IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 62-70
www.iosrjournals.org

Security Enhancement of Frequency Hopping Spread Spectrum Based On Oqpsk Technique

Vembu . M [1] ,Navaneethan . S [2]
[1] *Pg Scholar , Dept. of ECE , M.A.M College of Engineering , Trichy, India*
[2] *Associate Professor , Dept. of ECE , M.A.M College of Engineering , Trichy, India)*

Abstract: *Frequency hopping spread spectrum is an efficient technique to combat jamming. In this paper we analysis the effect of partial band noise jamming in Frequency hopping spread spectrum system. We consider a communication system that transmits OQPSK over a channel. Frequency Hopping Spread Spectrum (FHSS) system is often deployed to protect wireless communication from jamming or to preclude undesired reception of the signal. Such themes can only be achieved if the jammer or undesired receiver does not have the knowledge of the spreading code. For this reason, unencrypted M-sequences are a deficient choice for the spreading code when a high level of security is required. The primary objective of this paper is to analyze vulnerability of linear feedback shift register (LFSRs) codes. Then, a new method based on encryption algorithm applied over spreading codes, named hidden frequency hopping is proposed to improve the security of FHSS. The proposed encryption security algorithm is highly reliable, and can be applied to all existing data communication systems based on spread spectrum technique*.

Keywords: *Frequency Hopping Spread Spectrum; Key Encryption Key; Linear Feedback Shift Register; Frequency Hopping Code Division Multiple Access; Direct Sequence Spread Spectrum;oqpsk*

I. INTRODUCTION

Further employment of wireless communication system to exchange vital and critical electronic information requires an urgent attention to design reliable secure systems. This requirement is further strengthen for military communication systems where information transmission heavily relies upon wireless networks [1].

In fact the major advantage of a mobile set narrowband signal transmission is its efficient use of available frequency due to only a fraction of signal transmission frequency being used for a single subscriber.

Indeed, a drawback is obvious, as it requires a well coordinated frequency allocation for different subscribers' signal which are now quiet vulnerable to signal jamming and interception.

In [2,3], the fundamental goal of spread spectrum system is considered as; to increase the dimensional characteristic of the signal, hence, to make eavesdropping and/ or jamming more difficult since there are more Security Enhancement Of Frequency Hopping Spread Spectrum Based On OQPSK Technique dimensions of the signal to consider. In fact, the main method of increasing the dimensionality of the signal is to widen the signal's spectral occupancy [2,3].

In spread spectrum techniques, security against tapping and jamming is greater compared with narrowband spectrum techniques. Signals of spread spectrum are in- distinguishable from background noise to anyone who does not know the coding scheme. The disadvantage of spread spectrum is its relatively high complexity of the coding mechanism which results in complex radio hardware designs and higher costs. Nonetheless, because of its remarkable advantages, spread spectrum has been adopted by many wireless technologies. For example, the IEEE 802.11b standard for wireless LAN employs DSSS over the 2.4-GHz free spectrum, whereas the Bluetooth standard uses frequency hopping spread spectrum (FHSS) for simplicity [1-3].

A spread-spectrum transmission provides three main advantages:

- Avoids narrow band interference
- Difficult to intercept spread spectrum signals.
- Provides minimal interference when sharing the frequency band with other Conventional transmissions.

Furthermore, the main weakness of the wireless communication security system is the simplicity of accessing the communicating signal through the channel. Eavesdroppers can easily place an antenna in the desired field and after demodulation, the message bits can be obtained in the base-band form. If the messages are encrypted, after storing the encrypted messages with some crypto- analysis methods, the original message can be smeared out. Now, if the received radio signals from the wireless channel is spread in a form that the intruder cannot access the despread spectrum and receives only a signal similar to noise, a perfectly secure radio transmission.

Moreover, specifically the security of the frequency hopping code division multiple access (FH-CDMA) system mainly relies on the long-code generator that consists of a 42-bit long-code mask generated by a 42-bit LFSRs. However, if eavesdroppers can obtain 42 bits of plaintext-cipher-text pairs, the long-code mask can be recovered after dropping the transmission on the traffic channel for about one second [3,6,7].

