrypt the message bits.

5. Conclusion

Encryption significance of CDMA coding techniques were pondered upon from the basics, talking about how CDMA is an encryption modulation in communication, which was also demonstrated by establishing multi-processor serial communication using Intel's microcontroller chip, 8051. Where we concluded that end to end encryption was present in CDMA channel, and the broadcasted message was only decoded by desired microcontroller.

References

[1] Singhal, K. (2012). Walsh Codes, PN Sequences and their role in CDMA Technology. (EEL 201).

[2] M. I. Mandell and R. J. McEliece, "A comparison of CDMA and frequency hopping in a cellular environment," *1st International Conference on Universal Personal Communications - ICUPC '92 Proceedings*, Dallas, TX, USA, 1992, pp. 07.01/1-07.01/5.

[3] P. W. Baier, "A critical review of CDMA," *Proceedings of Vehicular Technology Conference - VTC*, Atlanta, GA, USA, 1996, pp. 6-10 vol.1.

[4] Shi Yuanyuan, Liu Jia and Liu Runsheng, "Single-chip speech recognition system based on 8051 microcontroller core," in *IEEE Transactions on Consumer Electronics*, vol. 47, no. 1, pp. 149-153, Feb. 2001.

[5] C. Masawi and D. Mashao, Comparing CDMA and GSM Speech On Speaker Identification Performance, 2012.

[6] O. B. Wojuola, S. H. Mneney and V. M. Srivastava, "CDMA in signal encryption and information security," *2016 Information Security for South Africa (ISSA)*, Johannesburg, 2016, pp. 56-61.

[7] W. C. Y. Lee, "Overview of cellular CDMA," in *IEEE Transactions on Vehicular Technology*, vol. 40, no. 2, pp. 291-302, May 1991.

[8] A. DeJaco, W. Gardner, P. Jacobs and Chong Lee, "Qcelp: The North American Cdma Digital Cellular Variable Rate Speech Coding Standard," *Proceedings., IEEE Workshop on Speech Coding for Telecommunications*, Quebec, Canada, 1993, pp. 5-6.

[9] R. Cox, (2019). Speech Coding. CRC Press LLC.

[10] V. Shankar, (1997). Shannon's Theory of Cryptography. (CS93136).

[11] "Multiprocessor Communication Using 8051 Microcontroller," http://basicembedded.blogspot.com/2014/10/multiprocessor-communication-using-8051.html.

[12] En.wikichip.org, https://en.wikichip.org/w/images/1/1a/MSM6275_chipset_solution.pdf