Security Improvement by using Dual Coded FHSS (DC-FHSS)

Rahat Ullah
Department of Computer Science and IT
Sarhad University Peshawar
Pakistant

Amjad Ali
Electrical Engineering Department
Sarhad University Peshawar
Pakistant

Shahid Latif
Department of Computer Science and IT
Sarhad University Peshawar
Pakistant

ABSTRACT

In this paper a technique is offered for improving the security of data transmission. In today's technical world the prime objective of wireless communication is to make the transmission not only clear, noise free and time efficient but also to make it well secure from unauthorized interceptors. Frequency hopping is a technique used for this purpose in which the random sequence is used to add with each hop of frequency which is used to change randomly at every instant. There was a draw back that if the attacker comes to know the sequence code for selecting the carrier frequencies, than the integrity of our information could be loss. To conquer this problem we have offered an algorithm in which the pseudorandom and its encrypted form both will be used. Its name is Dual Coded FHSS (DC-FHSS).

Keywords

Spread spectrum, FHSS, Pseudorandom Code, Encryption, Decryption

1. INTRODUCTION

Wireless transmission always has a threat from attacker to jam the transmission. For saving the transmission, spread spectrum (SS) technique represents a frequent way for achieving an anti-jamming communication [1]-[3]. SS is used in many applications as in military and commercial usage from device to device or from one device to many receiving devices [4]. The techniques used in spread spectrum, spreads the narrowband information into the wide band by using random sequence(code) or also called spreading code [5]-[7] as shown in fig.1. In fig.1 the signal having bandwidth "B" is converted to spread spectrum having bandwidth "B_{SS}". The spreading code is Ex-ORED with the information which transform the narrow band into wide-band information. The main function of spreading sequences is to increase the security and enlarging the user size [15]. By using SS techniques it is infeasible for an attacker to jam the wideband frequency [4] while the information is easily retrievable for the receiver by having the exact replica of random sequence. Some of the applications of spread spectrum(having random-sequence) are multi-carrier spread spectrum communication system [13], direct sequence code division multiple access (DS-CDMA) communication system [14], which gives good security, high speed rate, anti interferences ability [8-11]. The fundamental instances of spectrum spreading are direct sequence spread spectrum(DSSS), frequency hopping spread spectrum(FHSS), time hoping spread spectrum(THSS) and hybrid of the these [16]. The mentioned techniques are using for a variety of reasons i.e. robustness or security of a radio link, prevent detection, secure communication, multiple access between a number of users, noise or anti jamming of the communication, decreasing the interference etc. Among the mentioned one or more spread spectrum techniques are in use know days particularly for military radar, or police communications [17]. The Wireless LAN in IEEE uses spread spectrum, the band of 2.4 GHz [18]. Figures 1 shows the spreading of signal at the transmitter side. Repeater is used to converts one bit into eleven bits which is than Ex-OR with the code for encryption. Figure 2 shows the receiving of spreaded signal and its conversion into original narrowband information. At receiver side the packets of encrypted bits is Ex-ORed with the code and pass through the integrator which give the output in a single bit. Integrator selects the majority bit to be dispatched.

2. SUMMARY OF SPREAD SPECTRUM

The frequency hopping spread spectrum techniques uses *M* different carrier frequencies that are modulated by the source signal [19]. In FHSS the carrier frequencies are changes continuously; at one instant the signal modulates one carrier frequency while at a very next moment the carrier jumped to the next carrier frequency. Although in FHSS a number of frequencies are using as a carrier, but only one frequency can be used at a time for modulation [19]. The spreading sequence is the sequence of bits which indicates the carrier frequency. Table 1 explains the use of spreading sequence for indicating the carrier frequency through which one packet of data will be transmitted through these hops of frequencies. The sequence of codes used for indicating the carrier frequency of each hop. These codes should be known to the receiver for selecting the frequency to demodulate the information. For example the sequence 0001 is used to indicate that the carrier frequency is 950 MHz and similarly 1111 is used for 1650 MHz frequency.

The table reveals that the packet of information will be transmitted in 18 different frequency hops. In FHSS the transmitter and receiver must use the same carrier frequency

for modulation/demodulation to comprehend the information. We used four bits for codes for selecting the carrier frequency for modulating the data while the pseudorandom code is of long sequence of bits for security purpose. The longer the code, superior will be the security because by using long sequence of bits it will have no repetition in a short period of time. Fig.3 and 4 shows the block diagrams of transmitter and receiver used in FHSS.

