Sindh Univ. Res. Jour. (Sci. Ser.) Vol.46 (3) 357-362 (2014)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Proposing Grey Coded Direct Sequence Spread Spectrum (GC-DSSS)

R. ULLAH[++], A. ALI*, T. JAN**, S. HAQ***

Department of CSIT, Sarhad University of Science and Information Technology, Peshawar

Received 02nd May 2014 and Revised 16th July 2014

Abstract: Securing the information is the main goal of today's advance digital/analogue communication systems. Different organizations used especial techniques for the securing their information, and DSSS is one of them; which stands for Direct Sequence Spread Spectrum. In this technique a code is used for securing the information, called Barker code. This code changes narrow-band information into wide-band information on transmitter side. And at receiver side the original narrow and information can be easily achieve by again using the same barker code. As in network security cryptanalyst are always in search to break the security of encrypted information, nonetheless the same thread is still present for breaking the security provided by DSSS. Here we are proposing a technique for securing the information: in cease if the attacker hijacked the information about barker code, they will still be unable to achieve the original information. So in this proposed technique we are going to use two codes, one is the original barker code, while the other one is its grey-coded code. We are using grey code here for encryption of barker code.

Keywords*:* Grey coding, Spread spectrum, DSSS, barker code, encryption, decryption

1. INTRODUCTION

An algorithm which is used to convert the narrowband-information into wide band-information is Spread Spectrum. Basically for this conversion a sequence (code) of binary numbers is used (Zeng, Zhang. 2010). As because of integration, the designing in electronic and telecom industry has been very much improved. The designing in VLSI improves the quality and reduces the manufacturing cost and almost it needs no manual assembling (Wolf, 2002) (Neil *et al.,* 2005) Before the advancements in integration (VLSI), cordless phones were used for the communications which had many problems like interference, distortion, short distance communication, etc. Spread spectrum gave a solution to all these problems, but initially was expensive to implement and was only used by military (Scholtz. 1977). (Simon, *et al.,* 1994) Very large scale integration reduces the cost for implementing spread spectrum communication for a commercial use (Seok-Yee *et al.,* 2011) Spread spectrum signal can be get by the use of spreading code, which convert the narrowband information into wideband, that code should be known at both terminals for synchronization (Pickholtz, *et al.,* 2011). Basic transmitter and receiver Spread Spectrum can be seen in (Ullah, and Latif. 2012).

Spread Spectrum has two fundamental techniques, one is called Direct Sequence Spread Spectrum (DSSS), while second one is called Frequency Hopping Spread Spectrum (FHSS). These two techniques offered variety of applications including robustness or security of a radio link, secure communications, prevent detection, noise and anti-jamming the communication, decreasing the Interference, multiple access between a number of users. These techniques can be used to deploy secure communication in military and Police (Thomas 2010) similarly the IEEE 802.11 wireless LAN uses spread spectrum in the 2.4 GHZ ISM band On the average, in DSSS, (Andrew 2012) the information signal occupies additional bandwidth as compared to the information signal. Because, before transmitting the information signal, it is divided into small portions and at transmitting point each piece of information must be combined with spreading code, which protect the signal to be jammed or interference, even it provide security to the data for recovery (data could be recover in if damaged or distorted up to some extent). IEEE 802.11 standard committee uses two types of spreading Sequences: short sequences and long Tze *et al.,* 2007, Boer. 2001).

In this paper we proposed a new technique called Grey Coded Direct Sequence Spread Spectrum (GC-DSSS), which will double the security compared to DSSS. After employing GC-DSSS technique, security of the information will be much stronger than existing DSSS, also anti-jamming effect will be improved and additionally if someone want to apply other encryption techniques, than that will more complicate the security. (Wolf , 2002)

This paper contains five sections: section one concludes the introduction to spread spectrum with its applications, section two presents summary of DSSS, while section three explains grey coding system in

[++]Corresponding Author: rahat.csit@suit.edu.pk, Ph. +92 91 5230 931-3, Ext: 233
*PTCL, Khyber Exchange, Peshawar, Pakistan
** Department of Electrical Engineering, University of Engineering & Technology, Peshawar, Pakistan
*** Department of Electronics, University of Peshawar, Pakistan

detail. Proposed algorithm is explained in section four, and section five concludes the paper with future directions of research in the paper.

