Improving the Security Level in Direct Sequence Spread Spectrum using Dual Codes (DC-DSSS)

Rahat Ullah[1] and Shahid Latif[2]

Computer Science and IT department Sarhad University of Science and IT Peshawar, 25000 Pakistan[1, 2]
Rahat.csit@suit.edu.pk[1], shahid22latif@yahoo.com[2]

Abstract

The security of information in wireless communication is a hot issue for researchers throughout the technical globe and uses different techniques to secure the information. One of the techniques is Direct Sequence Spread Spectrum. In DSSS a barker code is use for converting the narrowband information signal into a much wider bandwidth. As the anti-security group is also in search of breaking chain of security for leaking out the information, so in DSSS the great threat is the breakage of the code used for spreading of the signal, if the attacker comes to know the code through somehow than all the information could be loss. In this paper we proposed a technique/idea in which the security of the information will not be loss even the hijacker break the code. We will encrypt the code first, and will use both the original and encrypted barker code. The proposed name for this technique is dual coded direct sequence spread spectrum-DC-DSSS.

Keywords: *spread spectrum, direct sequence spread spectrum, encryption/decryption, and barker code*

1. Brief Summary of Spread Spectrum

Spread spectrum is a technique which is used for converting the narrow band information signal into wideband spreaded signal, by using a code of fixed number of bits. This code should be synchronized with the code used at the receiver side for dispreading the information; otherwise the information will not be readable [1]. The cordless phones were in great use before the introduction of spread spectrum, but it had many disadvantages like high rate interference of cross talking, not a good quality of voice, lack of long distance communication, it became obsolete after spread spectrum [1, 2, 3]. Although this technology ride over all the disadvantages of cordless phones but it was out of range for a commercial use because of the very much expensive hardware used for its operation, it was using for military operations in the beginning. After getting improvement in the designing of cheap integrated circuit technologies, spread spectrum provided services for commercial use. In using spread spectrum the cross talk interference has so much decreased also the security level improves [4]. Spread spectrum expands the narrow band information signal into the wideband using barker code which should be synchronized with the code used at the receiver side for dispreading the signal, while the information remains the same during spreading process[4, 5]. Figure 1 & Figure 2 explains the concept of spreading and dispreading of the signal.

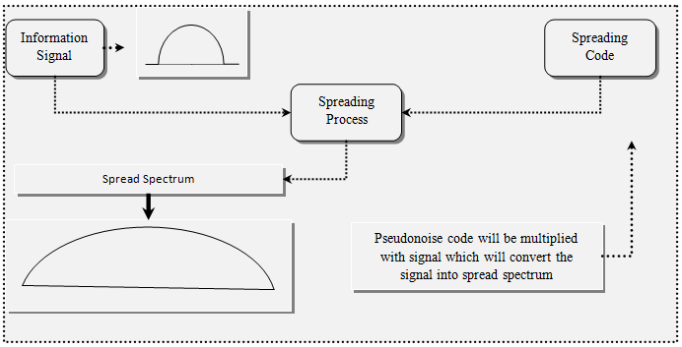

Figure 1. Conversion of a Narrowband Signal into Wideband Signal

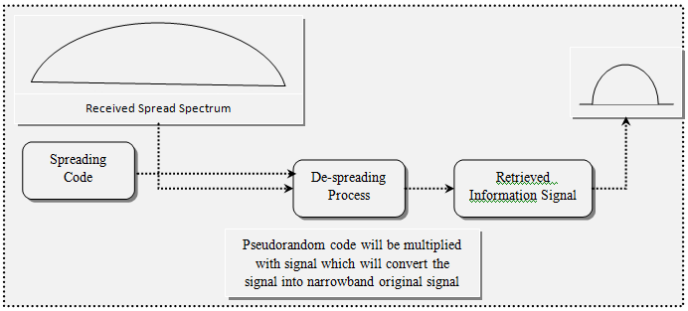

Figure 2. Retrieving the Original Narrowband Signal from Spread Spectrum

Frequency Hopping spread spectrum, direct sequence spread spectrum, time hopping spread spectrum, & the hybrid of these are the fundamental instances of spread spectrum [4]. This paper is divided into four sections, in the first section we have shortly explain the spread spectrum, the second section is about DSSS, and in the third section we will explain the proposed work in detail.