3. PROPOSED TECHNIQUE

In wireless communication the main goal is to make the information secure. In this paper we have designed an algorithm which increases the security of transmitted information. In FHSS a pseudorandom code indicates the carriers frequency but if someone hijacks that sequence of codes than they may leak out all the secure information. We have offered the encryption if pseudorandom code used in FHSS, and called it grey coded frequency hopping spread spectrum (GC-FHSS). The encryption of random sequence is done using grey code, to know about grey code and its conversion from binary to grey can be study in [21], a method is also discussed in [21], in which they showed that how an Ex-OR gates can be used for that conversion. In our proposed algorithm both the original pseudorandom code and its encrypted form will be used. At the very start of transmission the original code will be use; encrypted code will be use for the next hop. By doing this the security will be automatically increases because if the hijacker comes to know the original code than it will not be able to leak out the information because of the encrypted code. Fig.1 and Fig.2 shows that how original and encrypted code will be use to specify the carrier frequency. Also On comparing table.2 and Table.3, we can get the result that how the code changes for indicating the carrier frequency. The conversion of binary to grey code can be achieved in two ways.

The same table.2 is redrawn in table 3 in a different format, where the original and encrypted pseudorandom codes are indicating the carrier frequencies for packet one and two. The encryption of codes should be known at the receiver for synchronization. The original codes will be used for odd packets of data while the even packet can only be de-modulate by using the frequency indicated by the ciphered code (encrypted/hidden code). So it means that by using this dual coded FHSS, the security level is increased because if the attacker comes to know the sequence of original codes than it will not be able to break the encrypted codes.

4. CONCLUSION

In proposed algorithm, the security level of information increases which is the prime objective of spread spectrum. By using the pseudorandom code with its encrypted form will secure the information, even if the attacker comes to know the sequence of codes. Because the consecutive packet of data will be ride over on the encrypted carrier frequency. We have used grey code for encryption, but one can apply the modern and advance techniques for encryption of codes as well. Other applicable encryption techniques are vigenere cipher, DES, AES [22]. My future work includes the experimental work and formulations of these different techniques and its impact on the security level of sensitive data.

5. 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] 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

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

[6] M. K. Simon, J. K. Omura, R. A.Scholtz, B. K. Levitt, Spread Spectrum Communications Handbook, McGraw-Hill, New York, 1994.

[7] H. Taub, D. L. Schilling, Principles of Communication Systems, 2ed, McGraw-Hill, New York, 1986.

[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] Huang He, Liang Yan, Zhao Chunhui, Pan Quan, "Design of A Spread Spectrum Communication System Based on DSP", Proceedings of the 2011 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems March 20-23, 2011, Kunming, China.

[13] K. Fazel and S. Kaiser, "Multi-carrier and sprad spectrum system," John Wiley and Sons Ltd., 2003.

[14] M. K. Simon, J. K. Omura, R. K. Scholtz, and B. K. Levitt, "Spread spectrum communications handbook," McGraw-Hill, Inc., 1994.

[15] 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)

[16] M. K. Simon, J. K. Omura, R. A.Scholtz, B. K. Levitt, Spread Spectrum Communications Handbook, McGraw-Hill, New York, 1994.

[17] S.Ananthi, R.Hariprakash, V.Vidya Devi, 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) 0-7695-2522-9/06 $20.00 © 2006 IEEE.

[18] Andrew S.Tanenbaum, Computer Networks, pp.294-295,Prentice Hall (India) Ltd., Fourth Edition.

[19] Behrouz A Fourozan, "Data Communication and Networking", Fourth Edition, The McGrah-Hilll companies.

[20] Yazdi Z.Z, Nasiri-Kenari M.,"Mutiuser performance comparisons of frequency hopping and multicarrier slow frequency hopping systems: uncoded and coded schemes ", 6th IEEE Vehicular Technology Conference, 2004.

[21] Floyd, "Digital fundamental", Chapter No.6 Eighth Edition edition.

[22] William Stallings "Cryptography and Network Security", 4th Edition.