2. MATERIAL AND METHODS

Summary of Direct Sequence Spread Spectrum

Securing the information is the main objective of today's modern digital world. The security can be achieved by using different algorithms and techniques, which may be hardware or software based. The DSSS technology gives secured information comparatively to high level. As through the channel data can be damaged by noise. This technology detects the original information if data is damaged upto 49%. The damaged data can be detected and corrected while the original information will not be effected (Ullah, and Latif. 2012) In Spread Spectrum techniques the original information changes into wide-banded information. The DSSS technology uses barker code for this purpose (Ullah, and Latif. 2012).

DSSS technology converts the data into wide-band with the help of repeater and barker code. Barker code is of eleven bits, and the repeater repeats a single bit into the length of barker code for make it able to be Ex-ORED with the barker code. When each bit of information is Ex-ORED with the barker code, as a result it makes a much wider band of data compare with the original data bits. This process is shown in **(Fig 1),** where the narrow-band information, 100 is converted into wide-band information with the help of barker code and repeater. The process of Spreading is in **(Fig 2)**.

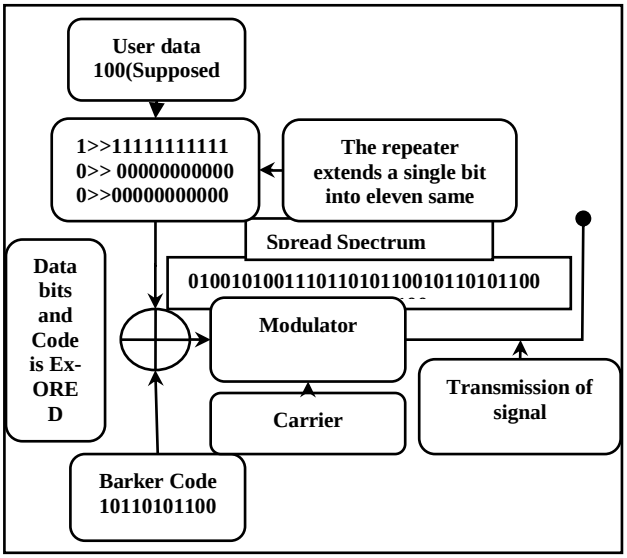

Fig. 1 Block diagram of DSSS on sender side

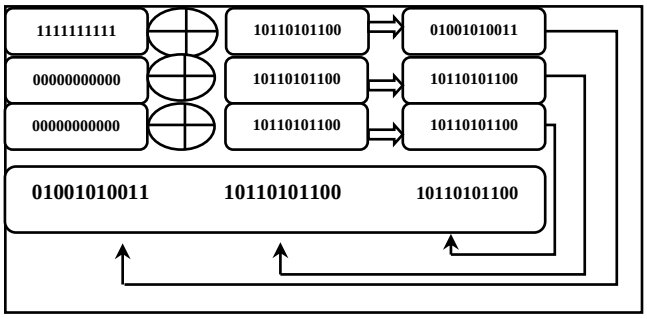

Fig.2 The spreading of narrow band data bits into wideband (Spreaded-data)

Three bit of data has been converted to thirty three bit data with the help of Barker code, which is much wider than the original data. Each bit of data is repeated eleven times and Ex-ORED with the barker code, shown in fig.2.

At the receiver side, the received signal is demodulated and each packet of data is Ex-ORED with the barker code to get the sequence of eleven bits. These bits are than passes through the integrator, which gives a single bit output. The integrator will count the majority bits and gives a bit at the output which is repeated for more than five times. If suppose error has occurred in a group of eleven bits. Consider that 01001010011 have been changed and five of bits have been get inverted due to error(less than 50%), and the bits pattern become 10110010011. These bits will be Ex-ORED with the barker code at the receiver. After that it will pass through the integrator, which will generate high if six or more of the eleven bits are high and will generate low, if six or more of the eleven bits are low. **(Fig. 3)** shows the receiver side of DSSS. The de-spreading of error free data is shown in **(Fig. 4)** and how the data could be retrieved from effected data using DSSS is shown in fig.5.

