ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

INVESTIGATIONS ON THE PERFORMANCE ENHANCEMENT OF SELF ENCODED SPREAD SPECTRUM IN WIRELESS COMMUNICATION

Kavitha Rani*, Dr.S Suresh Babu
*T.K.M College of Engineering,Kollam, Kerala, India
H.O.D Dept. of ECE, T.K.M College of Engineering, Kollam, Kerala, India

ABSTRACT

Spread spectrum systems are employed for the secure transmission of digital information which is achieved through spreading the signal in frequency domain. Pseudo-Noise (PN) sequences are conventionally used for this spectrum spreading and de-spreading process. However, the PN sequences are not truly random in nature and follow a deterministic pattern. Though the suitability of random sequences have been tested for the same purpose, feasible implementation of such systems is impossible as de-spreading at the receiver requires knowledge of the exact sequences that have been generated in the transmitter for signal spreading. The Self-Encoded Spread Spectrum (SESS) is a novel spread spectrum communication system developed to enhance the randomness and security of data transmissions through an inventive self-encoding principle. The self-spreading sequence is generated from the information to be transmitted and it eliminates the usage of PN sequences. The registers of SESS system used for generating the self-spreading sequence should be preloaded with a known sequence. As this initial sequence, chaotic sequences are used and its characteristics including correlation properties are evaluated. This paper presents the performance evaluation of SESS with chaotic initial sequence in different channel conditions such as Additive White Gaussian Noise (AWGN) channel and Rayleigh fading channel. Also the effect of jamming in SESS is studied to ensure its applicability as a secure communication system.

Keywords: Self-Encoded Spread Spectrum, PN sequence, spread spectrum, AWGN, Rayleigh, Jamming, Chaotic Sequence**.**

INTRODUCTION

Wireless communication is basically the transmission and reception of signals using electromagnetic waves in open space. The interest in wireless communication has grown dramatically in the past few decades. This growth has been seen in several fields like cellular telephony, personal communication networks, etc. The present scenario is that the data traffic is not only giving tough competition to voice traffic but also exceeding the voice traffic. In addition, wireless local area networks currently supplement or replace wired networks in many homes, businesses, and campuses. Many new applications, including wireless sensor networks, automated highways and factories, smart homes and appliances, and remote telemedicine, are emerging from research ideas to concrete systems. The increasing interest in this area has brought more focus on problems of wireless communication. The major disadvantages of wireless communication systems include the fading of signals due to multipath propagation, destructive interference of multipath components which will lead to very poor signal reception at the receiver and requirement of high SNR to achieve an admissible bit error rate. Capacity limit due to lack of spectrum availability is also an issue.

One possible method of mitigating the aforementioned problems is the use of spread spectrum communications. Two major benefits are its promise of high capacity and its ability to resist multipath interference [16]. In the field of secure wireless communication also spread spectrum technologies are widely used.

Spread Spectrum (SS) is a digital modulation technique in which the bandwidth of information to be transmitted is spread over a relatively wider bandwidth. It gives the transmitted signal a noise-like appearance. This process of spreading the spectrum of information signal to a higher bandwidth is achieved through different methods. One method is to multiply the original signal by a pseudo-noise (PN) code of much wider bandwidth. The PN code used should be independent of the information signal and an exact replica of this code is generated at the receiver for synchronous detection. Communication systems that employ spread spectrum is able to reduce the communicator's detectability and combat the enemy-introduced interference which are respectively referred to as low probability of

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

detection (LPD) and anti-jam (AJ) communication systems. However, spread spectrum systems have been using PN codes or some predetermined codes to achieve spreading from the very beginning. Being periodic and deterministic make such codes vulnerable to interception as it can be duplicated. Also, the pseudo-random code generators at the transmitter and receiver should be synchronized. This led to the development of self-encoded spread spectrum [14]. Spreading code is obtained from the random data source itself which enhances the transmission security. These codes are uncorrelated, arbitrary and varying in time. It makes detection of data by an unauthorized receiver practically impossible. Self-encoded system can provide some advantages over PN coded systems while maintaining a comparable system performance. These include the elimination of PN code generators, inherently asynchronous operation, spectrum smoothness, and code availability [9]. In conventional CDMA communications, the number of available PN codes depends on the code length and puts a limit on the number of subscribers. The constant code length makes it difficult to accommodate transmissions that have variable data rates. In a Self-Encoded Multiple Access (SEMA) system, the signals from simultaneous users are uncorrelated because their data should be random and independent from one another. Thus, unlike the conventional approach, self-encoding does not put a limit on the number of subscribers: the system is strictly interference limited by the multiple access interference from the simultaneous users [13]. Likewise, the problems associated with variable data rates are greatly mitigated because the spreading waveforms from different users are uncorrelated. This paper introduces use of chaotic sequence as the initial sequence of SESS and analyzes its performance in jamming channels. The paper is organized as follows: section two would outline the SESS system and the performance analysis of SESS system in AWGN and Rayleigh fading channels. It also describes the iterative detector that improves the performance of receiver of SESS system. Section three provides analysis on the applicability of chaotic sequence as the initial spreading sequence for SESS. Section four establishes the jamming channel and sets up the worst-case jamming model and examines the effects of jamming inside of AWGN and Rayleigh fading channels for SESS system with chaotic sequence.

SELF-ENCODED SPREAD SPECTRUM

The self-encoded spread spectrum (SESS) was developed and patented by Prof. Dr. Lim Nguyen of University of Nebraska. A model of the system is shown in figure 2.1. The random information bits are used to generate the spreading codes at the transmitter and receiver with the help of delay registers. These registers are constantly updated from an N-tap, serial delay of the data where N is the code length. N chip sequence that has been obtained from the previous N data bits is used to spread the current bit. Application of appropriate data compression methods to remove any redundancy in the data stream maximizes its entropy ensuring the random nature of the digital information source [14]. Hence the binary data symbols can be modeled as independent and identically distributed Bernoulli random variables. Symbol values of +1 and -1 occur equally likely with a probability of ½ [13]. Thus the randomly generated spreading sequence is independent of the current symbol as well as dynamically changing from one symbol to the next. This soothes out the spectrum of the signals and eliminates the presence of spectral lines associated with PN sequences. A chip rate of N/T is achieved using past N transmitted bits stored in the shift registers.