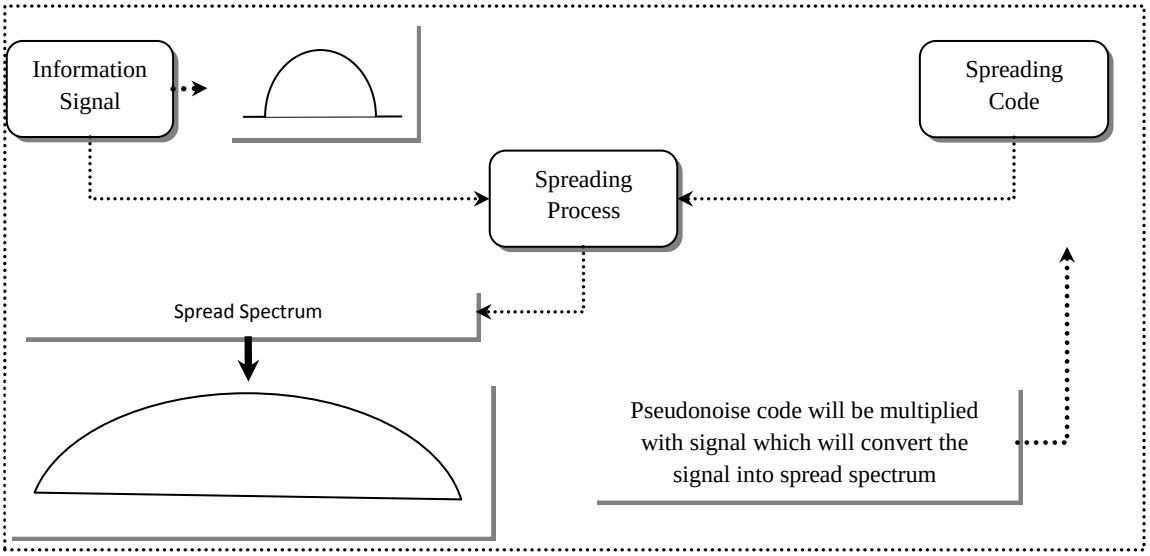

Fig.1 Conversion of a narrowband signal into wideband signal

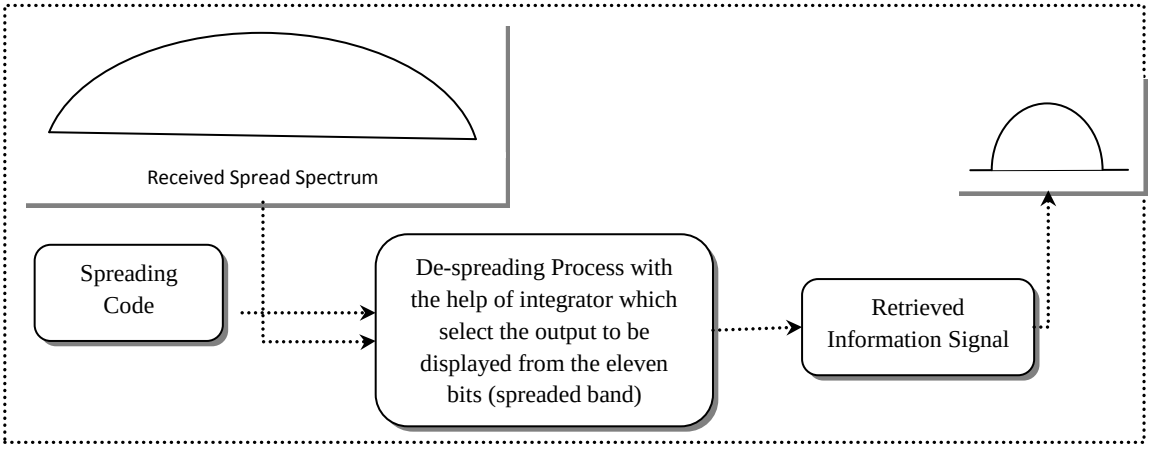

Fig.2 Retrieving the original narrowband signal from spread spectrum

Table.1 Code-Sequences showing the carrier frequencies for packet-1 and packet-2 of data