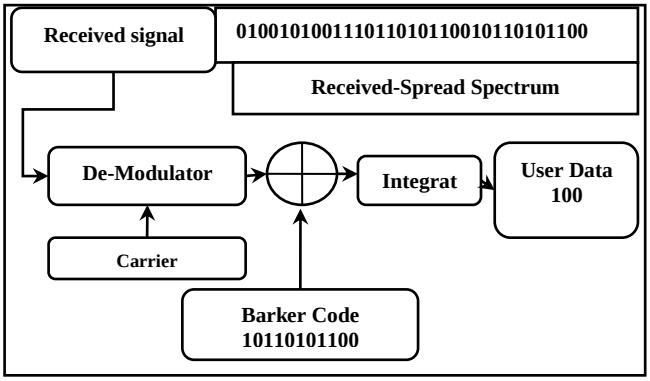

Fig. 3 Block Diagram of DSSS's receiver

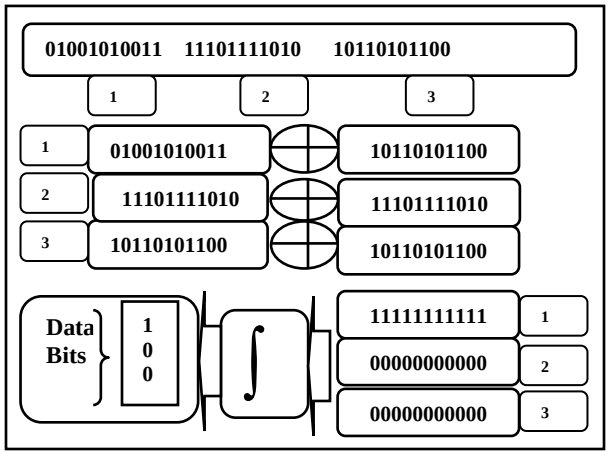

Fig. 4 De-spreading of error free data at receiver side

At the receiver, two possibilities may happen. The spreaded information may or may not be corrupted due to noise. Also the some portion of the data may get corrupted. The receiver will have the same barker code which is used at transmitter/sender side. It will use barker code for achieving the spreaded information bits. Fig. 6 shows that the received spreaded data is error free, and it explained the de-spreading of data in an easy way. In fig.5 two of three packets is being damaged (inverted) due to noise, shown in the figure where the bits are highlighted . From fig.2 the spreaded data at the sender side was:

01001010011 10110101100 10110101100
Through the channel the error has damaged the data and it becomes as, for example:
10111010001 10110101100 01110101111

The highlighted data has been damaged, & few of the bits has been inverted but less than 50% of the bits in a packet. **(Fig.5)** shows that how the original data has been recovered after inversion of the spreaded data.

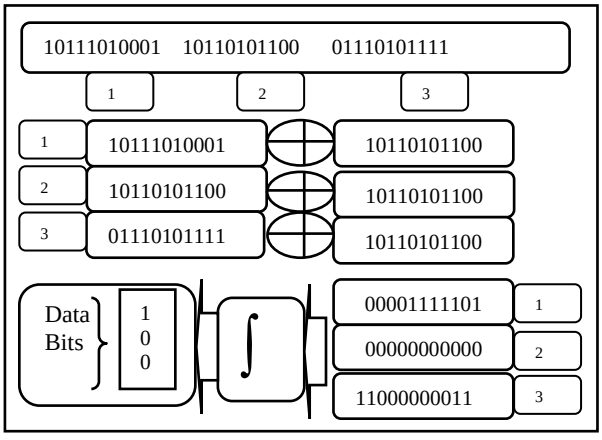

Fig. 5 Recovering the original data after been damaged by error

3. GREY CODE

Grey code is an un-weighted code. And it is quite different than binary pattern of bits, such that its value cannot be directly estimated because in grey code the bits position does not shows specific weights like in binary bits (Ananthi, *et al.,* 2006) Grey code is mostly used in shaft position encoders (Ananthi, *et al.,* 2006) . The process for converting the binary bits into grey code is quite easy. In the grey code and in the binary number, both the left most bits will be same. Proceeding from left to right add the two adjacent binary code bits to obtain the next grey code bit, the carry should be discarded (Ananthi, *et al.,* 2006). Consider 111001, is a binary number so its grey code will be:

1→ + →1→ + →1→+→0→+→0→+→1
↓ ↓ ↓ ↓ ↓ ↓
1 0 1 1 0 1

The logic used for code conversion from binary to grey can be achieved in two ways. One is the use of Ex-OR gates, the other one is by programming the programmable logic devices (PLDs) (Ananthi, *et al.,* 2006) but PLDs are expensive than the use of Ex-OR.

4. RESULT AND DISCUSSION

Proposed Algorithm

The proposed, Grey Coded Direct Sequence Spread Spectrum (GC-DSSS) uses two codes, instead of one barker code. One is the Barker code & the second one is its encrypted form. In our technique the encryption of barker code is done with the help of grey code. Grey code is an un-weighted code, which is mostly used in digital systems. In our proposed technique the odd number of packets of data will be Ex-ORed with the original barker code while even number of data packets will be Ex-ORed with the encrypted code. Suppose we have four bits of data, so the first and third data bit will be Ex-ORed with the original barker code, while the second and fourth bit will be Ex-ORed with the grey coded(encrypted) form of that barker code. A switch will be used which will demultiplex the data into even and odd packets and will forward it to be Ex-ORed with the barker and its grey coded form. After spreading a switch will transfer the bits from the Barker code and grey code conversion portion on a single path to the modulator.

