Random Selection of Multiple Spreading Codes Enhances the Security of DSSS Transmission (RSMC-DSSS)

Shahid Latif and Rahat Ullah

Department of Computer Science & IT
Sarhad University of Sciences and Information Technology (SUIT)
Peshawar, KPK, Pakistan
shahid22latif@yahoo.com, rahat.csit@suit.edu.pk

Abstract

Spread Spectrum technique transmits the information message (signal) over a bandwidth much larger than its frequency contents or the original bandwidth of information message. In SS technique, a signal (having a specific bandwidth) is spread in the frequency domain and results in a signal having wider bandwidth. Remember, the new resulting bandwidth of a signal is much larger than the minimum required frequency spectrum. In Direct Sequence Spread Spectrum, i.e., DSSS (one of the common techniques of SS) the transmitting information signal is multiplied or combined with the spreading signal (usually Barker code) of wider bandwidth and results in a modulation signal that take up the wide bandwidth of the spreading signal. This new consequential signal is then combined with a carrier signal before transmission. The most important advantage of DSSS technology is the accepted transmission security. In this paper, a novel scheme is proposed that helps out the traditional DSSS system to enhance the transmission security by using random selection of multiple spreading codes in DSSS. In this paper the 11-bit spreading (Barker's) code is taken under the consideration as the spreading code.

Keywords*: Multi-Coded DSSS, Information Security, Random Selection, Spreading Codes, Secure Transmission*

1. Introduction

Clear, noise free and secure communication is an important issue for the wireless communication systems and services. This issue is resolved up to some extent with the help of Spread Spectrum technology. A communication technique in which a telecommunication signal is transmitted on a larger/wider bandwidth than the bandwidth or the frequency content of the original information is called Spread Spectrum Technique. In Spread Spectrum technology several techniques including direct sequence (DSSS), frequency hopping (FHSS), Time hopping (THSS) and/or hybrid of these are available, which can be used for multiple access (like CDMA) and/or multiple functions. Main advantages of SS includes: Anti-jamming of signal, low interference to signal, lower probability of signal intercepting, CDMA, information privacy and much more. Using spread spectrum technique the potential interference can be decreased and the privacy of the transmission can be achieved [1].

SS technology normally uses a noise-like signal to spread the narrowband information signal over a relatively wideband signal (radio frequency or a band of radio frequencies). At the receiving side, the original information signal is recovered from the received spread signal using the same procedure in reverse. Actually, from [2, 3, 4], a spread-spectrum system uses a process to expand/spread the bandwidth of the signal instead of sending the information

signal directly. The two most common forms for spreading the spectrum are direct sequence and frequency hopping. These techniques provide the advantages like secure communication, robustness or security of a radio link, preventing detection, multiple accesses between a number of users, decreasing the interference, noise free communication and anti-jamming etc in wireless communication systems. These spread spectrum techniques are used particularly for Police Radar and military communications discussed in [5]. While the IEEE 802.11 wireless LAN uses spread spectrum techniques in the 2.4 GHz ISM band [6].

In DSSS, the transmitted signal is intentionally spread so that it takes up more bandwidth than the original information signal bandwidth which is being modulated. The information signal to be transmitted is divided into small packets. A frequency channel from a frequency spectrum is allotted to each packet of the signal, which, at the point of transmission is combined with a higher data-rate bit sequence (called spreading code: also pseudo noise (PN) code) using X-OR logic. This code helps in minimizing the interference to the signal and also enables the original data to be recovered if data bits are damaged during transmission. IEEE 802.11 standard committee use mainly two types of spreading codes/Sequences: long sequences and short sequences [7, 8, and 9], while [10] gives a new type of demodulation for DSSS and researches its performance. To reconstruct the original signal on the receiver side, the knowledge of the spreading code used at the transmitter side is compulsory. In DSSS, Multi-code and multi-carrier systems [11, 12, 13, 14] are responsible for the avoiding of multipath fading and potential applications for high-speed communications.