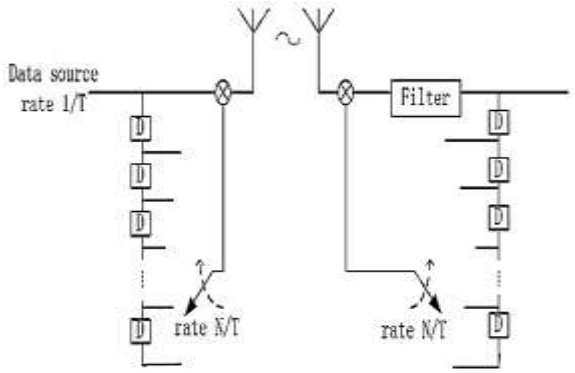


Fig. 2.1: Structure of SESS system

Feedback Detection

At the receiver, the feedback detection involves performing the inverse of self-encoding operation at the transmitter as shown in the figure 1. The recovered data are fed back to the N-tap registers at the receiver to obtain an estimate of the spreading codes required for signal de-spreading. Symbol is detected by means of a correlation detector. Let sp(0) be the spreading code at the transmitter and dsp(0) be the de-spreading code at the receiver during the 0^{th} bit interval. Then sp(0) and dsp(0) can be represented using previous N information bits b and N previously detected bits d respectively as:

$$sp(0) = [b(-1), b(-2), \bullet\bullet\bullet, b(-N)] \quad (2.1)$$

$$dsp(0) = [d(-1), d(-2), \bullet\bullet\bullet, d(-N)] \quad (2.2)$$

Considering a binary communication, $b(i) \in \{1, -1\}$ and $d(i) \in \{1, -1\}$. Let $b(-m)$ be the m^{th} previous transmitted bit, $d(-m)$be the m^{th} previously detected

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

bit. The spread spectrum sequence ss(0) from spread spectrum modulation of the current bit b(0) during the 0^{th} bit time is

$$ss(0) = b(0) \bullet [b(-1), b(-2), \bullet\bullet\bullet, b(-N)] \quad (2.3)$$

At the start of the transmission, the contents of the delay registers in the transmitter and receiver should be identical to establish synchronization. Thus it becomes impossible to recover the data by an unintended receiver without the knowledge of initial data in the registers and the tap register structure of the intended receiver. Thus enhanced transmission security can be achieved with this LPD communication system.

Iterative Detection

Iterative detection is a soft decision decoding technique which can be iterated several times to improve the bit error rate performance of a coding scheme.

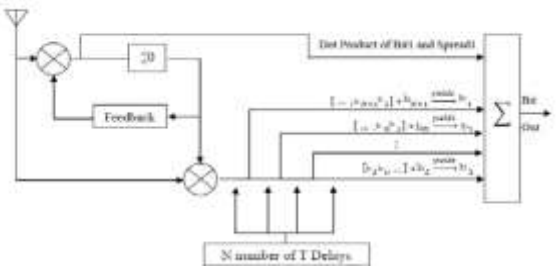


Fig. 2.2: Iterative detection

This detection method makes use of the property of SESS system that the current bit detected depends on previous N bits and is also used in the estimation of future N bits.

The iterative decoder has a complexity linear to that of the spreading code [5]. The design used requires storage of the N+1 received data bits. The definition of a SESS systems states that the spreading codes are generated from the information being transmitted. The transmitted SESS signals can be represented as

$$ss_1 = b_0b_1, \quad b_{-1}b_1, \quad \ldots\ b_{-N+1}b_1$$
$$ss_2 = b_1b_2, \quad b_0b_2, \quad \ldots\ b_{-N+2}b_2$$
$$ss_3 = b_2b_3, \quad b_1b_3, \quad \ldots\ b_{-N+3}b_3$$
$$ss_N = b_{N-1}b_N, b_{N-2}b_N, \quad \ldots\ b_0b_N$$
$$ss_{N+1} = b_Nb_{N+1}, b_{N-1}b_{N+1}, \quad \ldots b_1b_{N+1} \quad (2.4)$$

where b_i is the data bit. Since the current bit is spread by N previous bits, current bit bi is spread by N previous symbols $b_{i-1}\ldots b_{i-N}$ at a rate N/T. The current detecting bit d_1 is not only modulated by the previous N information bits, which are stored in the delay shift register $b_{-N+1}\ldots b$, but it also appears in N future transmitted signals $ss_2,\ldots,ss_{N+1}$: there is one chip in each N future transmitted signal, that contains the information about d_1. Thus the information contained in those N future bits about d_1, can be used to make the final decision on estimated b_1 at the receiver if there be excessive channel noise or jamming on b_1 that would normally cause an error. For soft decision decoding of bits, by considering the future transmitted signals together with previous detected bits, iterative detector is expected to demonstrate an improvement in performance over feedback detector as the feedback detector estimates the current bits by correlating with only N previous detected bits. Here only single iteration is considered for simplifying the implementation.

SESS Model

A simple model of SESS is modelled assuming that the system is initially in synchronization. The system is simulated in MATLAB tool. Here the result shown is for a data of length 100 bits and each of these 100 bits of data was spread using self-encoded spread sequence at a rate of 100 chips per bit. The information bits were recovered without any error ensuring the proper working of spreading and de-spreading of data by modelled SESS under zero noise conditions.

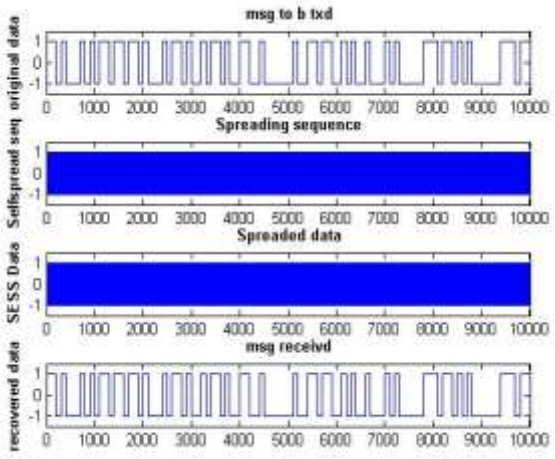


Fig 2.3: Self-encoded spread spectrum model

SESS Performance Analysis

AWGN is a channel model in which signal degradation is contributed by a linear addition of wideband or white noise and a Gaussian distribution of amplitude. It does not consider fading, frequency selectivity, interference, dispersion etc. To obtain the probability of bit error, P_e of the SESS system for an AWGN channel, it is assumed that synchronization between the transmitter and the receiver has been achieved. At the receiver, all detected bits including incorrect ones are inserted into the shift registers for generating decoding sequence and these incorrect bits

