2010

Frequency Domain Processing Based Chaos Communication for Cognitive Radio

Daniel Y. Sundersingh
Wright State University

Repository Citation

Sundersingh, Daniel Y., "Frequency Domain Processing Based Chaos Communication for Cognitive Radio" (2010). *Browse all Theses and Dissertations*. 355.
https://corescholar.libraries.wright.edu/etd_all/355

Frequency Domain Processing Based Chaos Communication for Cognitive Radio

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Engineering

by

Daniel Y. Sundersingh
B.S.E.E., Wright State University, 2008

2010
Wright State University

Wright State University
SCHOOL OF GRADUATE STUDIES

June 23, 2010

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY Daniel Y. Sundersingh ENTITLED Frequency Domain Processing Based Chaos Communication for Cognitive Radio BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF Master of Science in Engineering.

Zhiqiang Wu
Thesis Director

Kefu Xue
Department Chair

Committee on
Final Examination

Dr. Zhiqiang Wu

Dr. Vasu Chakravarthy

Dr. Yao Ma

John A. Bantle, Ph.D.
Vice President for Research and Graduate Studies and Interim Dean of Graduate Studies

ABSTRACT

Sundersingh, Daniel. M.S.Egr., Department of Electrical Engineering, Wright State University, 2010. *Frequency Domain Processing Based Chaos Communication for Cognitive Radio.*

Chaotic systems are deterministic non-linear dynamical systems which have intrinsic properties such as: irregularity, aperiodicity, and are impossible to predict over long periods of time. Cognitive radio on the other hand, has emerged recently as a powerful means to tackle the spectrum congestion problem. The goal of this thesis is to combine the benefits of the chaos communication system with the cognitive radio to create a robust, highly secure, flexible chaotic cognitive radio system. We first begin with a short survey of chaotic communication and cognitive radio technology. Then we compare chaotic waveforms to other conventional PN sequences and show its superiority in security and multiuser capabilities. We then propose a novel frequency domain based chaos communication system that is capable of operating over multiple non-contiguous frequency bands. Furthermore, we analyze the performance of this system in different channel models and in multiuser scenarios. Finally, we implement carrier-interferometry sequences along with the chaos sequence to increase the security and performance of the system.

Contents

List of Figures

Acknowledgement

I an so grateful to my supervisor Dr. Zhiqiang Wu, who was an excellent supervisor and helped me immensely during the course of my Masters study. I would also like to thank him for giving me the opportunity to work on this interesting topic. Also, I would like to thank Dr. Yao Ma and Dr. Vasu Chakravarthy for their excellent comments which have substantially improved my thesis work. Thanks also to the other graduate students Xue Li and Roulin Zhou for their assistance and help in my research. Finally, a special thanks to my parents who have consistently supported me with their prayers throughout my studies. This work was supported by Dayton Area Graduate Studies Institute Faculty/Student Research Grant. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agency.

Introduction

1.1 Chaos Communication

Chaos communication has been studied over the last two decades as a system that can improve the security of the transmitted signal. Chaos can be defined as an aperiodic long-term behavior in a deterministic system that exhibits sensitive dependence on initial conditions [1] . Chaotic systems are derived from non-linear dynamical systems and have intrinsic features such as: irregularity, aperiodicity, and are impossible to predict over long periods of time. These features provide chaos communication systems with unique advantages including: low power spectral density, mitigation to multi-path fading as well as high security and anti-jamming capabilities [2] [3] [4] [5].

Chaos theory has been established since the 1970s from many different research areas, such as physics, mathematics, and biology etc. Chaos is an aperiodic long-term behavior in a deterministic system that exhibits sensitive dependence on initial conditions. More specifically, the Aperiodic long term behavior indicates that the systems trajectory in phase space does not settle down to any fixed points, periodic orbits, or quasi periodic solutions as time tends to infinity. These systems are also deterministic, meaning that there are no probabilistic parameters in the system. Finally, the most unique feature of chaotic systems is their sensitive dependence on initial conditions. This means that trajectories originating from very nearly identical initial conditions will diverge exponentially quickly. Over the last two decades there has been much interest in utilizing chaos theory in telecommunication systems. Since chaotic systems are generated from deterministic systems, appear to be noise-like and are sensitive to initial conditions, telecommunication systems that require a high level of security have been developed using chaotic signals. Chaotic waveforms which are generated from chaotic non-linear dynamical systems are inherently wideband in nature and perfect candidates for spreading narrowband signals. Therefore, using chaotic signals to spread our data signal, results in a spread-spectrum signal that has a larger bandwidth and lower power spectral density. To understand how chaotic signals are generated, it suffices to understand discrete-time representations of dynamical systems. More specifically, when a system is described in discrete-time, its state-variables are sampled at fixed time intervals and its dynamics are described by an iterative function which expresses the state variables at one sampling instant in terms of those at the previous sampling instant, i.e., $x_n = f(x_{n-1},)$, where x_n is the vector of state variables sampled at the nth sampling instant, f(.) is the iterative function that describes the dynamics of the system, and is the vector of parameters that affects the system dynamics.