Packet-1		Packet-2	
Spreading code	**Carrier Frequency(MHz)**	**Spreading code**	**Carrier Frequency(MHz)**
0000	900Mhz	0000	900Mhz
0001	950Mhz	0001	950Mhz
0010	1000Mhz	0010	1000Mhz
0011	1050Mhz	0011	1050Mhz
0100	1100Mhz	0100	1100Mhz
0101	1150Mhz	0101	1150Mhz
0110	1200Mhz	0110	1200Mhz
0111	1250Mhz	0111	1250Mhz
1000	1300Mhz	1000	1300Mhz
1001	1350Mhz	1001	1350Mhz
1010	1400Mhz	1010	1400Mhz
1011	1450Mhz	1011	1450Mhz
1100	1500Mhz	1100	1500Mhz
1101	1550Mhz	1101	1550Mhz
1110	1600Mz	1110	1600Mz
1111	1650Mhz	1111	1650Mhz

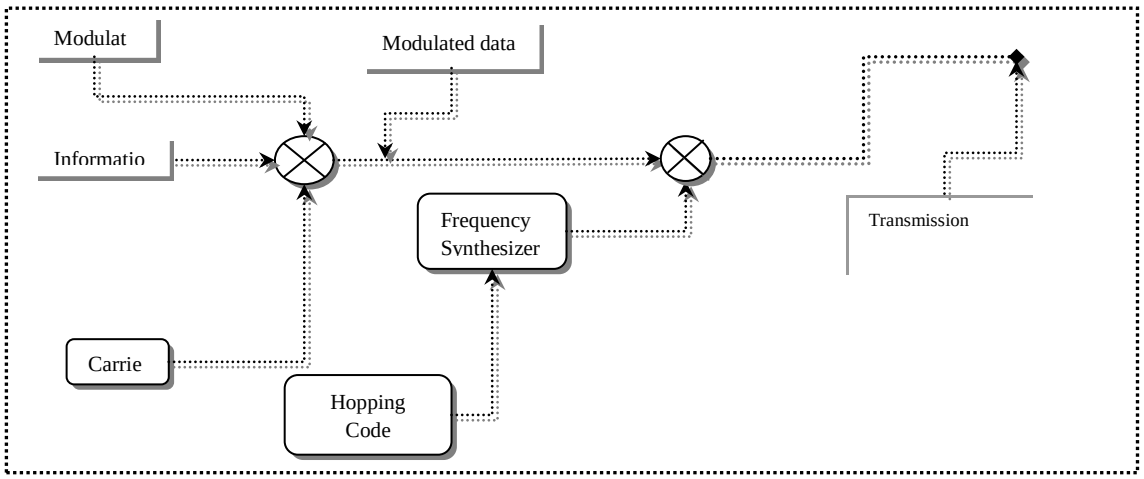

Fig.3 Simplified diagram of transmitter for FHSS

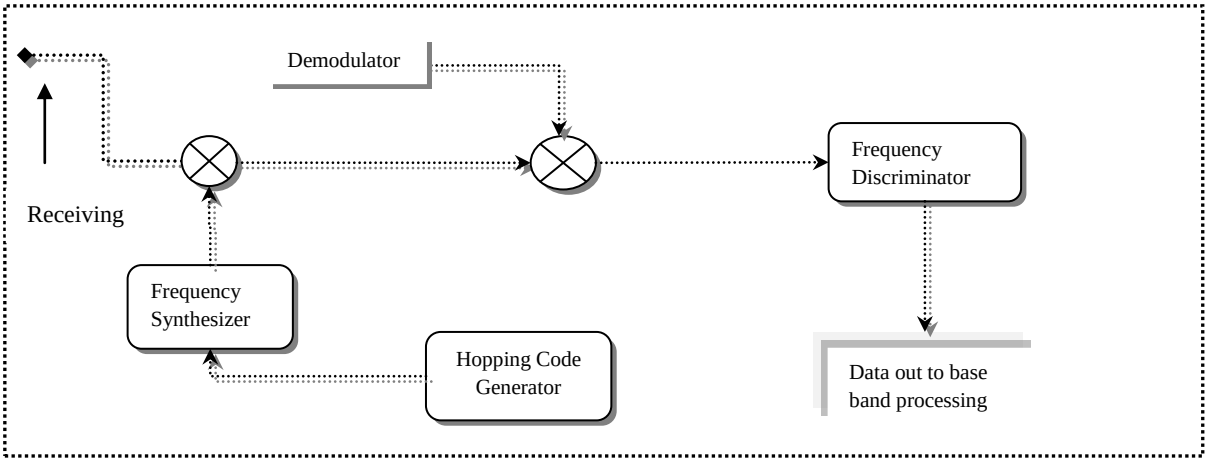

Fig.4 Simplified diagram of receiver for FHSS

Table.2 Two cycles of FHSS using original and encrypted pseudorandom codes

Packet-1		**Packet-2**	
Spreading code	**Carrier Frequency(MHz)**	**Spreading code**	**Carrier Frequency(MHz)**
0000	900Mhz	0000	900Mhz
0001	950Mhz	0001	950Mhz
0010	1000Mhz	0011	1000Mhz
0011	1050Mhz	0010	1050Mhz
0100	1100Mhz	0110	1100Mhz
0101	1150Mhz	0111	1150Mhz
0110	1200Mhz	0101	1200Mhz
0111	1250Mhz	0100	1250Mhz
1000	1300Mhz	1100	1300Mhz
1001	1350Mhz	1101	1350Mhz
1010	1400Mhz	1111	1400Mhz
1011	1450Mhz	1110	1450Mhz
1100	1500Mhz	1010	1500Mhz
1101	1550Mhz	1011	1550Mhz
1110	1600Mz	1001	1600Mz
1111	1650Mhz	1000	1650Mhz

Table.3 Presentation of table.2 in a different way

0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

Original Pseudorandom Codes indicating the carrier frequency in MHz for packet-1 of data

900	950	1000	1050	1100	1150	1200	1250	1300	1350	1400	1450	1500	1550	1600	1650

Encrypted Pseudorandom Codes indicating the carrier frequency in MHz for packet-2 of data