In this paper, a new technique called RSMC-DSSS, *i.e.*, Random Selection of Multiple Codes Direct Sequence Spread Spectrum is presented that enhances the security of the transmission by applying 2, 4, 8 or more different spreading codes along their random selection process to spread the modulated information signal over larger bandwidth. Remember that large number of spreading codes results in more secure transmission of information signal. Employing the proposed scheme will surely provide a much stronger security system than the existing. Moreover, spread spectrum technique that uses random selection of multiple spreading codes is also capable to use with BPSK system.

Apart from Section I, rest of the paper is organized in such a way that it consist of five sections. In Section-II, the detailed overview of the direct sequence spread spectrum (DSSS) and multi-coded DSSS techniques are presented. Then the proposed scheme, *i.e.*, RSMC-DSSS for enhancing the security of the transmission is illustrated in Section-III. In Section-IV, the complete block diagram/model of the transmitter and receiver for the proposed technique are covered. Finally, the last section concludes the paper.

2. DSSS

Although, clear and noise-free transmission of information is the need of wireless telecommunication, but it is not the only prime objective. It also requires that the transmission must be well secure from interception by the unauthorized users in both commercial as well as in defense communication. In wireless telecommunications, DSSS is a modulation technique, in which the transmitted signal is intentionally spread and it takes up more bandwidth than the information signal that is being modulated. As mentioned earlier, in DSSS, the information signal is divided into small packets; each of these packets is allocated with a frequency channel across the spectrum and at the point of transmission this packet is combined with a spreading sequence that divides the data according to a spreading ratio. This spreading code helps the signal to resist the interference and also enables the original data to be recovered if data bits are damaged during transmission. According to IEEE 802.11 standard committee, two different types of spreading Sequences are in use 1) Long sequences:

the sequence period is longer than the bit period and sections of it are inverted by the data in the modulation process, as specified in [7], and 2) Short sequences: the sequence period equals the bit period, as specified in [8, 9]. The simple DSSS transmitter and receiver block diagrams using 11-bit spreading code (short sequence) are shown in Figure 1 & 2 respectively. Figure 3 show the spreading of signal bits with 11-bit spreading code. Similar results may be obtained using MATLAB simulink as in Figure 3.

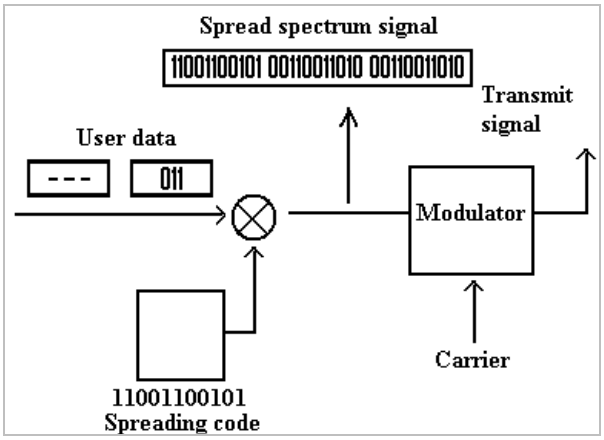


Figure 1. Block diagram of DSSS transmitter

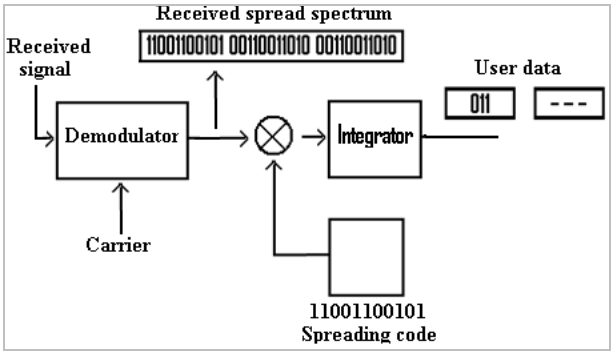
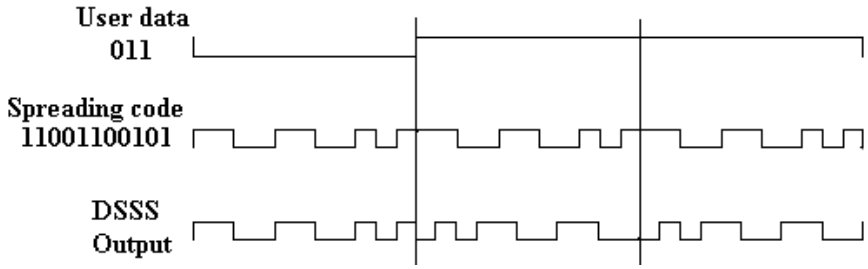