2. Direct Sequence of Spread Spectrum

The prime objective of spread spectrum is the anti-jamming, noise free, and clear communication. Spread spectrum uses digitl dignals and the information is divided into small packets, each of information's bit is Ex-ORED before transmittind with the psedonoise code in spread spectrum. There is always uses quadrature phase shift keying, frequency shift keying, or phase shift shift keying as coding technique[6]. The DSSS uses the spreading code for converting the narrow band information into the wideband information. That code is called barker code which has a specified length normally of eleven bits. In DSSS each of the information bit is EX-ORED (EX-OR logic) with the barker code at the point of transmission, as a result the whole information is converted into a very wideband and the information signal remains the same. This spread spectrum is able to reject the attack to be jammed, interference and also because of this coding technique (DSSS) the information signal can be recovered if less than fifty percent the data bits been damaged during propagation through the channel. If supposed less than fifty percent an error is occurred in the spreaded signal through the channel, and because of the synchronization of barker code at the receiver and transmitter, than the original information can be recovered. Figure 3 and 4 shows the transmitter and receiver of DSSS technique.

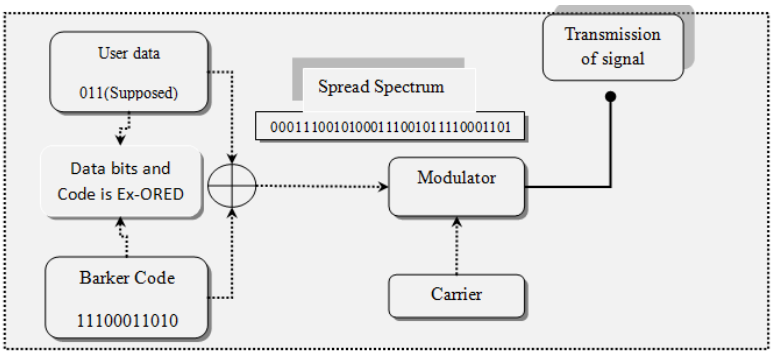

Figure 3. Transmission of Spread Spectrum Using DSSS Technique

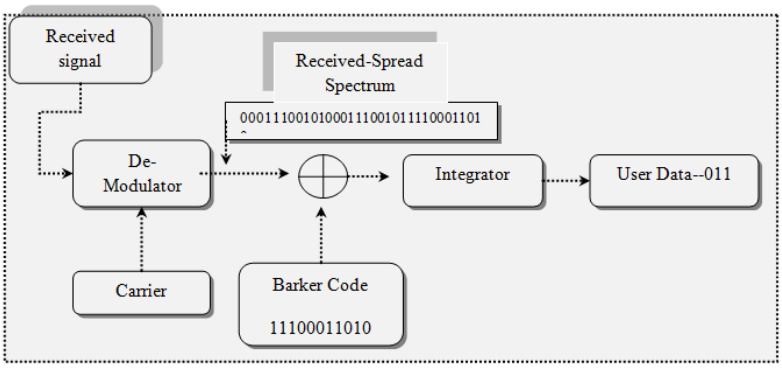

Figure 4. Receiving of Spread Spectrum Using DSSS Technique

Figure 3 and figure 4 shows the simple diagrams of transmitter and receiver using in DSSS modulation. At transmitter side each of the user data's bit is Ex-ORED with the barker code, which is converted into spread spectrum and transmitted after riding over at the carrier frequency. When the spreaded data receives at the receiver side than first of all through demodulation the spreaded data arrives, which is Ex-ORED with the barker code, and each of the eleven data bits enters into the integrator, which creates 1's and 0's depending on the majority of the bits, and as the code is eleven is longer and if five bits are changed/inverted than the integrator detects the original bit. The DSSS technology detects the original data if less than fifty percent data bits corrupts.