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

affect the decoding process until it is shifted out of the delay registers N bits later. Depending on the chip length, signal attenuation varies. Thus when the value of N is large, the erroneous bit would remain in the register for longer period, but attenuation caused by it would be smaller. Inversely, for a small N value a chip error would rotate out of the register quickly, but attenuation caused would be larger. Let the number of chip errors be m. The de-spreaded signal strength attenuation given m chip errors in the shift registers of receiver is:

$$A|m = 20\log(1 - (2m/N))\text{dB} \quad (2.5)$$

Then the conditional probability of error can be expressed as

$$P_e = Q\left((1-(2m/N))\sqrt{\frac{2Eb}{N0}}\right) \quad (2.6)$$

where Q(.) is the Q-function and E_b/N_o, is the energy per bit to noise ratio. Even under high SNR, signal may become irrecoverable in the presence of gross errors due to signal fading or bursty channel conditions as this could lead to excessive self-interference. This instability issue of self-coding designs can be kept under control if suitable synchronization measures are employed**.**

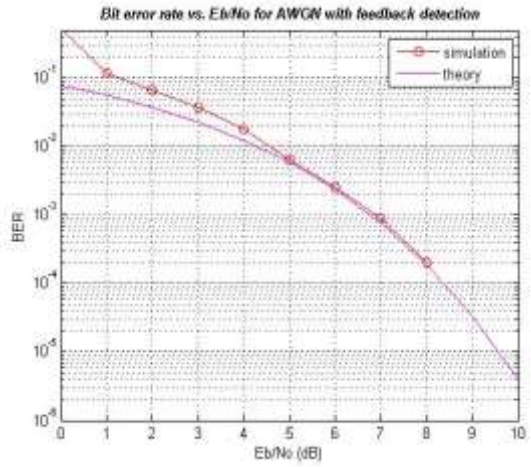


Fig.2.4: Performance of SESS system in AWGN channel with feedback detection

The SESS performance is impacted at low signal to noise ratios by error propagation. From the BER plot, a performance degradation is observed in comparison with BPSK at low SNR (<4dB). It is mainly due to the self-interference issue at low SNR. The value of N is also a factor that causes more degradation at lower SNR. The BER plot for different values of N shows that when N is large, SESS system converges quickly to BPSK in an AWGN channel. The effect of self-interference is reduced with increase in spread sequence length N. It is also observable that for N>64, this issue is eliminated. However, for lower N values, the BER stays closer to 0.5. Figure 2.6 shows that with iterative detection, a performance improvement of 3dB is obtained for a BER of 10^{-4}.

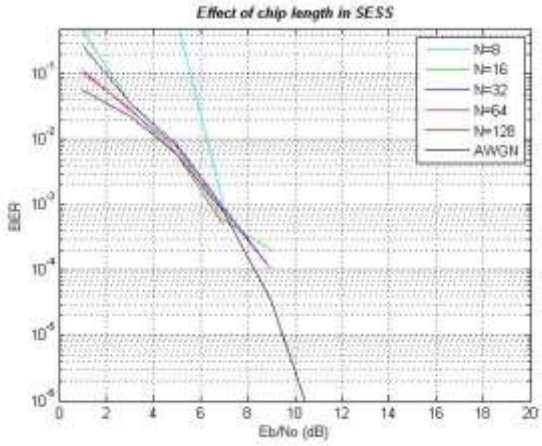


Fig.2.5: Performance of SESS system for different values of N

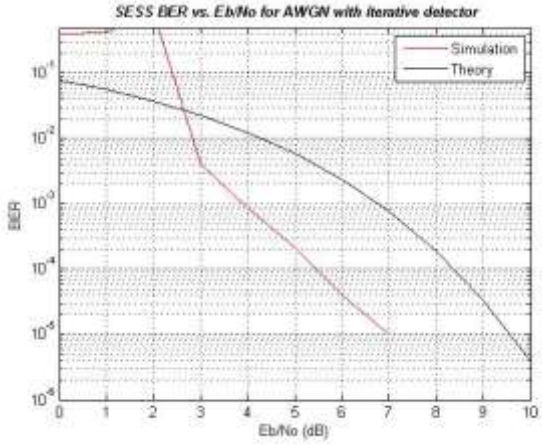


Fig2.6: Performance of SESS system in AWGN channel with iterative detection

Rayleigh fading model is most applicable in the absence of line of sight between the transmitter and receiver[12]. Slow fading will occur if the delay constraint of the channel is small relative to the coherence time of the channel. Flat fading occurs when the bandwidth of the wireless channel is greater than the bandwidth of the transmitted channel. For the slow, flat fading condition, it was assumed that the fading over each symbol period is independent of the other [14]. As the self-spreading sequence is generated from previously detected bits, the sequence is independent of the current symbol. Thus the chip errors in the receiver's delay registers are also independent of the fading over the current symbol period. Thus a lower bound on P is obtained as, the conditional error probability:

$$P_e \geq 0.5\left[1 - \sqrt{\frac{(1-2P_e)^2.SNR}{1+(1-2P_e)^2.SNR}}\right] \quad (2.7)$$

Here SNR is the fading symbol signal-to-noise ratio.

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

Since $P_e \leq 0.5$, this can be simplified as:

$$P_e \geq 0.5\left[1-\sqrt{1-(SNR)^{-1}}\right], SNR > 1 \quad (2.8)$$

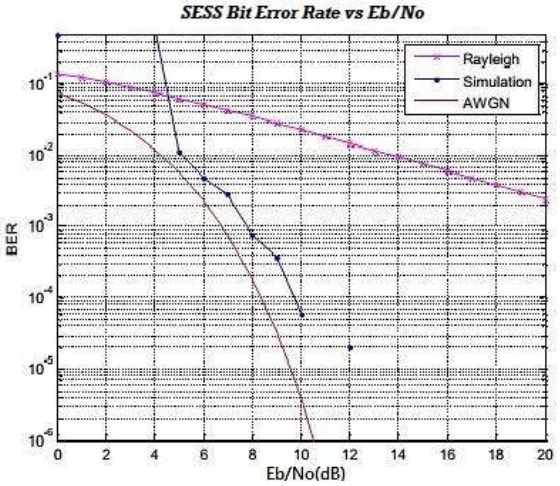


Fig.2.7: Performance of SESS system in Rayleigh channel with iterative detection

Due to fading in channel, more SNR is required to achieve lesser BER. With iterative detector, a BER of 10^{-3} is achieved at an SNR as low as 8dB whereas, theoretically with feedback detection, it required more than 20 dB SNR.

CHAOTIC SEQUENCES IN SESS

In order to limit the maximum SNR degradation in the SESS system, known and fixed code elements should be preloaded in the N-tap delay registers. This calls for a design trade-off in the system performance by using a combination of PN codes and self-encoding techniques [8]. The analytical result illustrates the importance for the receiver to have an accurate estimate of the transmitter's delay registers. Also we know that even under high SNR, the transmitted data may become irretrievable in the presence of gross errors due to excessive self-interference caused by signal fading or bursty channel conditions. Moreover, in a DSSS system, a large number of codes are needed often. But the number of PN sequences available for SS from m-sequence generators is very much limited. As an example, for a sequence length of $n=2^m-1$, where m is the number of flip flops in m-sequence generator, let m=5, then n=31, there are only 6 sequences and for m=7, $n=(2^7-1)=127$, there are only eighteen different sequences available. Hence the number of sequences available from an m-sequence generator is much restricted. When the number of sequences available becomes limited, the number of multiple access users also gets limited.