The fast correlation attack method based on a recently established linear statistical weakness of decimated LFSR sequences for reconstruction of LFSR code is described in [8]. With this method eavesdropper can re- cover LFSR sequence that he knows the LFSR feedback polynomial. A method of blind estimation of PN code in multipath fading direct sequence spread spectrum systems is proposed in [9]. In this article a combed method is presented to estimate the unknown PN spreading sequence for direct sequence spread spectrum (DS-SS) signals in frequency selective fading channel. It is proven that LFSR codes are vulnerable to cipher-text-only at- tacks [10] and security weakness of white Gaussian sequence is investigated in [11].

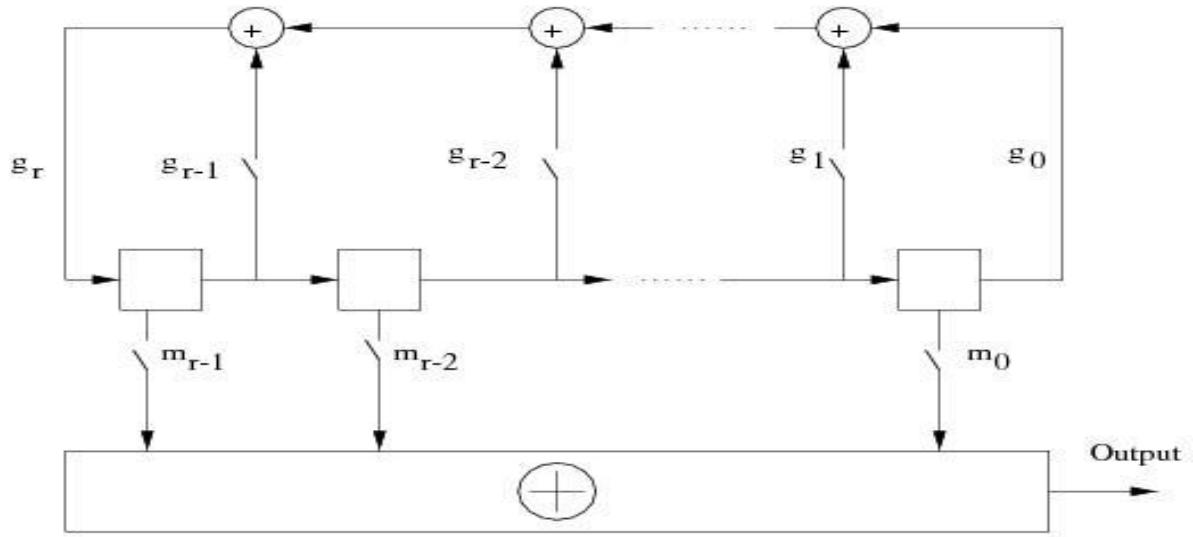
This preface and further studies show that LFSR codes, white Gaussian sequences and other unencrypted codes have security weaknesses and can be recovered by eaves- droppers. So a method which can guarantee systems against the probable attacks is urgently required.

In this manuscript, a new method called hidden frequency hopping spread spectrum is proposed to augment the built-in security of FH-CDMA systems by applying cryptographic algorithm in the channelization code sequence.Security Enhancement Of Frequency Hopping Spread Spectrum Based On OQPSK Technique

II. SYSTEM MODEL

A. PN Sequences

PN sequences are deterministic, periodic and binary sequences with a noise like wave form. It is also called Pseudo random noise as it seems random for the user who has no idea about the code. The longer the period of PN spreading code, the harder will be the detection of the sequence (Fig. 1). This sequence is generated by feedback shift registers which is made of m flip-flops with two states memory stages.