Direct sequence spread spectrum offers a secure and jamming free transmission, but as in wireless communication the detectors/ attackers are in a search to break the security of information and to read the information. In DSSS although the security level is quite good but if the interception occurs by the attackers and they come to know the barker code, than the security fails to secure the information any-more. In this paper we have proposed an idea for securing the information in such environment when the code is been detected.

3. Proposed Dual Coded Technique in Direct Sequence Spread Spectrum

Dual coded DSSS uses a barker code with its encrypted form, for spreading the information. It is a more secure technique for spreading the user data, because at a time two barker codes are using for spreading the user data, the two barker codes means that one is the original barker code, while the other one is the encrypted form of barker code. The user data's bit will be bit wise Ex-Ored with the barker code and encrypted form, so that the spread

spectrum will consists of serial wise packets of data, each of eleven bits. The first eleven will consists the output of original barker code, while the second one will be of the encrypted form of barker code. Know if the attacker comes to know the barker code, than it will never be able to intercept the data, because it will not understand the output of encrypted data.

The receiver will easily be able to detect the original data because it will know the barker code as well as the encryption technique used for encryption of the barker code. The received signal will be de-modulated and than each of the packet of eleven bits will be serially Ex-ORing with the barker and its encrypted code. And after integration the data will be received securely at the receiver.

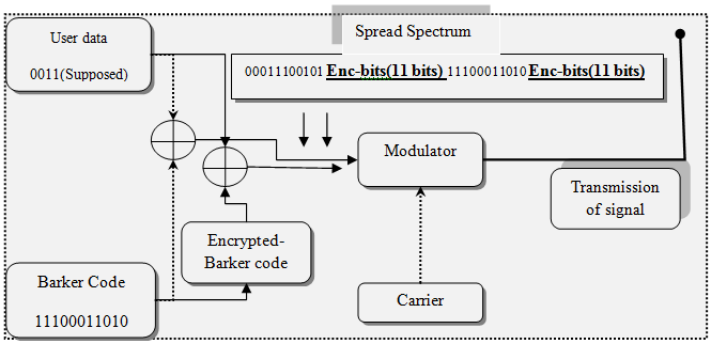

Figure 5. DSSS Transmitter using Barker Code and its Encrypted Form

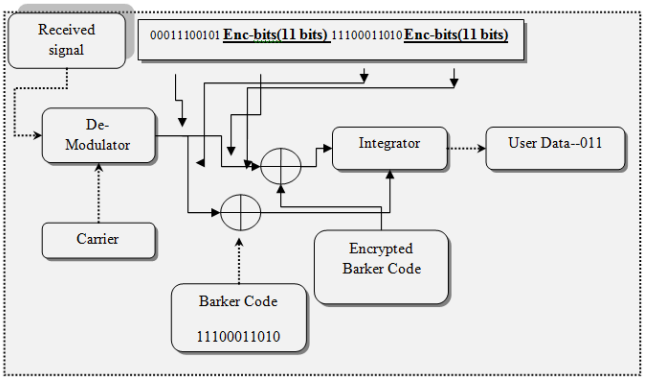

Figure 6. DSSS Receiver using Barker Code and its Encrypted Form

References

[1] R. L. Pickholtz, D. L. Schilling and L. B. Milstein, "Theory of spread-spectrum comm.—A tutorial", *IEEE Trans. Commun.*, vol. COM-30.

[2] R. A. Scholtz, "The spread-spectrum concept", *IEEE Trans. Commun.*,vol. COM-25, pp. 748–755, **(1977)** August.

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

[4] Seok-Yee Tang, Peter Muller, Hamid Sharif "*WiMAX 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.

[5] R. C. Dixon, *Spread spectrum Systems with Commercial Applications, 3ed*, John Wiley & Sons, New York, **(1994)**.

[6] Jan MIKULKA, Stanislav HANUS, "*CCK and Barker Coding Implementation in IEEE 802.11b Standard"* 1-4244-0822-9/07 ©C2007. IEEE **(2007)**.