The major advantage of SESS system is the elimination of PN code generators at the transmitter and receiver. Instead of going for a design trade-off by incorporating pseudo-random sequences, a chaotic sequence generator is proposed. Chaotic signals possess many properties that make them fit for SS communications. They are noise-like, yet reproducible. Two nearby trajectories of chaotic signals diverge quickly. In recent years, the sequences derived from chaotic phenomena are being considered for use in secure communication and for spread spectrum systems. Chaotic sequences are generated from nonlinear dynamic systems. Their essential feature is that they exhibit noisy-like behavior because of its strong sensitivity to initial conditions. Chaotic signals are wideband, yet, they can be generated by using a simple deterministic system. It therefore provides a simple means of generating a large number of uncorrelated sequences for spread spectrum communications. For generating chaotic binary sequences, correlation criteria is used to select the qualified sequences. The number of obtained sequences can be much greater than that of m-sequences of the same length. In addition, unlike conventional sequences, chaotic spreading codes can be generated for arbitrary length and for any number of sequences. Also, a simple method to obtain chaotic sequences is to use mapping functions.

A chaotic map is a mathematical transformation technique used to illustrate the phenomenon of chaotic motion. The map is described by mathematical equations. These equations can be used recursively on the same point so that the point gets mapped to new locations. Each execution of this equation is called an iteration of the map. The maps can be 1D, 2D etc in which 1D requires one initial condition, 2D requires two initial conditions etc. Here the mappings considered are logistic mapping and Bernoulli mapping.

Logistic Map

Logistic map is a polynomial mapping of degree 2, showing a chaotic behavior that can arise from very simple non-linear dynamical equations. A model derived from mayflies, a species of insects. Mathematically, the logistic map is written as

$$x(n+1) = r * x(n) * \left(1-x(n)\right) \quad (3.1)$$

There are two important parameters for the logistic mapping, the bifurcation parameter r and the initial value x_0. The parameter r must be selected so that the trajectories of nearly equal initial values will diverge quickly.

With fixed parameter r, each different initial value x_0 can then be used to generate a sequence of any length as a signature sequence for SESS system [17].

Depending on the value of r, the dynamics of this system can change dramatically, exhibiting chaos.

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

For 0 <r < rc = 3.57, the sequence (x) is periodic with period 2m, for some m, while, for rc < r<4, the sequence is, for all practical purposes, non-periodic and non- converging [20].

In fact, it is mathematically proven that, except for negligibly short intervals where the sequence has odd periodicities, this particular range of values of r causes the logistic map to be chaotic [11].

The sensitivity of the chaotic maps on their initial condition is usually measured by means of the lyapunov exponent, $\lambda(x)$. The Lyapunov exponent of a one-dimensional map is the average exponential rate of divergence of infinitesimally nearby initial conditions. Thus, for positive values of $\lambda(x)$ chaos occurs, while for negative values periodic solutions of the iterative map appear.

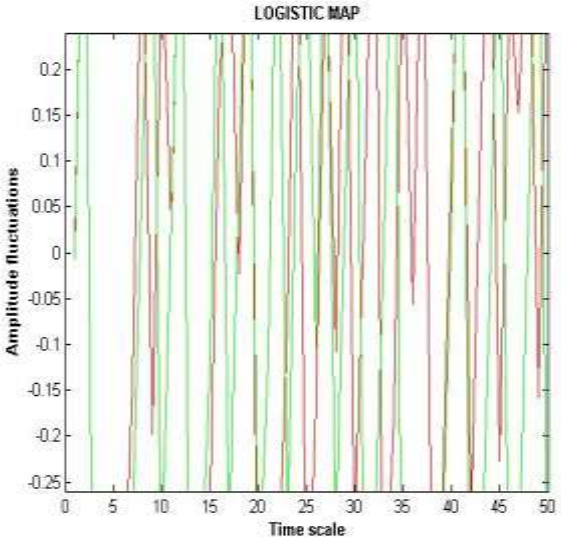


Fig.3.1: Sensitivity to initial condition for logistic map

This logistic map has a very sensitive dependence upon its initial value, x_o, for those values of r. This sensitive dependence can be illustrated by giving two very close initial points to the iterative map. After a few iterations, the two resulting sequences will look completely uncorrelated. Figure 3.1 is the illustration of the amplitude fluctuations generated by using two very closely spaced initial points, 0.1 (red) and 0.10001 (green) in the chaotic logistic map with r = 4.

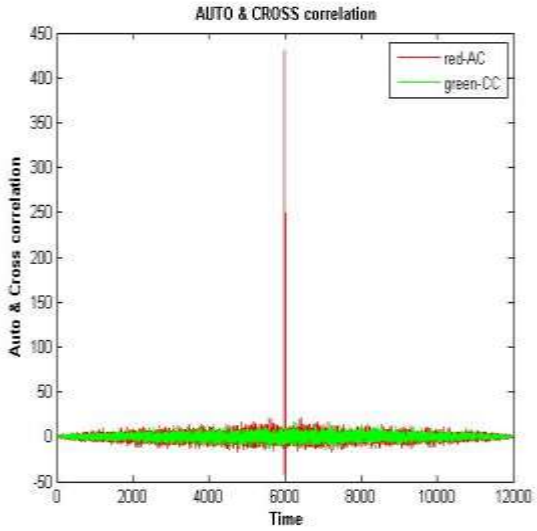


Fig.3.2: Autocorrelation and cross correlation of logistic map sequence

Figure 3.2 illustrate typical samples of correlation functions for the chaotic logistic map. The correlation properties of the chaotic sequences look very much like random noise. Their correlation functions are very similar except for the peak at zero lag in the auto- correlation function.