0000	0001	0011	0010	0110	0111	0101	0100	1100	1101	1111	1110	1010	1011	1001	1000

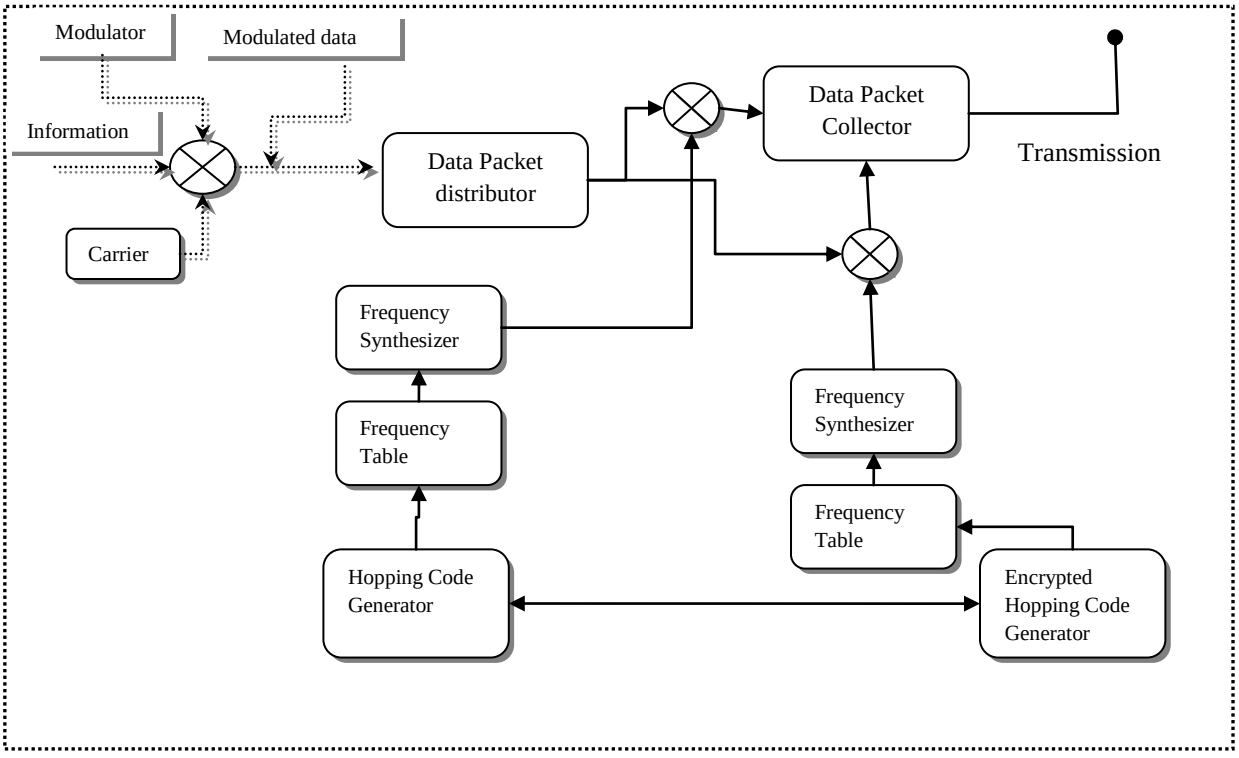