Figure 2. Block diagram of DSSS receiver

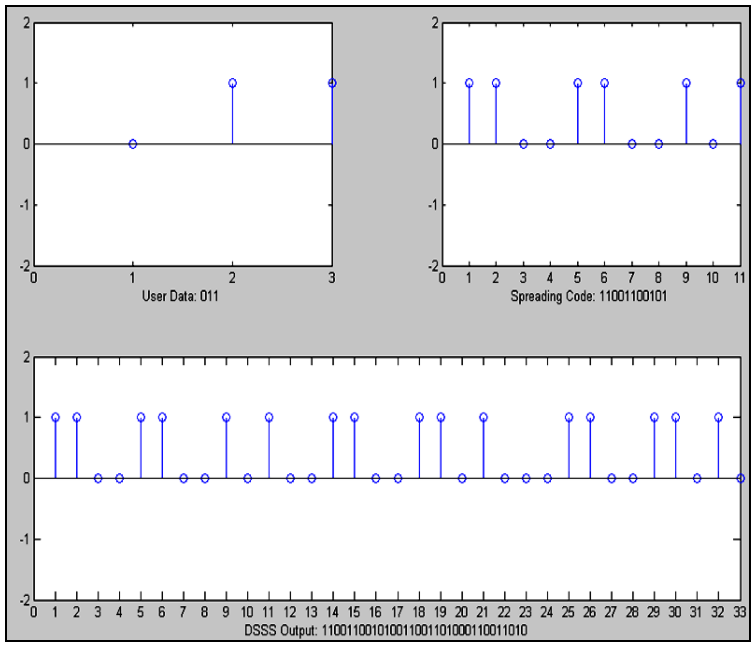
3. Multi-Coded DSSS

Multi-coded DSSS uses multiple spreading codes or N number of spreading codes having similar bit-size to spread the spectrum. This enhances the transmission security by assigning multiple and different spreading codes to the data packets of information signal. The number of spreading codes is directly proportional to the level of security. Large number of spreading codes will provide more security and vice versa. The transmitter and receiver block diagrams for multi-coded DSSS technique using 2 different spreading codes are shown in Figure 4 and 5 respectively. At the transmitter, each information bit of first data packet is multiplied through X-OR logic with one of the two spreading codes to spread the spectrum. After spreading the signal

packet a code-bit for the spreading code being used (say "0" for the first spreading code) is placed at the right of spread data and then it is forwarded to the transmitter for transmission.



(A)



(B)

Figure 3. Spreading of the signal with spreading code

Similarly each bit of the very next data packet is multiplied, using the same X-OR logic, with the second spreading and the corresponding code bit code (say "1" as code-bit) is placed at right to the spread data and then it is forwarded to the transmitter as shown in Figure 4. At the receiver, first of all the received signal is demodulated with similar carrier used at the transmitter. Then each spread data packet is X-ORed with the spreading code to reconstruct the original data. Knowledge of the spreading codes and their code bits is compulsory at the receiver side to successfully recover the original signal.

The two spreading codes and their corresponding code bits are shown in Table 1 as under.