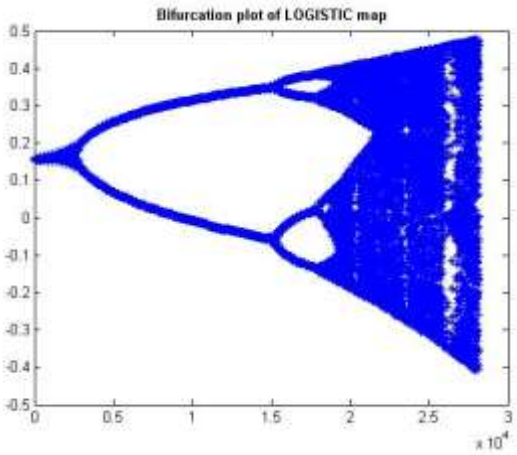


Fig 3.3: Bifurcation plot of logistic map

A bifurcation diagram demonstrates the possible long-term values (fixed points or periodic orbits) of a system as a function of a bifurcation parameter in the dynamical system [17]. The transition from one regime to another is called a bifurcation. The bifurcation diagram illustrates the splitting of the possible periods of stable orbits from 1 to 2 to 4 to 8 etc. Each of these bifurcation points is a period-doubling bifurcation as shown in figure 3.3.

Depending on initial condition x_0, given mapping functions can generate different real valued arrays on the interval (0, 1). For generating non-repetitive binary sequences, a transformation θ_t can be used, which is defined as

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

$$\theta_t = \begin{cases} 0, & x < t, \\ 1, & x \geq t \end{cases} \quad (3.2)$$

where t is a threshold value. Using this threshold function, chaotic binary sequence is obtained. These sequences are non-periodic, deterministically generated and sensitive to initial condition [4].

The chaotic binary sequences c_k used here are generated by mapping the real values obtained from logistic mapping to a binary sequence using the following transformation [11]

$$c_k = g(x_n - E(x_n)) \quad (3.3)$$

where g(x)=1 for $x \geq 0$ and g(x)=-1 for $x < 0$. Here g(x) is called as the threshold function which determines the threshold for mapping to 1 and -1. E(.) denotes the mathematical expectation operator and $E(x_n)=0.5$ for the logistic map when r=4.

However, a major disadvantage of logistic mapping is that for r = 4, logistic mapping becomes self-mapping. It maps real numbers, x[n], defined on interval (0, 1) to itself. Hence another mapping called the Bernoulli map can be considered to generate chaotic binary sequence.

Bernoulli Mapping

The Bernoulli map can be defined as follows:

$$x_{n+1} = f(x) = \begin{cases} Bx + 0.5, & x < 0 \\ Bx - 0.5, & x \geq 0 \end{cases}$$

$$0.5 \leq x_n \leq 0.5 \quad (3.4)$$

To guarantee the chaotic property of Bernoulli map, value of B should be chosen between 1.4 and 2. The figure 3.4 shows the sensitivity of the map to closely spaced initial points at initial conditions 0.25(red) and 0.25005(blue). Bernoulli map is also having better autocorrelation and cross-correlation properties than the logistic map as observable in the figure 3.5. The Bernoulli map is having more positive lyapunov exponents in the range in which it becomes chaotic[2]. Figure 3.7 proves the superiority of Bernoulli map sequences over both logistic map sequences and m-sequences in terms of correlation. The chaotic attractor is also larger than the one for logistic map and is reached faster than logistic map as shown in bifurcation diagram of Bernoulli map in figure 3.6. Hence Bernoulli mapping is also a suitable map for generating chaotic binary pseudorandom sequence. Here the threshold function is given by

Chaotic sequence

$$c_k = \begin{cases} -1, & x_n < 0 \\ 1, & x_n \geq 0 \end{cases}$$

(12)

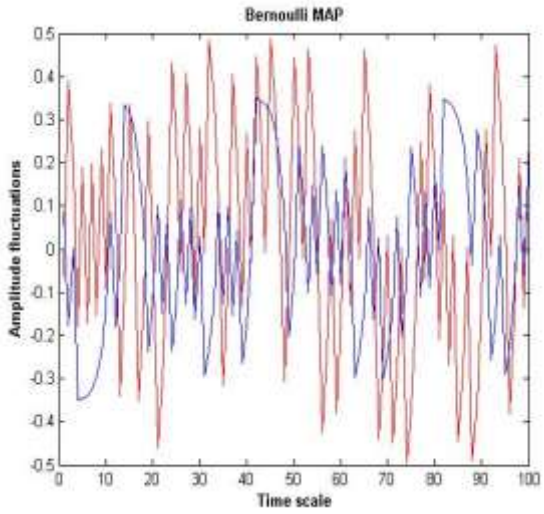


Fig 3.4: Sensitivity to initial condition for Bernoulli map

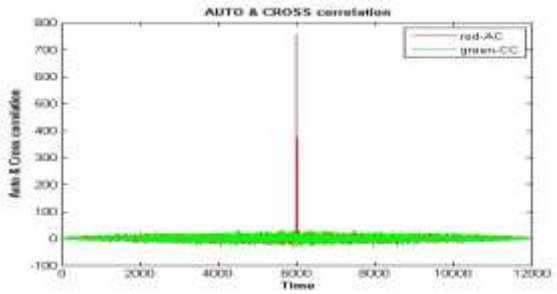


Fig 3.5: Autocorrelation and cross correlation of Bernoulli map sequence

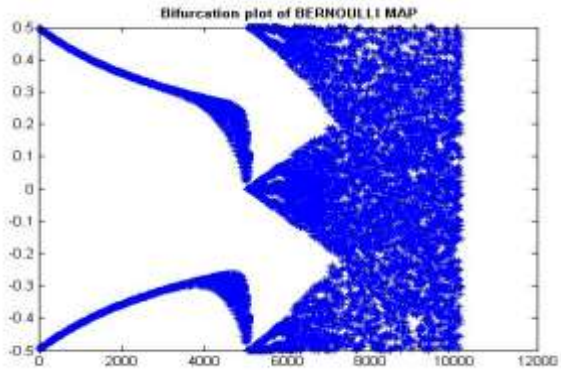


Fig 3.6: Bifurcation diagram of Bernoulli map

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

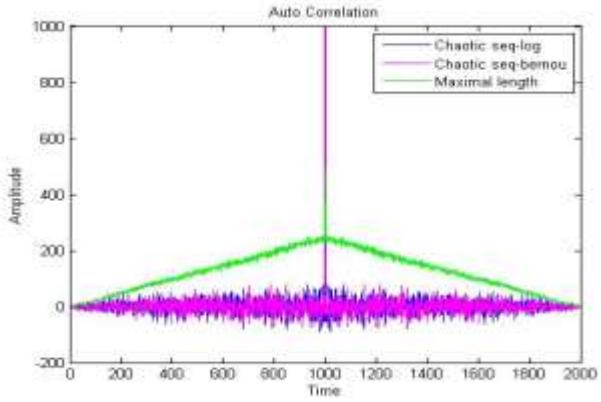
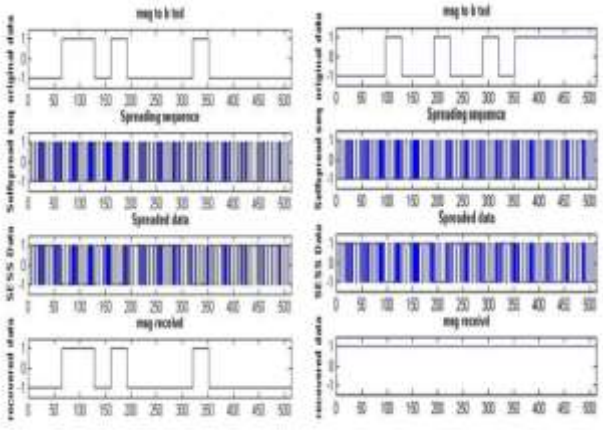