Packet-1 before Ex-Or with the barker code is eleven zeros. After Ex-ORED with the barker code it becomes 10110101100, similarly packet three is eleven ones which becomes 01001010011. Packet two is eleven zeros before Ex-ORED with the encrypted form of barker code, and it gives 11101111010 after Ex-ORed with the second code (encrypted form of Grey

code). The spreading and encryption of data using the two-code system is shown in fig.7 in detail. If we compare fig.2 and fig.7, one can sense the impact of encryption of code on the securing of data. In both the figures the second data was same, but the spreaded encrypted form is quite different. Similarly in fig.7 second and third data packet was same (eleven zeros), but the final result is quite different. In GC-DSSS the data become more secure than in the ordinary DSSS, which uses only barker code. Second packet of spreaded/encrypted data is looking quite different in fig.2 & fig.7, although the information bits were same. The second packet which is highlighted in **(Fig.6, 7)**. The attacker will be unable to comprehend the original information because he may hijack only the barker code, not its encrypted code.

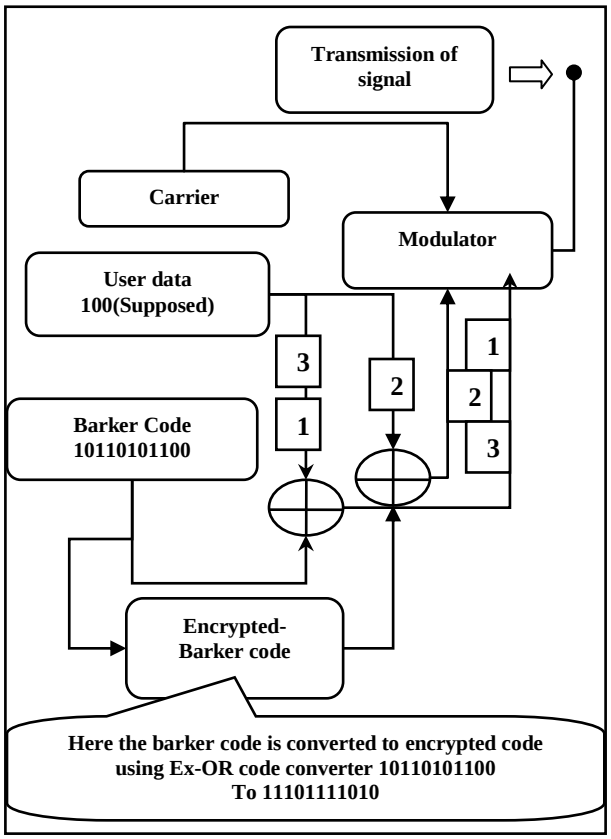

Fig.6. Proposed Transmitter of GC-DSSS

The receiver will entertain the spread spectrum, which may be attacked by noise or may not. After demodulating the signal, the packets will be Ex-ORED with the codes used at transmitter side. Odd number of data packets will be Ex-ORed with the barker code and even packets of received data with encrypted form of Barker code. After this operation these packets will pass through the integrator. Integrator will accept eleven bits-packets and will produce only one bit at the output, which will be our original information (de-spreaded). Block diagram of proposed GC-DSSS is shown in **(Fig. 8).**

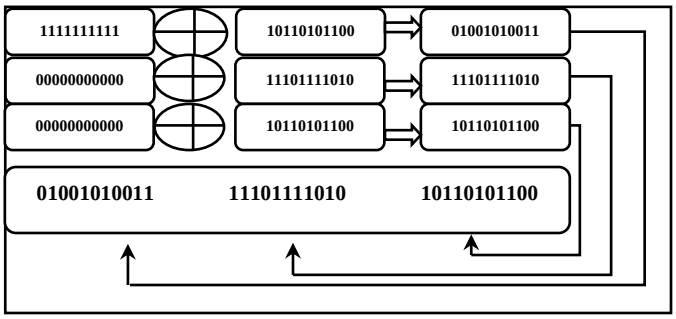

Fig. 7 Encryption of Information using DC-DSSS before transmit

The de-spreading and decryption of GC-DSSS is shown in **(Fig.8)**. Packet one and three are Ex-ORed with the original code and packet two is decrypted with the encrypted code. Received packet two is enveloped/encrypted at transmitter side with the encrypted code which opened/decrypted at receiver side by using the . After de-spreading the original data is retained easily.

