Signal Anti-Jamming Through Encrypted Spreading Codes Based On Frequency Hopping Spread Spectrum

Amit Kumar Tripathi¹ & Dr. Anjali Ashish Potnis²
¹Research scholar in Digital Communication, NITTTR Bhopal MP India
²Asst. Professor in DEEE Department, NITTTR Bhopal MP India

Abstract: Now a days is fully digitalized time and communication is one of the most important part in our modern life [1]. Everywhere digital system are present like railway, radar, satellite, missile launchers, GPS, Wi-Fi, radio transmission, cellular mobile communication, vehicles, sensors, etc. digital signal play very important role in digital communication system for assessment of signal security, anti-jamming is very important for secure communication system, interferences [2]. In present time many techniques are developed for anti-jamming but here we are focused on Frequency hopping spread spectrum anti-jamming improvement with Encrypted spreading codes. This technique is based on encrypted PN-sequence which is based on frequency hopping spread spectrum modulation technique. This technique give better result in signal anti-jamming in terms of signal-to-noise ratio, throughput and Bit error rate. This new method based on encryption algorithm applied over spreading codes, named hidden frequency hopping is proposed to improve the security of FHSS. Existing data communication systems based on spread spectrum techniques, which is very useful us.

This paper addresses a study of spread spectrum signal by analyzing the performance of the system using the MATLAB code. To achieve this, after a brief introduction the principles of the spread spectrum systems are explained in details, then the techniques of the detection which are used to retrieve the message signal are presented.

Key Words: Frequency hoped Spread Spectrum, PN-sequence, Anti-jamming, Signal to noise ratio, Bit error rate.

1. Introduction

Because FHSS is widely used in military applications, security purposes, satellite communication, radars, railways and many other reason that 'why interested in making this research in that direction'.

OBJECTIVES OF THE RESEARCH:

An exhaustive survey has been done which suggests immediate need of a method which should have the capability to predict exact security level of resistance of jamming and anti jamming signal network at each instant. In order to achieve this desired goal we have set certain objectives. So the research objectives are as follows:

i. Handling of signal jamming and anti-jamming using frequency hoped spread spectrum.
ii. Handling of imprecise, inaccurate and sparse data for jammed and anti-jammed signal.
iii. The proposed encryption security algorithm is highly reliable.
iv. Researcher needs a unique learning approach that work well, smoothly and stable under all circumstances.

PROBLEM STATEMENT:
“Signal anti-jamming through encrypted spreading codes based on frequency hopping spread spectrum”

PROBLEM SPECIFICATION:
Above mentioned problem statement is formulated in perspective of following problem specification:
1. Transmission bandwidth.
2. Bit error rate.
3. Signal to noise ratio.
4. Interference rejection.
5. Anti-jamming.
6. Low probability of intercept.
7. Multiple accesses.
8. High resolution ranging.
9. Multi-path suppression.
10. Diversity reception.

FEEQUENCY HOPPING SPREAD SPECTRUM:
Frequency hopping is a spread spectrum technique that involves partitioning the allocated frequency band, called the hopping band, into a large number of smaller Sub-bands. These sub bands are also called carrier frequencies, channels, tones, sub channels, or sub-carriers. Transmission is carried out in short bursts on one sub-band at time, hopping from sub-band to sub-band in a pseudo-random fashion after each burst [1].
TYPES OF SS BASED ON THE KIND OF SPREADING MODULATION:
Spread spectrum systems are broadly classified as-
(i) Direct sequence spread spectrum (DS-SS) systems.
(ii) Frequency hopping spread spectrum (FH-SS) systems
(iii) Time hopping spread spectrum (TH-SS) systems.
(iv) Hybrid systems.

BASIC BLOCK DIAGRAM OF FHSS:

Figure 1.1 Block diagram of FHSS

OUTCOMES:
The expected outcome of this proposed work is as follows:
i. There will be a generic and more efficient signal anti-jamming at the output.
ii. Reduction in transmission bandwidth.
iii. Bit error rate.
iv. Signal to noise ratio.
v. Interference rejection
vi. Multiple security states could be predicted.
vii. The encrypted spreading is expected to perform well, smooth and stable under all circumstances with improved signal ant jamming.