Fig 3.7: Autocorrelation comparison

SESS with Chaotic Initial Sequence

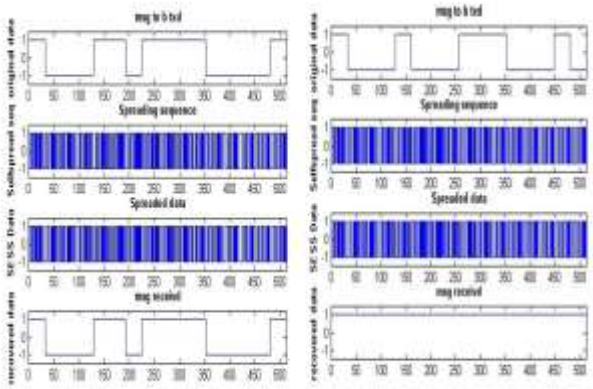
Figure 3.8 is the SESS model using logistic map sequence. Here the control parameter r=4 at both transmitter and receiver. The initial condition is x_0=0.1 at the transmitter and receiver in figure 3.8.a and the output is recoverable. In the figure 3.8.b, the value of initial condition, x_0 is 0.1 at the transmitter and 0.10001 at the receiver. As observable, when the input initial condition at the receiver is varied by 10^{-4}, the result is totally undesirable. This shows that the system has very low probability of detection by unintended receivers.



(a) *(b)*

Fig 3.8: SESS model with Logistic map sequence

Similar is the case with SESS system using Bernoulli map sequence as shown in figure 3.9 with B=2. Initial condition is x_0=0.25 at transmitter and receiver in figure 3.9.a and x_0 is 0.250001 at receiver in figure 3.9.b. Hence the LPD property is enhanced.



(a) *(b)*

Fig 3.9: SESS model with Bernoulli map sequence

The major advantage of using a chaotic initial sequence generator is that from the mapping, it is possible to obtain random sequence of any length. There is no limitation in number of sequences that can be obtained from a chaotic mapping and hence preferable for multiple access systems. Moreover, if there is a need to change the processing gain of SESS by changing the chips per bit, if PN sequence generators are used, the feedback connections should also be varied along with the number of registers and there are only limited periodic sequences available from it. But in the case of chaotic sequence, there is only a need of allocating more registers as the delay registers of SESS and vary the initial condition for chaotic sequence generation by a value as small as 10^{-4}.

PERFORMANCE ANALYSIS OF SESS IN JAMMING CHANNELS

Jamming in a communication channel is the process of disrupting communication between intended transmitters and receivers using undesirable signals which worsens the probability of error. Thus the proper reception of signals at the intended receiver would get jammed. Hence in the presence of jamming, BER will be greater than that of fading channels or standard noise so that the latter can be neglected. For any time varying spread spectrum techniques like DSSS and SESS, the most potent jamming method is the pulsed noise jamming. Rather than just continuously jamming a communication channel, a pulsed noise jammer (PNJ)/ partial time jamming can block the channel at chosen times with a greater power [12]. This type of effective jamming is often used in electronic countermeasure operations. PNJ is a jammer that turns on with just adequate power to degrade spread spectrum system performance significantly, but does not totally annihilate system performance when it is turned off.

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

Thus the jammer selects the duty cycle that maximizes the error probability. Hence the worst case pulse jamming in DSSS [12] has an error probability given by

$$(Pe)max \approx \frac{0.083}{(\frac{Pav}{Jav})(\frac{W}{R})} \quad (4.1)$$

when E_b/J_o, the energy per bit to jamming power spectral density is at least 0.709 where $J_o = Jav/\rho W$, where Jav is the jammer power, ρ is jammer duty cycle, W is the bandwidth occupied by the spread spectrum signal, P_{av} is the average signal power and R the information rate of data to be transmitted. Thus an upper bound on the BER of worst case jamming effect in DSSS system is obtained. Hence for different jamming duty cycles, the BER would remain in close proximity to or less than the probability of error due to worst case jamming.

In the case of SESS with chaotic initial sequence assuming perfect synchronization, the probability of error can be expressed as:

$$Pe|m = Q(\left(1 - \frac{2m}{N}\right)\sqrt{\frac{2Eb}{No}}) \quad (4.2)$$

where m refers to the number of incorrectly detected bits in the receiver delay registers, and N is the chip length. The probability of error when jamming is added to the system is

$$Pe|lEb = (1-\rho)Q\left(\left(1 - \frac{2m}{N}\right)\sqrt{\frac{2Eb}{N_o}}\right) + \rho Q((1\frac{2m}{N})\sqrt{\frac{2Eb}{N_o + \frac{Jo}{\rho}}}) \quad (4.3)$$

If it is assumed that jamming dominates than additive noise in the channel, then the probability becomes

$$Pe = \rho Q((1-2Pe)\sqrt{\frac{2Eb}{Jo}/\rho} \quad (4.4)$$

By applying the upper bound of Q function,

$$Pe \leq \frac{\rho}{(1-2Pe)} e^{-\rho(\frac{Eb}{Jo})(1-2Pe)^2} \quad (4.5)$$

By taking the first derivative of equation (4.5) with respect to ρ , equating it to zero, solving for ρ, and substituting for ρ in Pe, the worst-case jamming [7] can be found as,

$$Pe(1-2Pe)^2 = \frac{Q(1)}{2Eb/Jo} \cong \frac{0.083}{(\frac{Pav}{Jo})(\frac{W}{R})} \quad (4.6)$$

Thus by comparing (4.1) and (4.6) the SESS also performs compatibly in comparison with the DSSS system.