Table 1. Multi-coded DSSS with 2 spreading codes

Spreading Code	Spreading Code	Code-bit
1	11001100101	0
2	11110000111	1

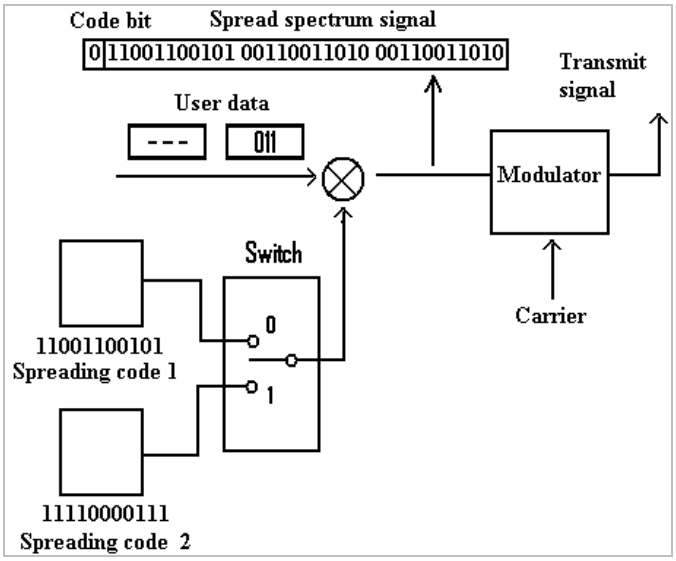


Figure 4. DSSS Transmitter with 2 spreading codes (Multi-Coded DSSS)

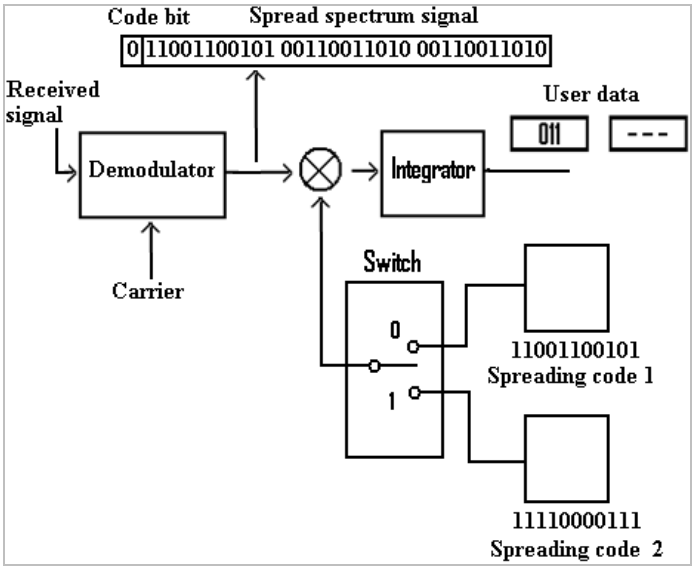


Figure 5. DSSS Receiver with 2 spreading codes (Multi-Coded DSSS)

Similarly, a multi-coded DSSS system can be implemented with the various number of spreading codes like four, eight, sixteen, and so forth. The size of the code-bits depends upon the number of spreading code used for spreading the data. For example, in case of four spreading codes the code bits 00, 01, 10 and 11 are used, while for eight spreading codes the code bits 000, 001, 010… 111 are used.

Table 2. Multi-coded DSSS with N spreading codes

Spreading Code	Spreading Code	Code-bit
1	11001100101	00
2	11111111110	01
3	00001111001	10
4	00110011001	11
…	…	…
N	01010101010	xxx

4. RSMC-DSSS

In this paper a new technique known as Random Selection of Multiple Spreading Codes Direct Sequence Spread Spectrum (RSMC-DSSS), a modified form of Multi-Coded-DSSS, is proposed to enhance or increase the security level of the transmission in wireless communication. In this technique the selection of the spreading code to spread the information signal data packet is set random rather than sequential. The spreading code selection is the only difference between the two, while rest of the procedure of transmitting and receiving information signal packet is similar. The spreading code selection can be achieved using shift registers or selection switches. The main advantage of this technique over the multi-coded DSSS is that the unauthorized users or eavesdroppers face the problem of finding that which spreading code is used to spread the considered information data packet. Like multi-coded DSSS, the RSMC-DSSS can also be design for N number of different spreading codes (like 2, 4, 8…so forth), depends upon the required level of security. The transmitter and receiver block diagrams for RSMC-DSSS technique using four different spreading codes are shown in Figure 6 and Figure 7 respectively. Here two code-bits instead of one will be placed along each spread data packet. In the same manner, the technique can be extended to any number of spreading codes.