B. Spread Spectrum

Bandwidth and signal power plays an important role in any digital communication systems. These two key parameters must be improved to reach effective performance and efficient communication. But, in some cases, this efficiency must be sacrificed to provide security which is a significant objective in communications. There is no usage of system, if messages are detected by unwanted listeners. The major advantage of Spread Spectrum (SS) is the ability to reject interferences whether it is the unintentional interference that can be occurred due to another user trying simultaneously to transmit over the channel or the intentional interference (i.e. another trying to jam the transmission). A spread spectrum modulation scheme is a digital modulation technique that utilizes a transmission bandwidth much greater than the modulating signal bandwidth, independently of the bandwidth of the modulating signal. There are several reasons why it might be desirable to employ a spread spectrum modulation scheme. Among these are to provide resistance to unintentional interference and multipath transmissions, resistance to intentional interference, signal with sufficiently low spectral level so that it is masked by the background noise and to provide a means for measuring range between transmitter and receiver. Fig. 2 shows the block diagram of a spread spectrum system.
Spread Spectrum modulation can be described in two ways:

Security Enhancement Of Frequency Hopping Spread Spectrum Based On OQPSK Technique

- The signal occupies a minimum bandwidth which is necessary to send the information.
- Spreading is done by means of spreading signal which is independent o

F the data and dispreading is accomplished by the correlation of the received spread signal with a synchronized of the spreading signal used to spread the information.

There has been an ongoing discussion concerning which spread spectrum technique to prefer in military systems. Spread spectrum dependent on a variety of factors given by the operational environment. Characterizing the environment and establishing consensus about the relative importance of the various factors influencing a system is usually a difficult task, particularly since some of these factors are largely dependent on conditions like geographical and topographical placement which are not fixed for mobile users. Some of the factors to consider are [13], [14]:

- Teleservices to support;
- Capability or co-existence with other systems;
- Operational area (urban environments or rural areas);
- Doppler frequency shifts caused by relative motions;
- Interference, both narrowband and wideband;
- Fading characteristics;
- Severe specular multipath;
- Necessity for message integrity;
- Response (blind acquisition required);

_ Etc.

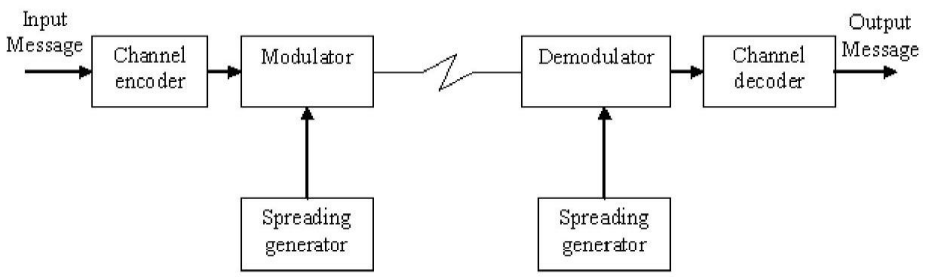


Figure 2. Architecture of spread spectrum (SS)

Spread Spectrum is a very convenient technology possessing the following advantages:

- Interference suppression.
- Cross talk minimization.
- Reduction of signals energy density
- Multiple channel accesses.
- Fine time resolution.

Security Enhancement Of Frequency Hopping Spread Spectrum Based On OQPSK Technique

There are two techniques widely used as Spread Spectrum (SS) modulation techniques: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopped Spread Spectrum (FHSS). Both methods can operate in presence of noise like spreading code called pseudo random sequence.

Frequency hopping spread spectrum

- It spreads the signal by hopping from one frequency to another across a bandwidth of 83 MHZ
- Jamming on one frequency affects only a few bits
- FHSS operation is typically 2^k carriers frequencies forming 2^k channels
- Channel spacing corresponds with bandwidth of input
- Each channel used for fixed interval
- Some number of bits transmitted using some encoding scheme

ADVANTAGES

- Simpler to implement
- No near/far problem

DISADVANTAGES

- Long latency time
- No processing gain
- Short outdoor range

Direct Sequence of Spread Spectrum

The prime objective of spread spectrum is the anti-jamming, noise free, and clear communication. Spread spectrum uses digitl diand 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.