Fig. 5 Transmitter of Proposed Technique

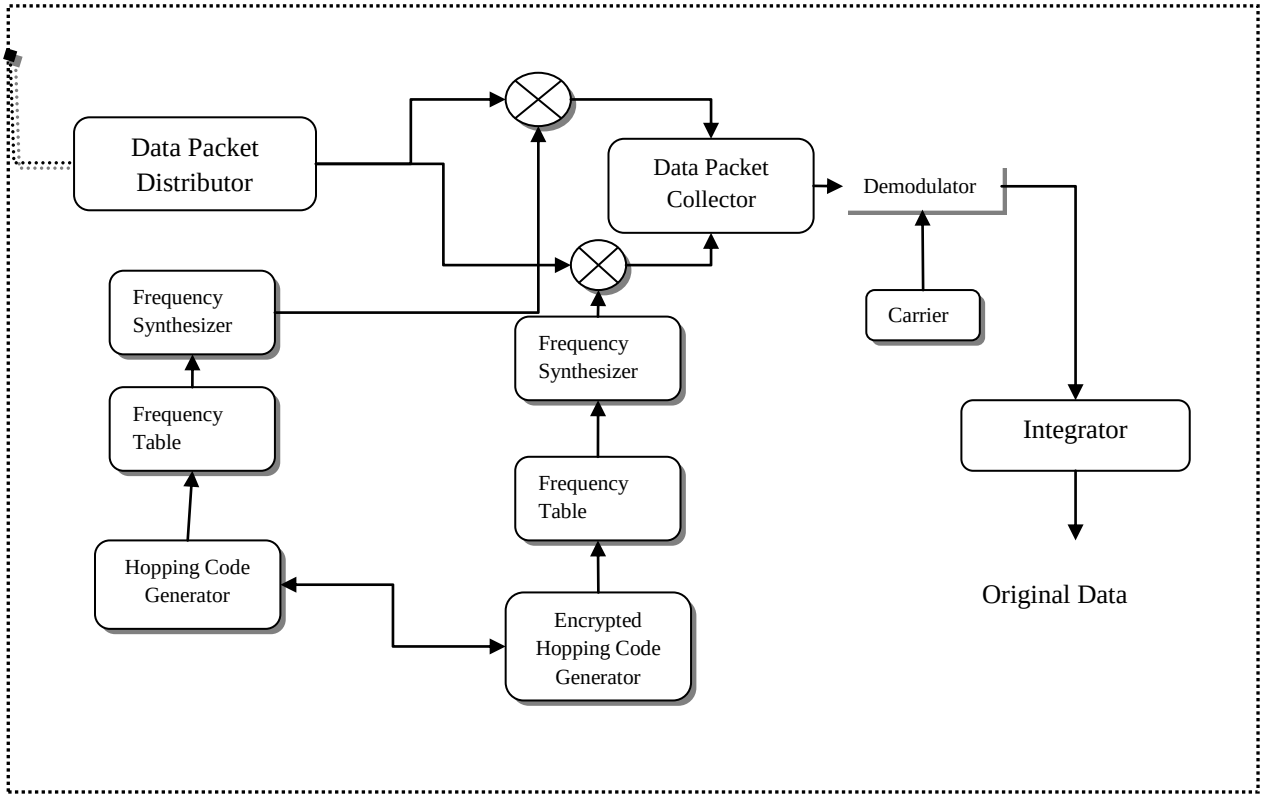

Figure.6 Receiver of Proposed Technique