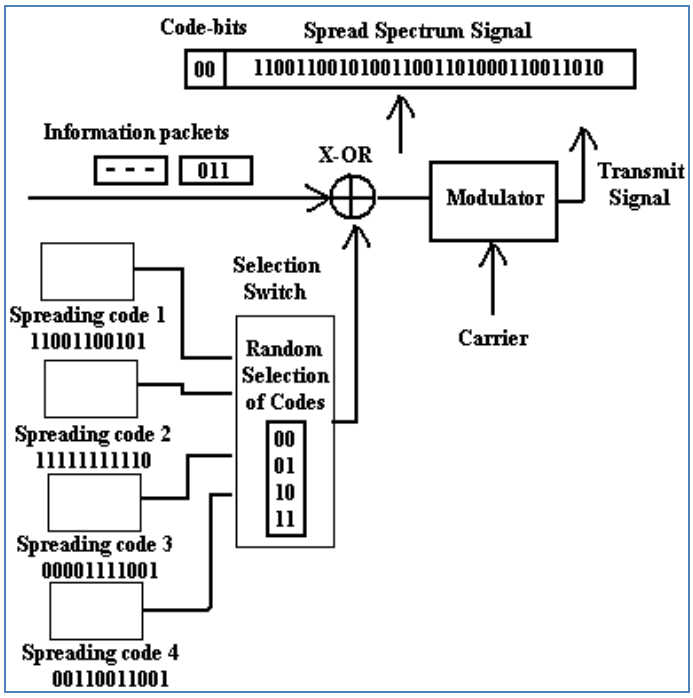


Figure 6. DSSS transmitter with 4 spreading codes (RSMC-DSSS)

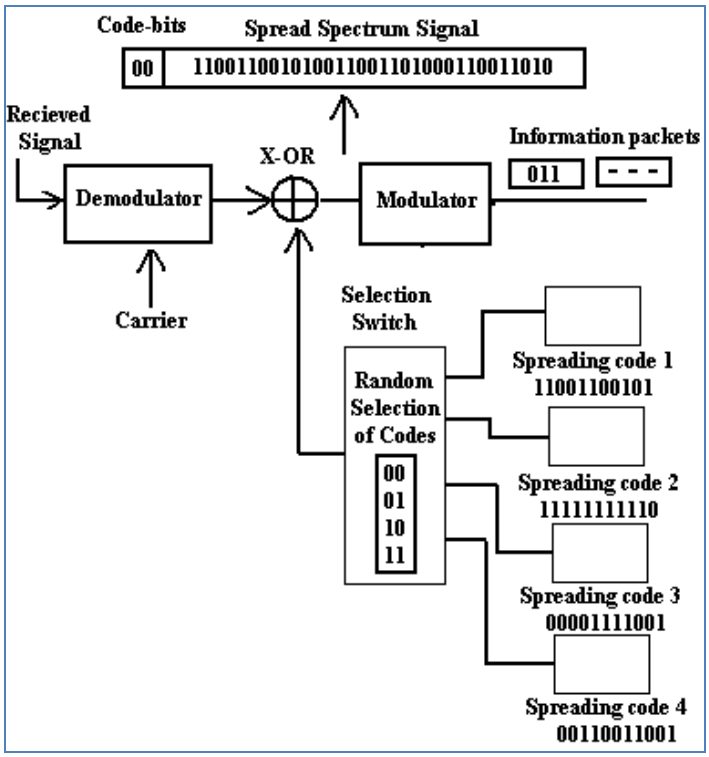


Figure 7. DSSS receiver with 4 spreading codes (RSMC-DSSS)