Figure 1.1 shows a simple overview of chaos shift keying (CSK) digital communication system. The system works as follows. The transmitter consists of two chaos generators f and g, producing signals $\hat{c}(t)$ and $\breve{c}(t)$ respectively. If a binary +1, $\hat{c}(t)$ is to be sent , is transmitted and if -1, $\breve{c}(t)$ is to be sent, is transmitted. On the receiver end, the exact same chaotic signals are replicated by just knowing the initial conditions used to generate f and g. Then the incoming signals are correlated with the replica chaotic signals at the receiver to make a decision on the transmitted bit. This system can also be considered a CDMA-BPSK system using chaos-based spreading sequence. There are many benefits of using chaotic signals in communications systems. We mentioned earlier that chaotic signals have random, noise-like behavior and broad-band power spectra. Thus by embedding data information in these signals, it is possible to increase the security of the signals substantially. Since chaotic signals are broadband signals, they inherit the conventional advantages of spread spectrum signals such as low probability of interception, anti-jamming, mitigation

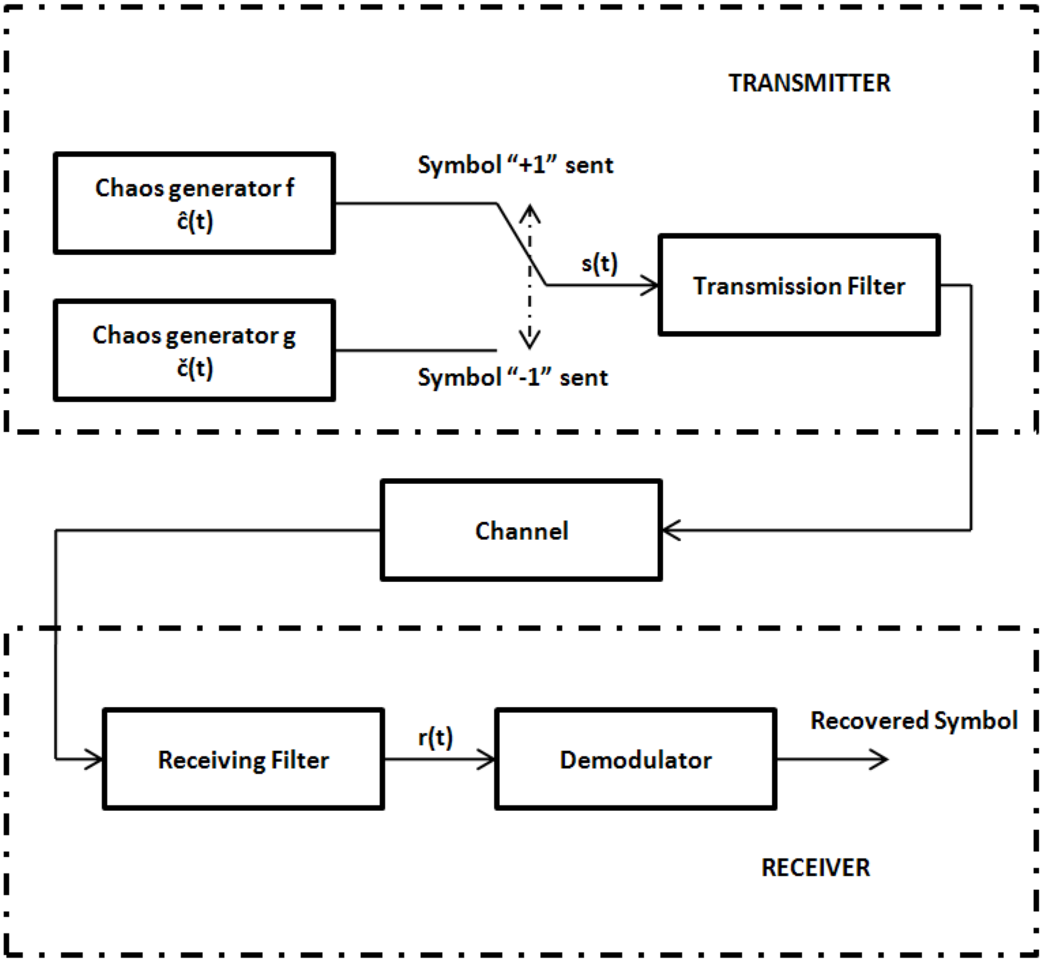

Figure 1.1: Chaos Communication System

of multipath fading etc. Also, chaotic signals are easy to generate and theoretically infinite in quantity, thus providing a low-cost solution to spread-spectrum communications.

1.2 Cognitive Radio

Cognitive radio has emerged recently as a powerful means to tackle the spectrum congestion problem. A cognitive radio transceiver is aware of its environment and capable of adapting it RF parameters according to the environment. Figure 1.1 shows the autonomous adaptive process of a cognitive radio. One of the main focus of research in cognitive radio is