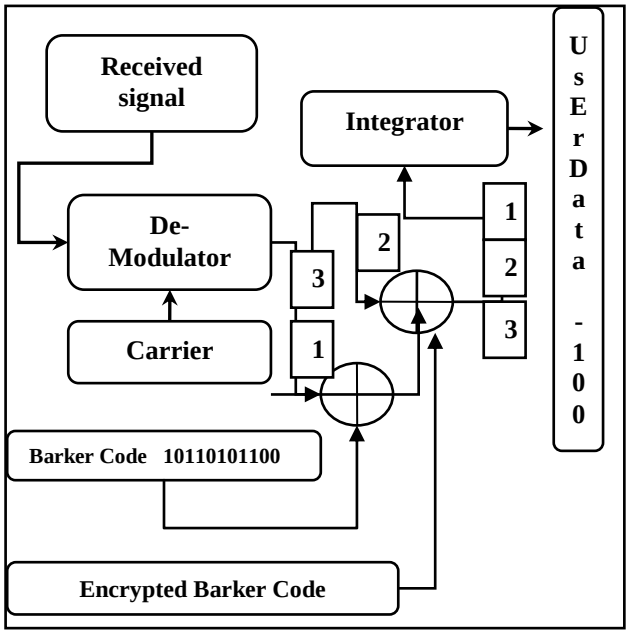

Fig.8 Proposed Receiver of GC-DSSS

5. CONCLUSION

In this paper we have introduced a new algorithm for securing the direct sequence spread spectrum. We called it grey-coded DSSS (GC-DSSS). DSSS uses barker code for spreading the data. GC-DSSS uses two codes for spreading the data. One is the barker code, the second code used for spreading the data is the encrypted form of barker code. Both the codes

will be used for encrypting the spreaded data at the same time. The encrypted code will be applied on even numbers of packets, and the original spreading code will be applied on Odd number of data's packet. This new coding technique will improved the security level of DSSS. Similarly in future we could implement this algorithm experimentally and mathematically using simulation tools like MATLAB.

REFERENCES:

Ananthi, S., R. Hariprakash, V. Vidya K. Devi, (2006) *Spread Spectrum Communication Using Wavelets of Signal for More Security,* Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services IEEE. 87Pp.

Andrew S. T. (2012) Computer Networks, Prentice Hall (India) Ltd., Fourth Edition.. 294-295,

Boer. J. (2001) Proposal for 2 Mbits/s DSSS PHY", doc: IEEE P802.11-93/37

Neil H., E. Weste, and K. Eshraghian. (2005) Principle of CMOS and VLSI Design A Systems Perspective 3rd Edition, Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA ©1985 ISBN:0-201-08222-5

Pickholtz, R. L., D. L. Schilling, and L. B. Milstein (1982). Theory of spread-spectrum comm.-A tutorial, IEEE Trans. Commun., vol. COM-30, No.5.

Scholtz. R. A. (1977) The spread-spectrum concept, IEEE Trans. Commun.,vol. COM-25, 748–755.

Simon, M. K., J. K. Omura, R. A. Scholtz, and B. K. Levitt. (1994) Spread Spectrum Communications Handbook, revised New York, McGraw-Hill.

Seok-Yee T., P. Muller, H. Sharif. and WiMAX (2011) Security and Quality of Service: An End-to-End Perspective, John Wiley & Sons Ltd, the Atrium Southern Gate, Chichester, West Sussex, PO 19 8SQ, UK..

Thomas L. F. (2010) Digital Fundamentals, seventh/eighth edition, ch.2 & 6. Page 30 and 297.

Tze R. and M. Sheng. (2007) A Draft Proposal for Direct Sequence Spread Spectrum PHY Standard, IEEE.

Ullah, R., S. Latif. (2012) Improving the Security Level in Direct Sequence Spread Spectrum using Dual Codes (DC-DSSS), International Journal of Security and Its Applications Vol. 6, No. 2, 55-60.

Wolf W. (2008) Modern VLSI Design Systems-on-Chip Design 3rd Edition, Prentice Hall, 4th Edition, ISBN-10: 0137145004.

Zeng, F., Z. Zhang. (2010) Binary sequences with Large Family Size and High Linear Complexity for Spread Spectrum Communication Systems, 2nd International Conference on Signal Processing Systems (ICSPS).