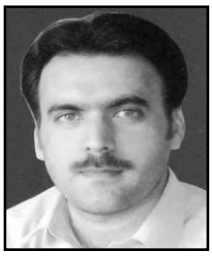
5. Conclusion

Two or more entities communicating and in need that a third party do not get or listen what they share or the entities need to communicate over secure channel in a way which is not susceptible to eavesdropping or interception is called secure communication. In Spread Spectrum, the spreading code/sequence and information signal multiplication is in use that possesses the advantage of security by its randomness. Only because the receiver knows the spreading code, it is possible to retrieve the signal. In this particular paper a new method named Random Selection of Multiple Codes Direct Sequence Spread Spectrum RSMC-DSSS is proposed to enhance the security of the existing DSSS systems by applying N number of spreading codes and their random selection in DSSS communication. The use of multiple spreading codes ensures that the proposed scheme produces much stronger transmission security in a communication system, while random selection of codes enhance further the security issue of that system. Moreover, the RSMC-DSSS can also be used with the BPSK system. RSMC-DSSS is an innovative technique and massive advancement over traditional DSSS system and also is the best technology choice for future secure transmission of information.

References

[1] S. -Y. Tang, P. Muller and H. 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.
[2] R. C. Dixon, "Spread spectrum Systems with Commercial Applications", 3rd edition, John Wiley & Sons, New York, **(1994)**.
[3] M. K. Simon, J. K. Omura, R. A. Scholtz and B. K. Levitt, Spread Spectrum Communications Handbook, McGraw-Hill, New York, **(1994)**.
[4] H. Taub, D. L. Schilling, "Principles of Communication Systems", 2ed, McGraw-Hill, New York, **(1986)**.
[5] S. Ananthi, R. Hariprakash, V. Vidya Devi and K. Padmanabhan, "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, AICT/ICIW 2006 IEEE, **(2006)**.
[6] A. S. Tanenbaum, "Computer Networks", Prentice Hall (India) Ltd., Fourth Edition, pp. 294-295.
[7] R. Tze and M. Sheng, "A Draft Proposal for Direct Sequence Spread Spectrum PHY Standard", IEEE P802.11, 93/38, **(1993)**.
[8] J. Boer, "Proposal for 2 Mbits/s DSSS PHY", IEEE P802.11-93/37, **(1993)** March.
[9] P. Struhsaker, "Physical Layer Draft Specification for 2.4 GHz Direct Sequence Spread Spectrum Media", IEEE P802.11-94, **(1994)** July.
[10] X. D. He, C. X. Pei and Y. H. Yi, "Despreader for direct sequence spread spectrum system and its performance analysis", Transactions of Tianjin University, vol. 16, no. 4, pp. 275-278.
[11] J. A. C. Bingham, "Multicamer modulation for data transmission: an idea whose time has come", IEEE Cornrnunication Magazines., vol. 28, no. 5, **(1990)** May, pp. 5-14.
[12] L. J. Cimini, Jr., "Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing", IEEE Transactions on Communications, vol. 33, no. 7, **(1985)** July, pp. 665-675.
[13] K. B. Letaief, J. C. -I. Chuang and R. D. Murch, "Multicode high-speed transmission for wireless personal communications", IEEE I995 Global Telecommunications Conference, Singapore, **(1995)** November.
[14] C. -L. I and R. D. Gitlin, "Multi-code CDMA wireless personal communications networks", Proceedings of 1995 IEEE International Conference on Communications, Seattle, USA, **(1995)** June, pp. 1060-1064.

Authors



Shahid Latif, Assistant Professor (Electronics) at Department of Computer Science and IT, Sarhad University of Science and Information Technology Peshawar Pakistan. Also, PhD Scholar at Department of Computer Science (DCS), University of Peshawar, KPK, Pakistan.

Rahat Ullah, Assistant Professor (Electronics) at Department of Computer Science and IT, Sarhad University of Science and Information Technology Peshawar Pakistan. Also, PhD Scholar at Institute of Physics and Electronics (IPE), University of Peshawar, KPK, Pakistan.