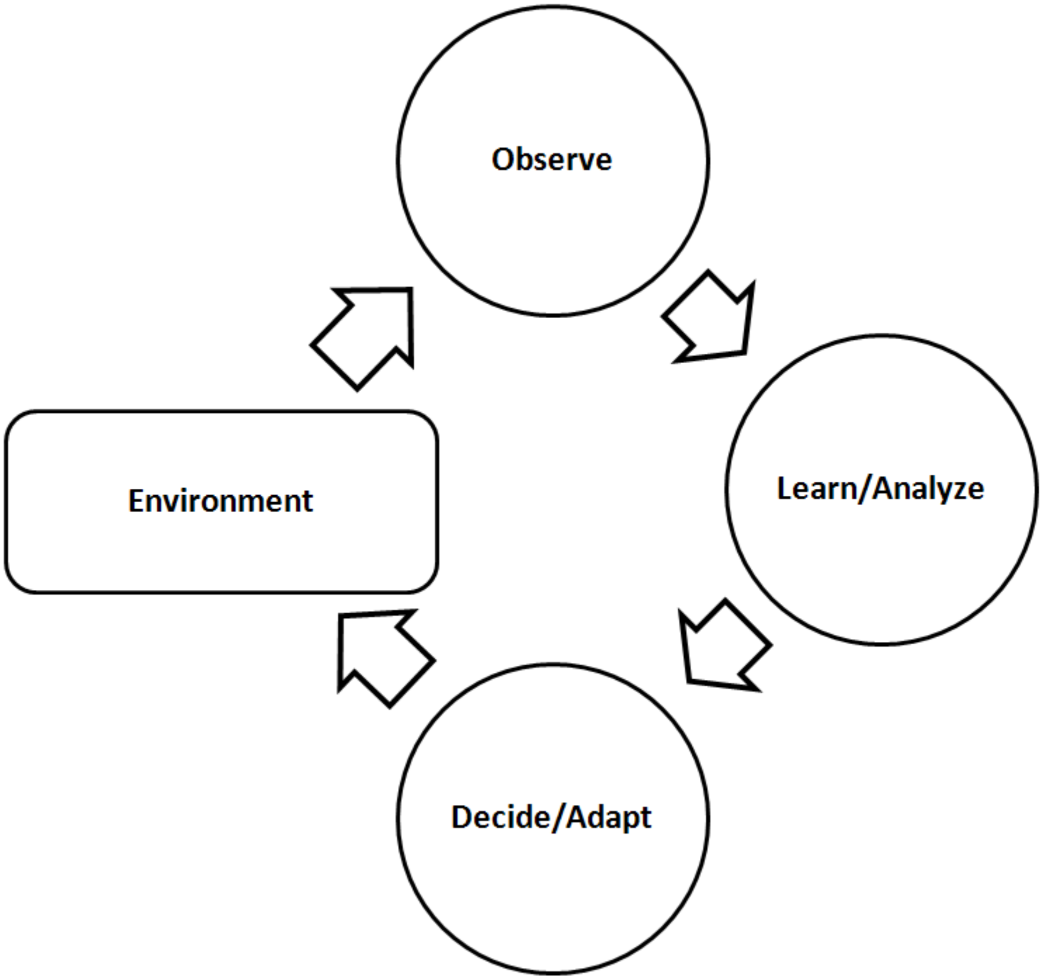

Figure 1.2: Cognition cycle of a Cognitive Radio

dynamic spectrum access (DSA). While majority of spectrum has been allocated to different users, most of the spectrum is not used efficiently. Recent studies suggest that most of the allocated spectrum is unused or under-utilized most of the time. To exploit such unused spectrum, an overlay cognitive radio can improve the spectrum efficiency by transmitting over spectrum holes without causing harmful interference to the primary users [6] [7] [8].

It is highly desired to combine the benefits of the chaos communication system with the cognitive radio to create a robust, highly secure, flexible chaotic cognitive radio system. However, current chaos communication systems employ time domain generated chaotic signals. Such chaotic signals occupy one single contiguous frequency band, making it impossible to exploit the non-contiguous nature of spectrum holes available in a cognitive radio and DSA scenario.

Chaos vs. Conventional PN

The application of chaos to direct-sequence spread spectrum was reported by Heidari-Bateni and McGillem in 1992. The basic principle called to replace conventional PN sequences such as m-sequences or Gold sequences by chaotic sequences generated by a discrete-time non-linear map. It has been shown that chaotic sequences have comparable auto-correlation and cross-correlation properties and superior bit-error rate performances in multiuser communication than conventional PN sequences. There are also several properties of chaotic sequences that make them superior to conventional sequences. Firstly, conventional PN sequences are generated by linear feedback shift registers (LFSRs). This makes these codes much easier to decipher once a short set of bits from the sequence is known. Chaotic sequences on the other hand are considered very secure because of its aperiodicity and unique property of high sensitivity to initial conditions. Secondly, for a given m-stage LFSR, there is a limit to the maximum number of sequences that can be generated. However, with the large number of chaotic maps available and the fact that changing the initial conditions, generates a completely new sequence, there are theoretically an infinite number of chaotic sequences that can be generated. We can conclude that when our primary design considerations are security, simple implementation, and many users required on the communication system, chaotic sequences are definitely the better choice over conventional PN sequences [9] [10] [11].

Now that we have given a brief overview of chaotic spreading sequences, we will compare them with two other well known spreading sequences. M-sequences and Gold sequences are the most popular conventional spreading sequences in spread spectrum systems. M-sequences, also known as maximum-length sequences are sequences that repeat every 2n-1, where n is an integer. These sequences can be implemented using shift registers. Similarly, Gold codes are constructed from a preferred pair of m-sequences, by the element-by-element multiplication of one m-sequence with every time shift of the second m-sequence [12] [13].