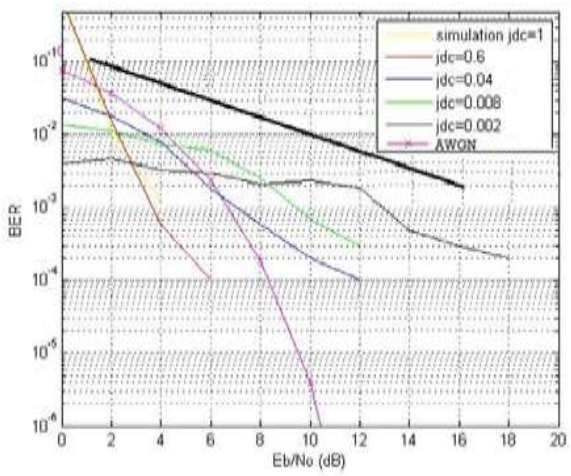


Fig 4.1: Performance of SESS with chaotic initial sequence in jamming channels with iterative detection

In the simulation result, the black line depicts the worst case error probability of SESS and the thin lines show the BER plots of SESS for different jamming duty cycles. The length of sequence N used is 64 and initial sequence generated using Bernoulli mapping. The assumption made is that the initial spreading sequences are synchronized and the channel noise is neglegible.

The deviation from the worst case jamming line is observed when the SNR values are below 2 dB. It is due to the error propagation in the SESS system. The SESS with the iterative detector improves the worst-case jamming by 6 db at a BER of 10^{-3} due to soft decision decoding as seen in figure 4.1.

In the previous simulation, the assumption was that the noise level in channel is negligibly lower than the jammer power and hence it was ignored. The soft decision made by the iterative detector on data bits under jamming scenario were found to perform better than the worst case scenario. At the low values of ρ, the majority of the data being sent is not jammed and was sent through a noiseless channel. The noiseless channel makes it easy for the soft decision detector to recover from errors at lower ρ. Thus the jamming over the channel no longer dominates the noise of the channel. This reveals the need to add noise or fading back to the channel during the jamming simulations. Taking into account the noise and fading in jamming channels, the simulation was carried out.

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

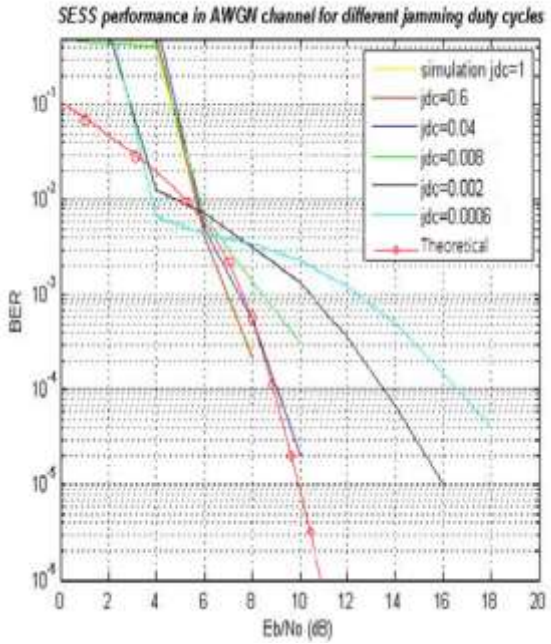


Fig 4.2: Performance of SESS with chaotic sequence in jamming channels with AWGN

The channel noise was ignored in previous simulations because the jamming was assumed to dominate the noise. The result appears to remain the same for higher SNR range as the values for the worst-case jamming remain close to the same. The only part of the graphs where the channel noise or fading had any effect was the SNR values from zero to ten where BER has increased for corresponding SNR due to channel noise compared to the results without noise in jamming channels. An additional 4dB was required to achieve the same BER in noisy AWGN jamming channel and an additional 10 dB was required in Rayleigh fading channel with jamming compared to SNR values before 10dB.

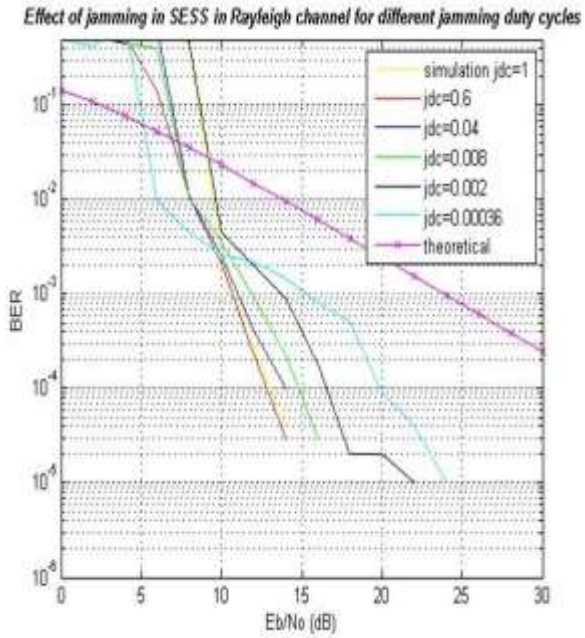


Fig 4.3: Performance of SESS with chaotic sequence in jamming channels with Rayleigh fading

RESULTS AND DISCUSSIONS

The SESS model is first developed in MATLAB. Under zero noise conditions, the model demonstrated the spreading and de-spreading of data using the random information sequence itself without any chances of error with feedback detector. Then the iterative detector is implemented and the performance of SESS in AWGN and Rayleigh channels are analyzed. The feedback detector showed that the results are in agreement with the theoretical results where as the iterative detector provided better results. For both the detection schemes, high BER ($>10^{-2}$) is observed at low SNR(<4dB) due to error propagation. Then the study is carried out with varying chip length N. For small values of N, the errors caused greater degradation of received signals and larger the values of N, the quicker the results converged to theoretical results.

Two chaotic sequence generators are used to generate the initial spreading sequence of SESS. The logistic map sequence and the Bernoulli map sequence exhibited better correlation properties than the m-sequences. Moreover, when there is a slight variation in initial condition of chaotic sequence generator by a value as small as 10^{-4}, the bits are found to be detected incorrectly which demonstrate the low probability of detection by unintended receivers.

Further, a study on the effect of jamming in SESS with chaotic initial sequence was carried out. Mathematically SESS is found to perform

comparable to that of DSSS. With iterative detector, the SESS system performed better by 6 dB at a BER of 10^{-3} in jamming channel. With both jamming and noise, attenuation due to noise was predominant at low values of SNR (<10dB) and at higher values, the BER remained close to the worst case jamming error probability.

CONCLUSIONS

The conventional spread spectrum modulation techniques are known to provide security to information transmitted over communication channels by giving the data a noise-like appearance in the channel. The use of PN generators at the transmitter and receiver pose several drawbacks including the periodic and deterministic nature of PN sequences, vulnerability to unintended detection, limited code availability for a given length of sequence and difficulty in synchronizing the PN generators at the transmitter and receiver. The self-encoded spread spectrum is a novel approach which exhibit improved transmission security than PN approach. Since the information to be transmitted is used to generate the spreading sequence, ensuring randomness of transmitted data creates dynamically varying waveforms. This makes undesirable detections to be practically impossible. Here the ease in generation and regeneration of spreading and de-spreading sequence at the transmitter and receiver respectively arise as a result of self-encoding. The omission of PN sequence generators at the transmitter and the receiver, absence of spectral lines and availability of random codes are the major features which makes SESS a better choice. Instead of making a design trade-off by using PN sequence as the initial spreading sequence, chaotic sequences are used which possess better autocorrelation than m-sequences. It also improves the low probability of detection as such systems are heavily sensitive to its initial conditions at the transmitter and receiver. Self-encoded system possesses these merits over PN-coded systems though it exhibits a comparable system performance.