III. PROPOSED SYSTEM MODEL

Although spread spectrum systems are used for narrow-band interference mitigation and have good efficiency in preventing intentional and unintentional channel interference, if jammer uses similar spreading

codes method, it can be successful in deteriorating such techniques. The level of signal destruction depends on similarity between jammer and transceiver PN codes. This mechanism is different for FHSS and DSSS systems but FH systems are desired. In this method, jammer operates intelligently, after accessing the channel and receive spread signals, it finds spreading technique and PN sequence pattern. Then it generates similar PN pattern and can synchronize itself with the transceiver system to track the modulation type. It should be mentioned that jammer can be located between transmitter and receiver so to provide the man in the middle attack. So jammer can interfere with data signal or change receiver to a useless one and mask itself as an allowable user.

A proposed hidden frequency hopping method can be used to prevent sequence pattern disclosure. Therefore, complexity in this process solely depends upon encryption complexity. Let's consider OQPSK transceiver which employs FHSS with encrypted PN sequences, Gaussian noise power and partial band noise jamming function j(*t*). Suppose that jammer can access channel and obtain de- sired information from this system.

Offset Quadrature Phase Shift Keying

Offset quadrature phase-shift keying (OQPSK) is a variant of phase-shift keying modulation using 4 different values of the phase to transmit. It is sometimes called staggered quadrature phase-shift keying(SQPSK).

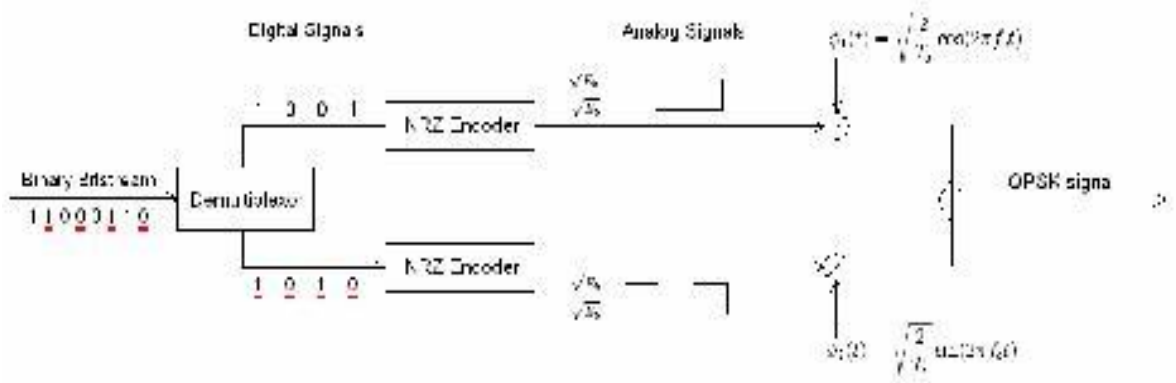


Fig 3:Block diagram of oqpsk

The input binary sequence is applied to demultiplexer and it divides into two separate bit streams of the odd numbered and even numbered bits. The first even bit occurs after the first odd bit. Therefore even numbered bit sequence starts with the delay of one bit period due to first odd bit. Thus first even bit is delayed by one bit period 'Tb ' with respect to first odd bit. This delay of Tb is called as offset. Hence the QPSK is named as OQPSK