2.1 Auto-Correlation

One of the most important characteristics of PN sequences is its auto-correlation properties. At the receiver, the received signal is mixed with a locally generated PN sequence. This must result in maximum auto-correlation, or signal strength at the point of synchronization for the best decision to be made on the incoming signal.

Figures 2.1 and 2.2 show, the autocorrelation of a 31-bit m-sequence and Gold codes respectively. Figure 2.3 shows the autocorrelation of a L = 31 chaotic sequence. M-sequences are said to have very good autocorrelation properties because of their balance property, which means that the sequence will have exactly one more high bit than low bit. This is the closest a sequence consisting of an odd number of 1 s can get to a zero average. The autocorrelation is given as N when the time lag is 0 and given as -1/N at all other times. Gold sequences can be unbalanced and thus causing some spikes in their autocorrelation properties. The table below shows the correlation bounds of the non-zero lags of the auto-correlation. We can notice that the auto-correlation bounds are comparable between the Gold sequence and chaotic sequence given in Figure 2.3.

	$Mean$	Max	$Bounds$
m-sequence	5.22e-4	1	[0,-0.09]
Gold	0.0259	1	[0.23,-0.21]
Chaos	5.28e-4	1	[0.21,-0.24]

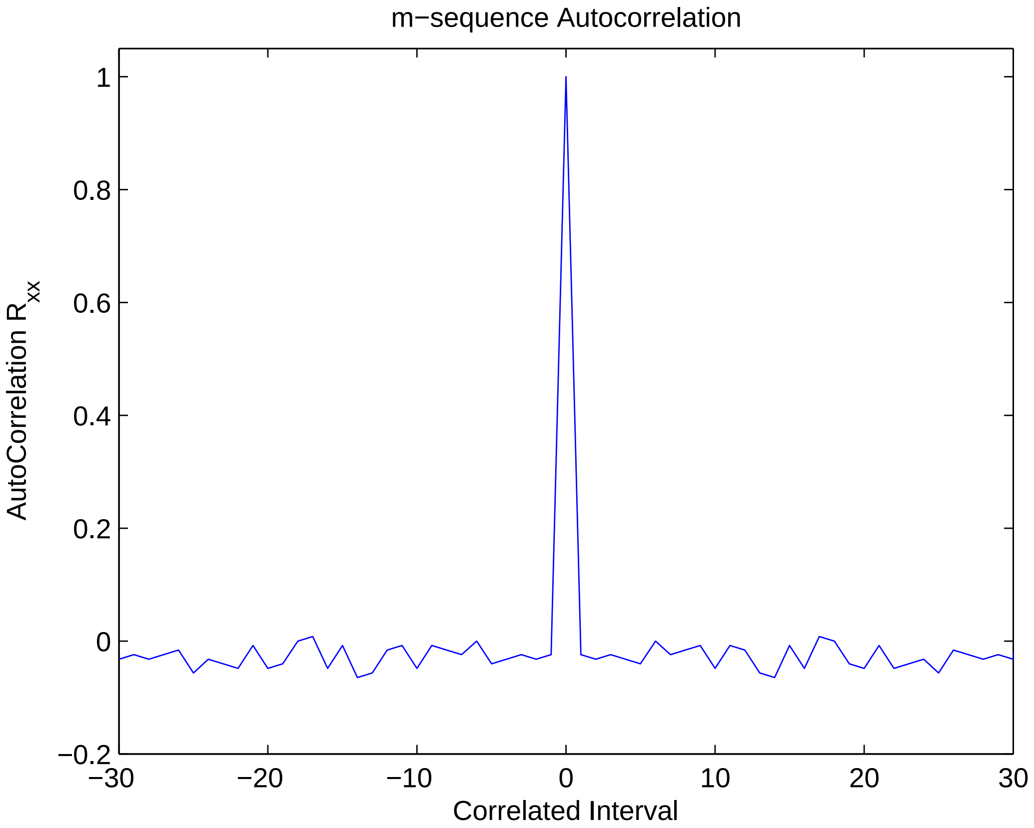

Figure 2.1: Auto Correlation of m sequence

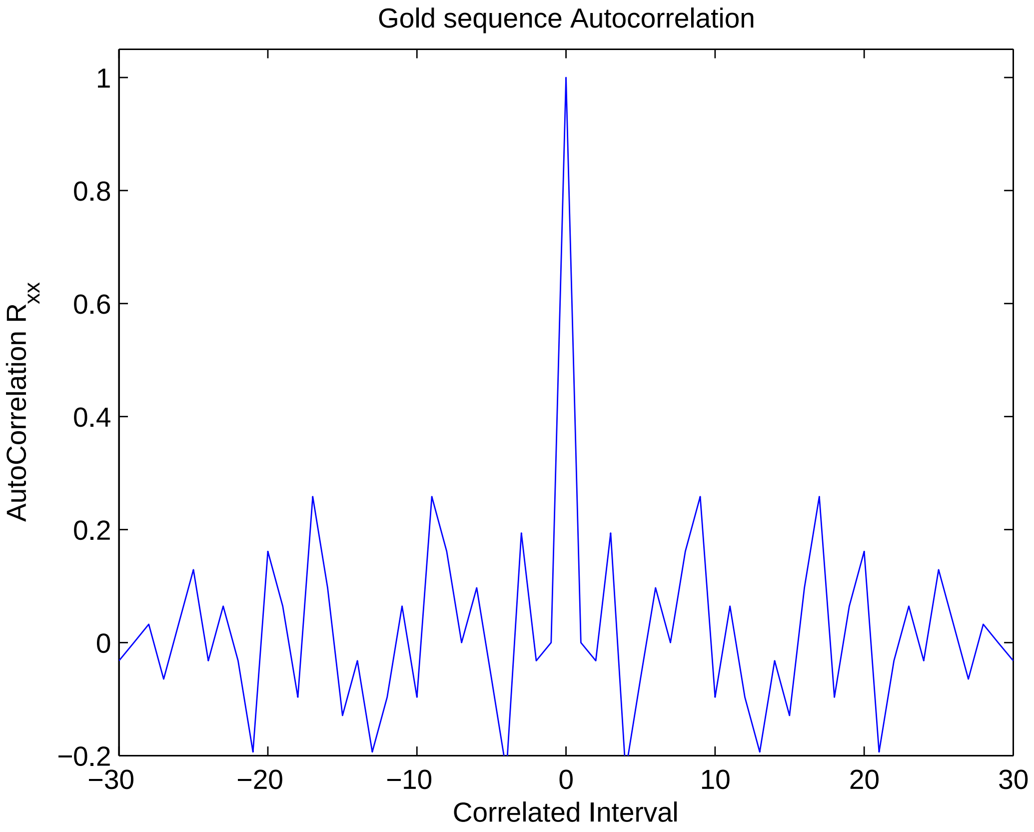

Figure 2.2: Auto Correlation of Gold sequence

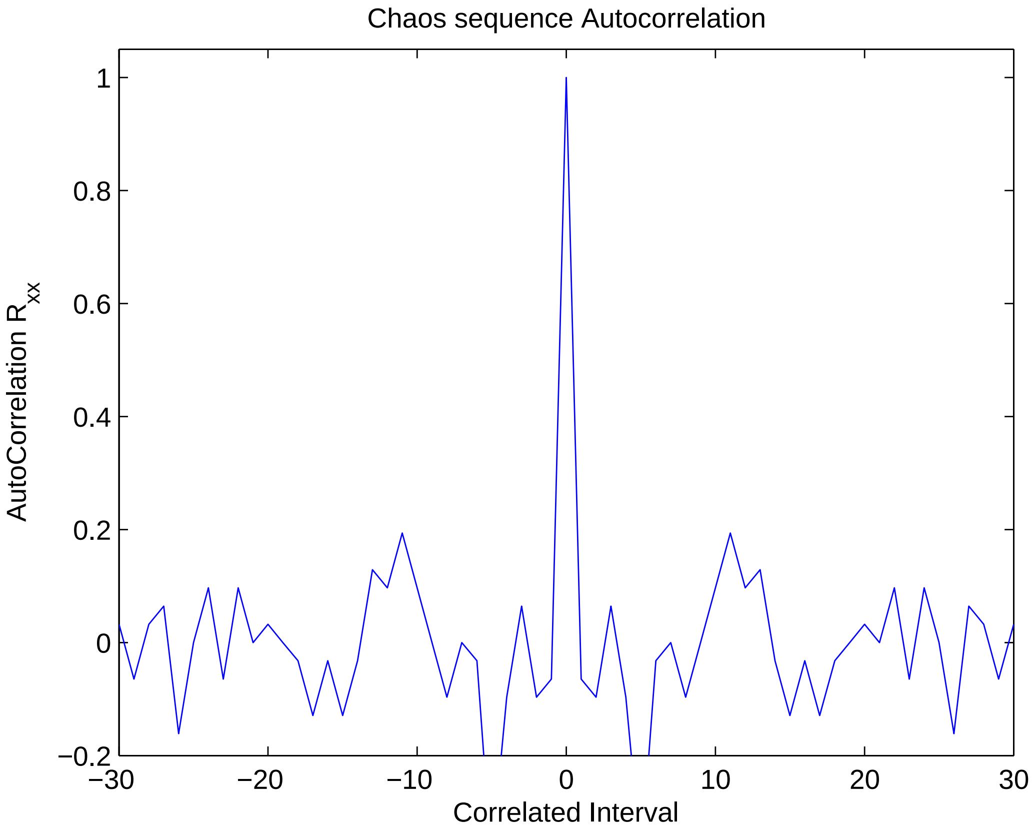

Figure 2.3: Auto Correlation of Chaos sequence

2.2 Cross-Correlation

Another desired property in PN sequences is minimum cross-correlation. In a spread-spectrum system with multiple users, when the received signal is mixed with the locally generated PN sequence, it must result in minimum signal strength. This would ensure the receiver would be able to differentiate between the transmitted PN sequence, and PN sequences of other users.

Figures 2.4,2.5 and 2.6 show the cross correlation of m-sequences, Gold and Chaos sequences. We can see from the table below that the cross-correlation bounds are approximately the same for all three sequences. Studies show that m-sequences have very bad cross correlation properties. In our simulation we see that the correlation bounds are about 0.21 and -0.24 for all three sequences. For much longer sequences, Gold codes have much lower cross-correlation than m-sequences, and chaotic sequences have been known to achieve much lower cross-correlation bounds than Gold codes [14] [15].