FLOW CHART OF RESEARCH METHODOLOGY:

Figure 1.2: Flow Chart of Research Methodology
In order to realize the above adapted technology, Encrypted bit sequence FHSS methodology is being proposed in this section. The experimental methodology has been elaborated through a schematic flow chart and can be carried out in a series of sequential steps given below:
- Modulator.
- Channel.
- Demodulator.

2. FHSS TRANSCEIVER MODEL:
FH/BPSK Transmitter Architecture:
In FH/BPSK transmitter, the input to the system is digital data, which is transmitted by varying its characteristics to the intended receiver. FH/BPSK transmitter architecture is shown in figure 2.1. The block describes the FH/BPSK system of the FHSS spreading and modulation the incoming signal to pass over a channel [4]. The FHSS transmitter architecture has four stages. At first, the digital data is taken as input the FH/BPSK system and makes synchronization with the clock signal. In order to reduce the attenuation, the incoming signal is processed with the carrier frequency to
modulate. Then FHSS spreading is carried out for the modulated signal with the help of spreading frequency. Finally, FHSS spreaded signal is send over a channel with the help of transmitter.

Fig 2.1 Block diagram of encrypted FHSS transmitter
FH/BPSK Receiver Architecture:
In FH/BPSK receiver end the received signal is fed to the mixer to which the output of a frequency synthesizer. The frequency of the signal produced by this synthesizer is controlled by a PN code generator which is identical to and synchronism with the one at the transmitter [5]. The set of frequencies produced by the frequency synthesizer and their hopping pattern are also exactly identical to these at the transmitter. The de-spread M-ary signal coming out from the BPSK.

IMPLEMENTATION FLOW CHART:
How research is proceeded step by step is discussed here. Flow chart for implementation flow chart shown below Fig 2.3:

3. RESULTS:
At the transmitter ends:
The MATLAB results at each step are shown below. The following figures demonstrate MATLAB results for encrypted spread transmission system. The results are displayed in the form of snapshots of scope signals. These figures demonstrate we can know easily what happens exactly inside a transmitter.

Fig 2.2 Block diagram of encrypted FHSS receiver

Figure 2.3. Flow chart of implementation technology
To perform the encrypted FHSS three main step follow. In first and second step information sequence is first modulated by base band BPSK, then mix with PN sequence which is FHSS then pass through the channel [6]. This encrypted sequence is not jammed by other user and not interference by other signal. In step-3 signal is demodulated and original signal is extract from the encrypted sequence.
Figure 3.1. At the transmitter end in MATLAB.

At the receiver end:
By observing these figures, we can know easily what happens exactly inside the Receiver. The transmitted signal is passed through a AWGN channel. The noisy version of the transmitted signal at the input of receiver is shown in Figure 3.2.

Figure 3.2. At the receiver end in MATLAB.

4. CONCLUSIONS
The results and performance analysis clearly shows that “Signal anti-jamming through encrypted spreading codes based on frequency hopping spread spectrum” is the far more efficient intelligent system based security assessment technique in comparison of conventional based technique. It gives higher precision to security assessment than other based system.

a) Result analysis of proposed method for digital system security analysis have performed well and shown high degree of accuracy [9].

b) Proposed method is highly efficient and fast enough for security assessment. Remedial action suggested were taken and verified [10].

5. REFERENCES:


[6] Myeongsu Han, Student Member, IEEE, Takki Yu, Member, IEEE, Jihyung Kim. OFDM channel estimation with jammed pilot detector under narrow-band jamming. IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 57, NO. 3, MAY 2008


BIOGRAPHIES:
2. Dr. Anjali Ashish Potnis. Assistant Professor from DEEE Department, NITTTR Bhopal MP India.