It is apparent from the simulation that the numerical results of performance evaluation of SESS in AWGN and Rayleigh fading channels are tactically in concurrence with the theoretical results when feedback detector was used. The simulation results established that the iterative detector outperforms feedback detector.

The effect of jamming in SESS with chaotic sequence is analyzed and is found to be comparable with DSSS theoretically. With an iterative detector, SESS using chaotic sequence as the initial spreading sequence showed an improvement of 6dB at a BER of 10^{-3}. Under jamming and noisy channel conditions range of SNR (<10dB). An additional 4dB was required to achieve the same BER in noisy AWGN jamming channel and an additional 10 dB was required in Rayleigh fading channel with jamming for SNR values less than 10 dB. At higher values of SNR, the BER was found to remain close to that of BER due to worst case jamming. Thus it is evident that degradation caused by channel noise is predominant for low SNR values, and jamming is predominant for high SNR values.

In future, as the extension of this work, the synchronization of transmitter and receiver of SESS systems with chaotic sequence generators can be experimented by using synchronization techniques for chaotic systems. Some major synchronization techniques for chaotic systems are already developed [15]. Thus by using the chaotic sequence generators, initial spreading sequence generation as well as synchronization can be achieved for SESS systems and then it can be extended to multiple access systems.

together, the noise had effect on BER at lower

REFERENCES

[1] W. M. Jang and L. Chi, “Self-Encoded Multi-Carrier Spread Spectrum with Iterative Despreading for Random Residual Frequency Offset,” Journal Of Communications and Networks, Vol. 15, No. 3, pp. 258–265, June 2013.

[2] Qilun Yang, Yunhua Zhang, and Xiang Gu, “A Signal Model based on Combination Chaotic Map for Noise Radar,” Progress In Electromagnetics Research, Vol. 28, pp.57-71, 2013.

[3] R. Nawkhare and A. Tripathi, “DS-SS Communication System using Pseudo Chaotic Sequences Generator,” International Conference on Communication Systems and Network Technologies, pp. 78–82, 2013.

[4] S.Sajic, N.Maletic, B.M.Todorovic and M.Sunjevaric, “Random Binary Sequences in

ISSN: 2277-5528
Impact Factor: 2.745 (SIJF)

Telecommunications," Journal of Electrical Engineering, Vol. 64, No. 4, pp. 230–237, Jan. 2013.

[5] L. Chi, W. M. Jang, and L. Nguyen, "Distributed and Centralized Iterative Detection of Self Encoded Spread Spectrum in Multi-Channel Communication," Journal of Communications and Networks, Vol. 14, No. 3, pp. 280–285, June 2012.

[6] R. Kumar and P. Kumar, "Performance Evaluation of Various Modulation and Coding Techniques on Self-Encoded Spread Spectrum," Proc. of the International Conference on Advanced Computing and Communication Technologies, pp. 978–981, 2011.

[7] C. L. Deyle, "Performance Of Self-Encoded Spread Spectrum Under Worst-Case Jamming," Dissertations & Student Research in Computer Electronics & Engineering. Paper 3, DigitalCommons, University of Nebraska - Lincoln 2010.

[8] P. Duraisamy, and L. Nguyen, "Coded-Sequence Self-Encoded Spread Spectrum Communications," Proc. IEEE GLOBECOM'09, Honolulu, Hawaii, pp. 1–5, 2009

[9] K. Hua, L. Nguyen, and W. M. Jang, "Synchronization of Self-Encoded Spread Spectrum System," Electronics Letters, Institution of Engineering and Technology (IET), Vol. 44, No. 12, pp. 749-751, June 2008.

[10] W. Kinsner and S. Member, "Characterizing Chaos Through Lyapunov Metrics," IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications and Reviews, Vol. 36, No. 2, pp. 141–151, 2006.

[11] Y. Fu and H. Leung, "Narrow-Band Interference Cancellation in Spread Spectrum Communication Systems Using Chaos," IEEE Transactions on Circuits and Systems—I: Fundamental Theory And Applications, vol. 48, no. 07, pp. 847–858, July 2001.

[12] John Proakis, Digital Communications, 4th Edition, Mc Graw Hill, 2001.

[13] L.Nguyen, "Self-Encoded Spread Spectrum and Multiple Access Communication," IEEE 6th International Symposium on Spread Spectrum Techniques & Applications, Vol. 00, pp. 394–398, Sept. 2000.

[14] L.Nguyen, "Self-encoded spread spectrum Communications," Proceedings of the IEEE Military Communications Conference (MILCOM '99), Vol. 1, pp. 182–186, Oct. 1999.

[15] M. P. Kennedy and L. O. Chua, "The Role of Synchronization in Digital Communications Using Chaos — Part II : Chaotic Modulation and Chaotic Synchronization," IEEE Transactions on Circuits and System I: Fundamental Theory and Applications, Vol. 45, No. 11, pp. 1129–1140, Nov. 1998.

[16] R.M.Beuhrer, "Spread Spectrum for Wireless Communication," Wireless Personal Communications, The Springer International Series in Engineering and Computer Science, Chapter3, pp. 55-74, 1995.

[17] G. Heidari-bateni, C. D. Mcgillem, and L. Fellow, "A Chaotic Direct-Sequence Spread-Spectrum Communication System," IEEE Transactions on Communications, Vol. 42, No. 21314, pp. 1524–1527, April 1994.

[18] Scholtz, Robert A, "The Evolution of Spread-Spectrum Multiple-Access Communication," Spread Spectrum Techniques and Applications, IEEE ISSSTA, pp. 4–13, 1994.

[19] Simon, Marvin K. and Omura, Spread Spectrum Communications Handbook, McGraw-Hill, Inc., 1994.

[20] G. Heidari and C.D. McGillem, "Chaotic Sequences for Spread Spectrum: An Alternative to PN-sequences," Proc. IEEE International Conference on Selected Topics in Wireless Communications, pp. 437-440, 1992.

Scholtz, Robert A, "The Origins of Spread-Spectrum Communications," IEEE Transactions on Communications, No.5, Vol.C, pp. 822-854, May 1982.