	$Mean$	Var	Max	$Bounds$
m-sequence	-1.22e-18	0.5328	0.2395	[0.21,-0.24]
Gold	-1.47e-18	0.6294	0.3316	[0.31,-0.24]
Chaos	-6.82e-19	0.5907	0.3112	[0.29,-0.21]

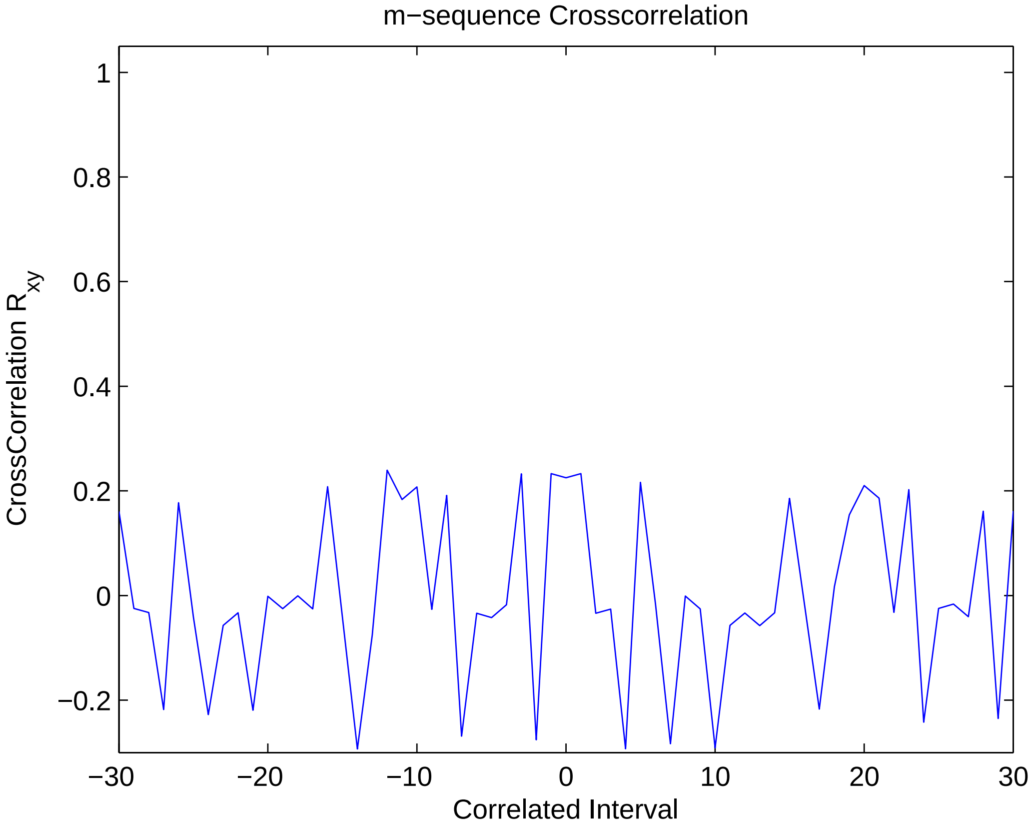

Figure 2.4: Cross Correlation of m sequences

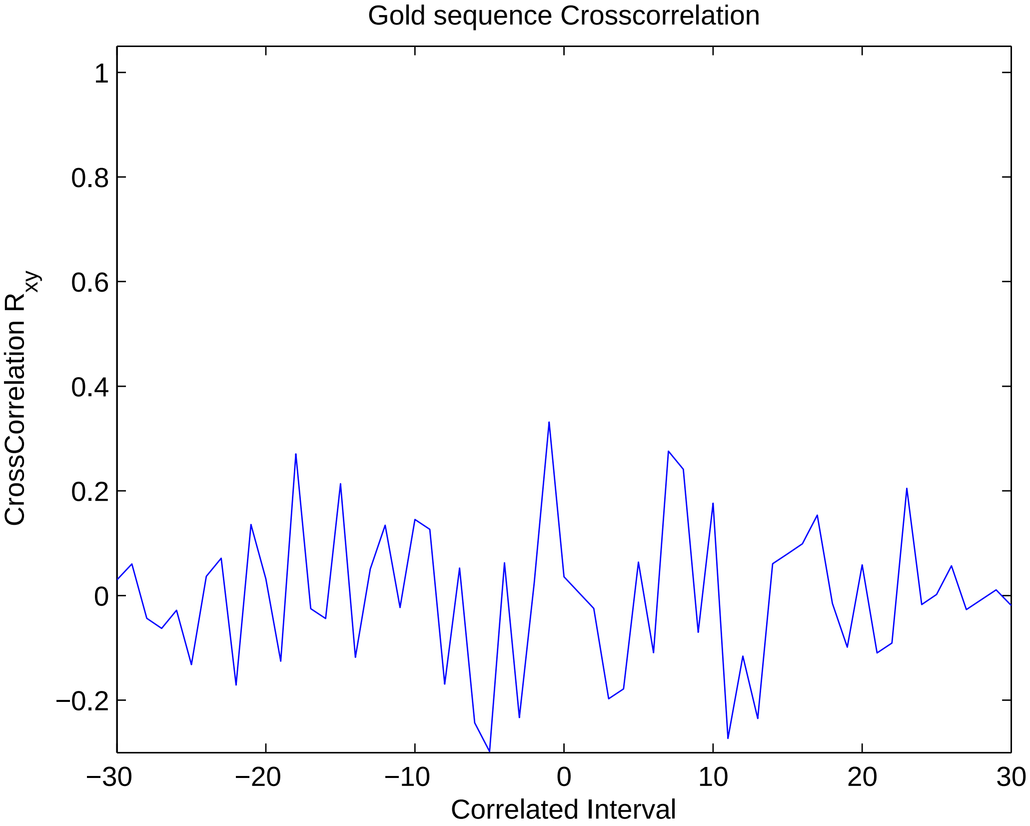

Figure 2.5: Cross Correlation of Gold sequences

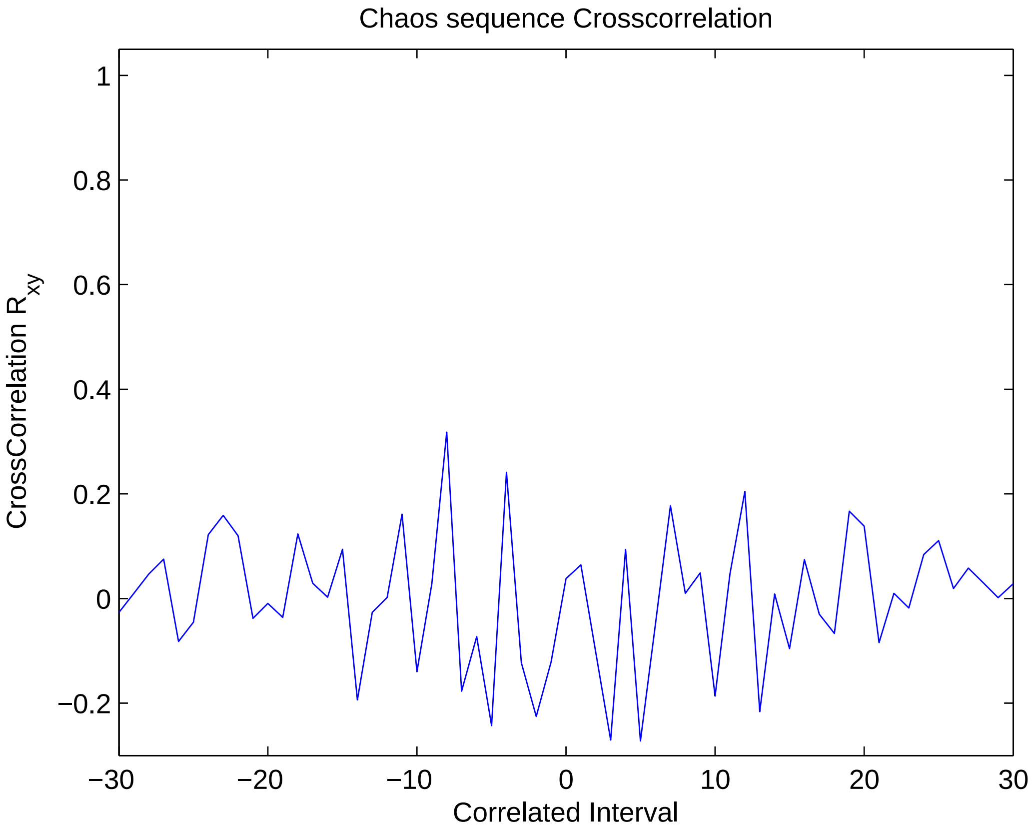

Figure 2.6: Cross Correlation of Chaos sequences

2.3 BER Performance

In digital communication, the bit-error rate (BER) is the number of errors in decoding a received bit, divided by the number of transmitted bits during a certain time interval. The errors can be caused due to noise in the channel or interference from other users on the same channel. The bit error rate is one of the best performance measures in comparing different communication systems. Following is a comparison of the BERs of conventional spreading sequences to chaotic spreading sequences. Figure 2.7 and 2.8 show the multiuser performance of length 31 of these sequences in AWGN Channel. Gold sequences seems to perform the best, followed by chaotic sequences and finally m-sequences. There seems to be only about 0.5dB difference between these sequences. If performance is not top priority but rather security, chaotic sequences seem to be the better choice [16] [17] [18].