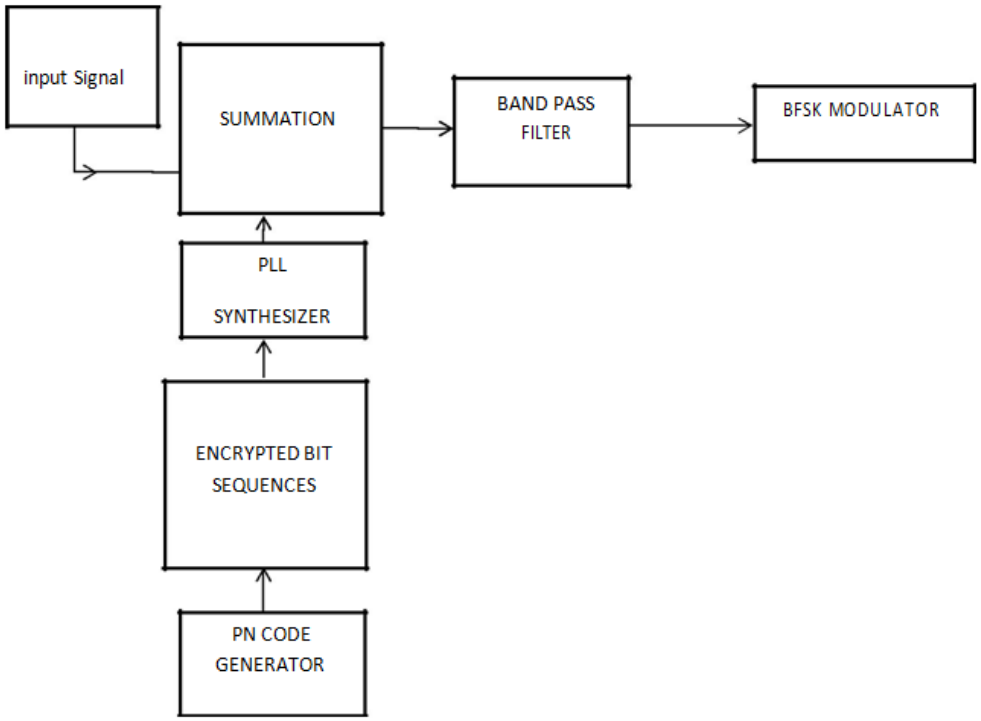


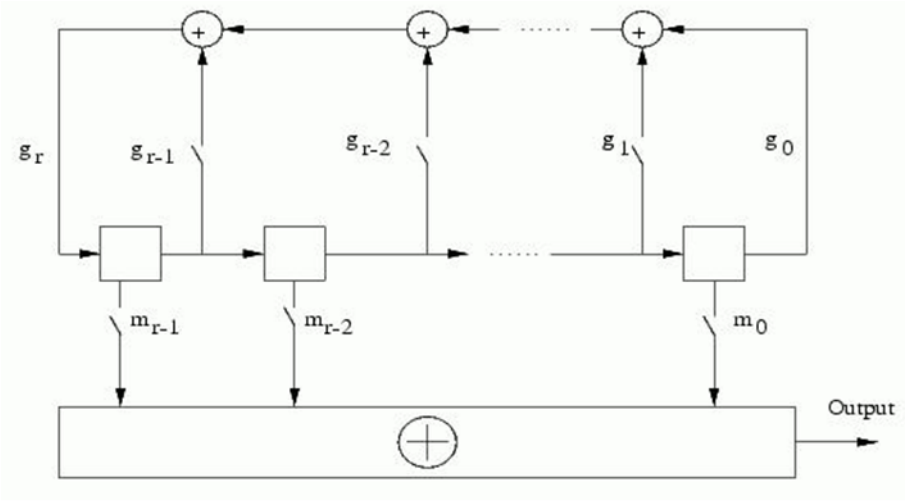
Fig 4: Proposed FHSS with hidden PN sequences for OQPSK receiver

PLL Synthesizer

A phase locked loop is a feedback control system. It compares the phases of two input signals and produces an error signal that is proportional to the difference between their phases. [11] The error signal is then low pass filtered and used to drive a voltage-controlled oscillator (VCO) which creates an output frequency. The output frequency is fed through a frequency divider back to the input of the system, producing a negative feedback loop. If the output frequency drifts, the phase error signal will increase, driving the frequency in the opposite direction so as to reduce the error. Thus the output is *locked* to the frequency at the other input. This other input is called the reference and is usually derived from a crystal oscillator, which is very stable in
frequency. The block diagram below shows the basic elements and arrangement of a PLL based frequency synthesizer. The key to the ability of a frequency synthesizer to generate multiple frequencies is the divider placed between the output and the feedback input. This is usually in the form of a digital counter, with the output signal acting as a clock signal. The counter is preset to some initial count value, and counts down at each cycle of the clock signal. When it reaches zero, the counter output changes state and the count value is reloaded. This circuit is straightforward to implement using flip-flops, and because it is digital in nature, is very easy to interface to other digital components or a microprocessor. This allows the frequency output by the synthesizer to be easily controlled by a digital system.

