Securing Information by Using Encryption of Pseudorandom Code

Rahat Ullah[1], Shahid Latif[2]
Department of Computer & IT, Sarhad University of Science and IT Peshawar Pakistan[1, 2]
Rahat.csit@suit.edu.pk[1], shahid22latif@yahoo.com[2]

Abstract. The main task of frequency hopping spread spectrum is to secure the information from the detectors. In FHSS a pseudorandom code is multiplied with each of the information packet, which makes a hop. These codes randomly changes for securing the communication and also these codes are used in FHSS for indicating the carrier frequency at the receiver side. As in today's world the prime goal of wireless communication is security of information, although FHSS provide security but it has a threat from the unknown interceptor, if the hijacker come to know that sequence of pseudorandom than for surely the security will be collapsed. To save that data from leaking out, we have generated a new idea. If we use pseudorandom random code with one hop of the frequency and use the encoded form of pseudorandom code for the next hop, than the security level will be increase.

Keywords: Spread Spectrum, Frequency hopping spread spectrum, Encryption techniques, Security of communication.

1 Introduction to Spread Spectrum

Spread spectrum which is know a day's using for commercial usage and was initially used for military applications, provides a secure transmission from jamming because wireless communication/transmission has a threat to be jammed [1]-[3]. In spread spectrum communication the spreading sequence plays a vital role which spread the information in SS-signal which increases the security level of the signal [4]. The spread spectrum technique provides an anti- jamming communication by spreading the signals having wideband frequency [5] as shown in fig.1, while at the receiver side the information can be easily dig up from the SS-signal. Spread spectrum has many techniques [6][7], which are used for many applications i.e. security/ robustness of broadcasting the link, security of communication, fast speed rate, anti-interference ability[8-11].

1.1 Frequency Hopping Spread Spectrum (FHSS)

The carrier's frequency is arbitrarily changes in FHSS, the signals jumps at different carrier frequencies randomly according to the pseudorandom code, which specifies the carriers frequency at the receiver side because at the transmitter side each of the hop of frequency have this code for identity of carriers frequency [12]. In FHSS the pseudorandom code is used for the identification of the carrier frequency.

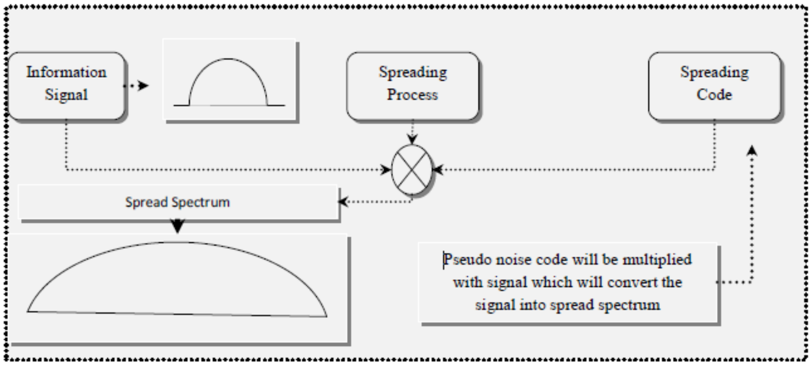
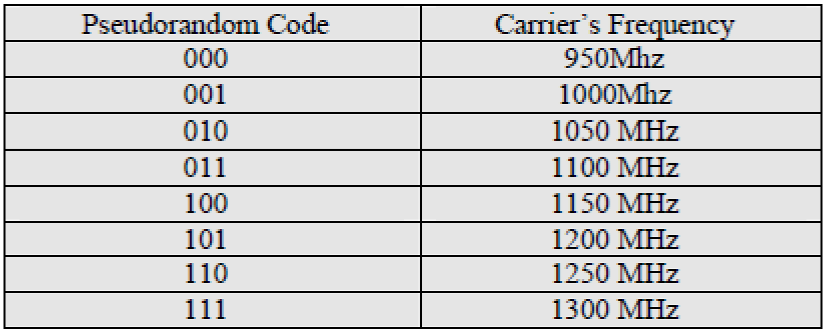

Information Signal
Spreading Process
Spreading Code
Spread Spectrum
Pseudo noise code will be multiplied with signal which will convert the signal into spread spectrum

Fig.1 Spreading of a signal using pseudo-noise code

Suppose we have a total bandwidth of 400 MHz from 900 MHz to 1300 MHz, and at this instant of time we use three bits of spreading code having the given sequence 000, 001, 010, 011, 100, 101, 110, 111. So we can divide the given bandwidth into eight different frequencies, 950Mhz, 1000Mhz, 1050Mhz, 1100Mhz, 1150Mhz, 1200Mhz, 1250Mhz, & 1300Mhz. Table.1 show that how the pseudorandom code will identify the carrier's frequency.