PN Sequence Generator

The PN Sequence Generator block generates a sequence of pseudorandom binary numbers. A pseudonoise sequence can be used in a pseudorandom scrambler and descrambler. It can also be used in a direct-sequence spread-spectrum system



All *r* registers in the generator update their values at each time step according to the value of the incoming arrow to the shift register. The adders perform addition modulo 2. The shift register is described by the **Generator Polynomial** parameter, which is a primitive binary polynomial in *z*.

Band Pass Filter:

A bandpass filter is an electronic device or circuit that allows signals between two specific frequencies to pass, but that discriminates against signals at other frequencies.

BPSK Modulation

BPSK (also sometimes called PRK, phase reversal keying, or 2PSK) is the simplest form of phase shift keying (PSK). It uses two phases which are separated by 180° and so can also be termed 2-PSK. It does not particularly matter exactly where the constellation points are positioned, and in this figure they are shown on the real axis, at 0° and 180°. This modulation is the most robust of all the PSKs since it takes the highest level of noise or distortion to make the demodulator reach an incorrect decision. It is, however, only able to modulate at 1 bit/symbol and so is unsuitable for high data-rate applications.

The jammer applies interference power on narrow band hopped channels randomly and so the bit error rate can be computed as

Ps-encrypted=Ps(error/hit) x Phit+Ps(error/no-hit) x Pno-hit---------- (1)

where PS presents symbol error probability and Phit is the probability of signal hitting the jammer.

Suppose that the transceiver and jammer have the same hop period TH, the number of hoped channel

NH with different start signaling. Because jammer doesn't have session key, it can't obtain spreading codes, synchronize with transceiver and to know start transceiver signaling. Thus, the time of transceiver signaling is given by

Tsent-signal= TH-Tso---------- (2)

Figure 4 describes the transceiver signal and jammer signal collision behaviour. So within this behaviour, the probability of jammer and transceiver signal hit in *k*-th hop is

Pno-hit=1-Phit---------(3)

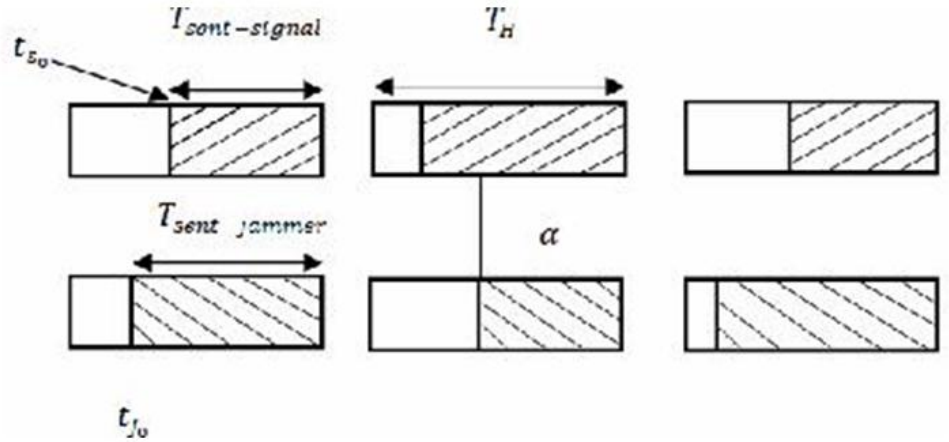


Fig 5: **Collision of jammer and transceiver signals.**

The cross-correlation of some codes such as Gold and Kassami is lower than the encrypted codes, so a method must be used to optimize the input interference of the system to an acceptable extent. For this reason, an interference threshold is selected for the channel according to the channel interference average for 100 or 1000 times tests. In these tests the channel minimum value interference are calculated and a constant threshold is selected for a channel with a number of users, then the multi-user interference is estimated for each user who enters the network and this value is compared with the threshold level. If the result is less than threshold level, the optimum pair "key-input" is saved for new user and the data is sent confidently such that the interference do not exceed the threshold level. If the interference value is more than the threshold level, the user has to generate another PN and give it to the cryptographer for generating a frequency whose interference is not more than the threshold level.