Table.1 Usage of Pseudorandom Code, identifying carrier frequency

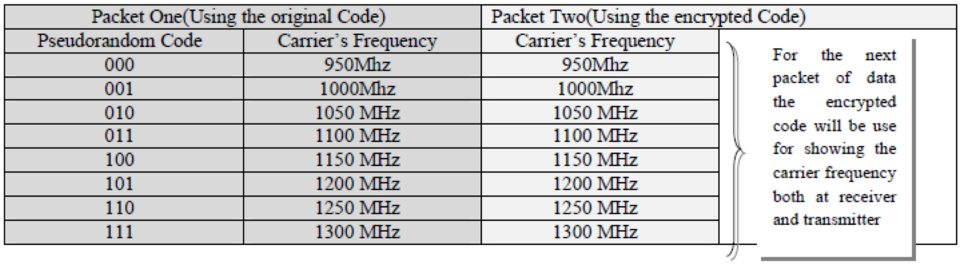


Pseudorandom Code	Carrier's Frequency
000	950Mhz
001	1000Mhz
010	1050 MHz
011	1100 MHz
100	1150 MHz
101	1200 MHz
110	1250 MHz
111	1300 MHz

2 Proposed Work

The security matters in the field of wireless communications and in frequency hopping spread spectrum, the pseudorandom code is using for the identification of carriers frequency of each hop, but if someone get some information or suppose it succeeds in breaking out that sequence of random codes than the integrity of information will be lose. To overcome this draw back we have proposed/designed a technique in which the original pseudorandom code and its encrypted code will be use consecutively, so that if some break the sequence code than after breaking that security, they will still be unable to leak out the secure information. It depends on the designer that what encryption technique they use for encryption. Only the receiver will be able to get the original information, because it will know about the encryption technique used for encryption of random sequence and also the original pseudorandom code. Table.2 will show the main concept of the paper that how both the original and the encrypted pseudorandom code will be use in the FHSS technique.

Table.2 showing the main idea of the paper
The left two columns shows the use of original code for packet one and the right columns shows the use of encrypted code



Packet One(Using the original Code)		Packet Two(Using the encrypted Code)	
Pseudorandom Code	Carrier's Frequency	Carrier's Frequency	
000	950Mhz	950Mhz	For the next packet of data the encrypted code will be use for showing the carrier frequency both at receiver and transmitter
001	1000Mhz	1000Mhz	
010	1050 MHz	1050 MHz	
011	1100 MHz	1100 MHz	
100	1150 MHz	1150 MHz	
101	1200 MHz	1200 MHz	
110	1250 MHz	1250 MHz	
111	1300 MHz	1300 MHz	

References

1. R. A. Poisel, Modern Communications Jamming Principles and Techniques, Artech House Publishers, 2006.
2. D. Adamy, A first course in electronic warfare. Artech House, 2001.
3. B. Sklar, Digital communications: fundamentals and applications. Prentice-Hall, 2001.
4. Fanxin Zeng, Zhenyu Zhang, “Binary sequences with Large Family Size and High Linear Complexity for Spread Spectrum Communication Systems”, 2010 2nd International Conference on Signal Processing Systems (ICSPS).
5. Christina P¨opper, Mario Strasser, “Anti-Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques”, ieee journal on selected areas in communications, vol. 28, no. 5, june 2010.
6. K. Fazel and S. Kaiser, “Multi-carrier and sprad spectrum system,” John Wiley and Sons Ltd., 2003.
7. M. K. Simon, J. K. Omura, R. K. Scholtz, and B. K. Levitt, “Spread spectrum communications handbook,” McGraw-Hill, Inc., 1994.
8. P. G. Flikkema, “Spread-spectrum techniques for wireless communication,” IEEE Trans. Signal Proc., vol. 14, pp. 26–36, May 1997.
9. C. WANG and M. AMI N. “Performance analysis of instantaneous frequency-based interference excision techniques in spread spectrum communications,” IEEE Trans. Signal Proc., vol. 14, pp. 70–82, August 1998.
10. T. Samanchuen and S. Tantaratana, “A closed-loop noncoherent pseudonoise acquisition scheme for direct-sequence spread-spectrum systems,”IEEE Conf. Circuits and Systems, Tailand, pp.97–100, November 1998.
11. Suwon Kang and Yong-Hwan Lee, “Rapid acquisition of PN signals for DS/SS systems using a phase estimator,” IEEE Journal on Selected Areas in Communication, vol. 6, pp.1128–1137, June 2001.
12. Behrouz A Fourozan, “Data Communication and Networking”, Fourth Edition, The McGrah-Hilll companies.