IV. SIMULATION RESULTS

The Simulation results show that when the proposed encrypted codes are utilized, the received channel interference increases. Naturally, this phenomenon makes the signal detection procedure more complex.

Therefore, an optimum pair "key-input" algorithm is proposed to re- duce the associated interference to the desired level. For instance, by employing codes with a good orthogonal behaviour, indeed, still algorithm can provide small amount of error but it also reduce the data transmission speed

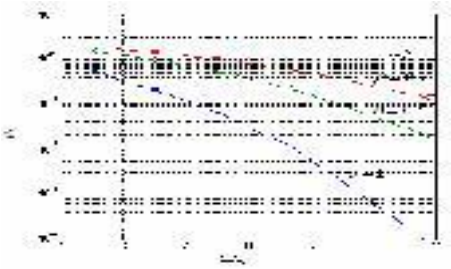


Figure 6. Degradation in FH/OQPSK performance due to worstcase, PBNJ with M =4.

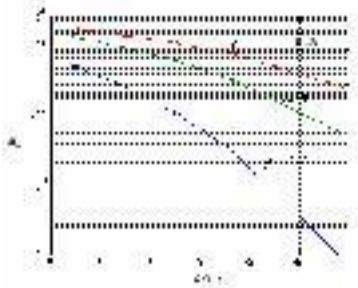


Figure 7. Degradation in FH/OQPSK performance due to worstcase, PBNJ with M =8

Figure 8. Degradation in FH/OQPSK performance due to worstcase, PBNJ with M =16.

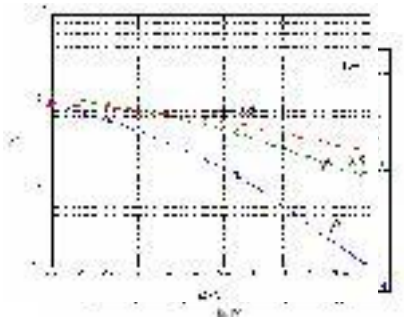


Figure 9. Degradation in FH/MFSK performance due to worstcase,PBNJ with M=2.

V. CONCLUSION

This paper provide frequency hopping spread spectrum operating in the presence of partial band noise jamming. The performance of the encrypted FH/SS code is as good as unencrypted sequences when correct key is applied. When a wrong key is employed, system security is guaranteed.

REFERENCES

[1]. P. Zheng, L. Peterson, B. Davie and A. Farrel, "Wireless Network Complete," Elsevier publisher,Amsterdam, 2009.
[2]. Telecommunications Industry Association, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System," Telecommunications Industry Association, Arlington, 1998.
[3]. M. Tafaroji and A. Falahati, "Improving Code Division Multiple Access Security by Applying Encryption Methods over the Spreading Codes," IET Communication, Vol. 1, No. 3, 2007, pp. 398-404. doi:10.1049/iet-com:20060295
[4]. J. L. Massey, "Shift-Register Synthesis and BCH Decoding," IEEE Transactions on Information Theory, Vol. 15, No. 1, 1969, pp. 122-127. doi:10.1109/TIT.1969.1054260
[5]. I. Mansour, G. Ghalhoub and A. Quilliot, "Security Architecture for Wireless Sensor Networks Using
[6]. Frequency Hopping and Public Key Management," IEEE International Conference on Networking, Sensing and Control (ICNSC), Delft,11-13 April 2011, pp. 526-531.