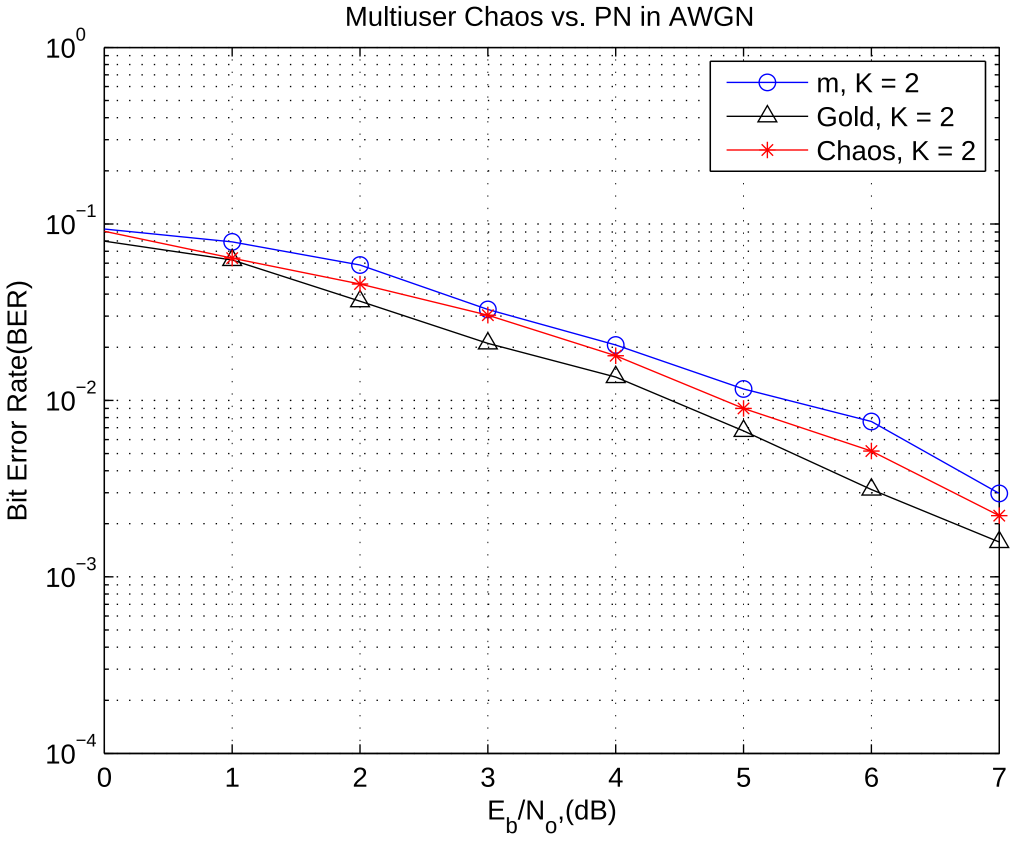

Figure 2.7: Two-User: Chaos vs. Conventional PN Sequences

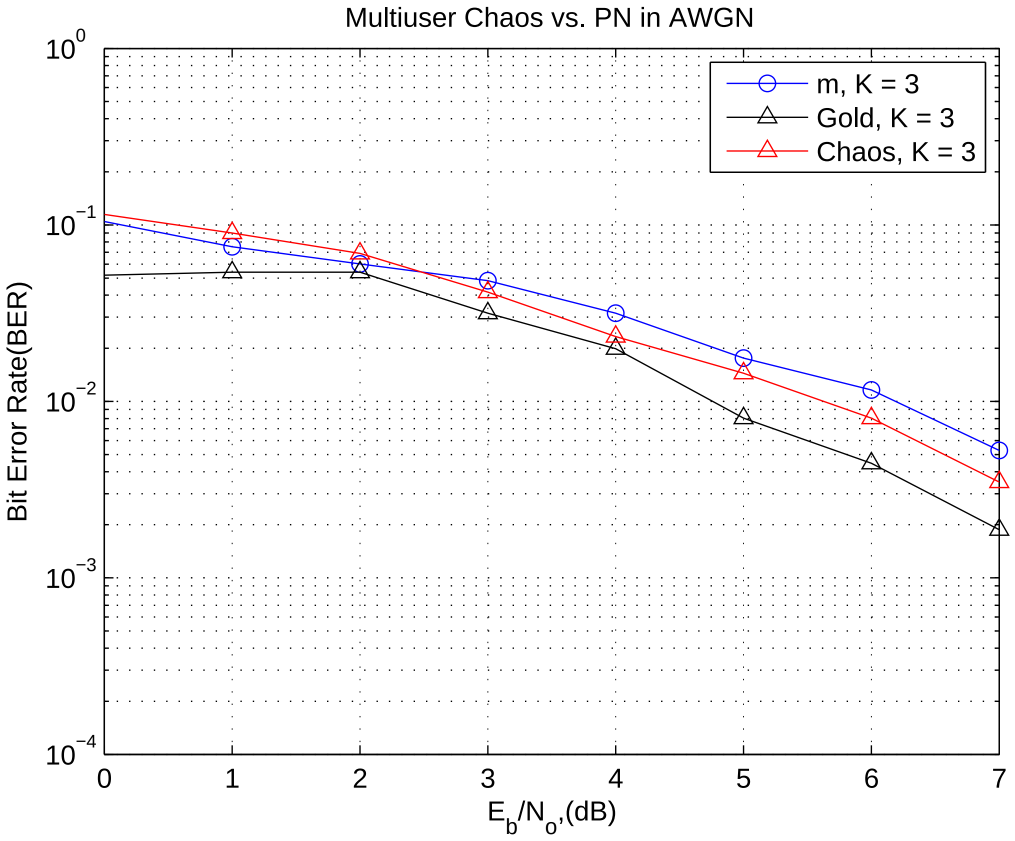

Figure 2.8: Three-User: Chaos vs. Conventional PN Sequences

2.4 Multiuser Capability

N	$m - sequence$	$Gold$	$Chaos$
7	2	9	>>9
15	2	17	>>17
31	6	33	>>33
63	6	65	>>65
127	18	129	>>129
255	16	257	>>257
511	48	513	>>513

We now come to the main advantages of Chaos sequences. The first of these is its higher multiuser capability. As shown in the table above, m-sequences have certain properties and only a limited number can be generated given a certain length of the sequence. Gold Codes have a much greater benefit over m-sequences in the number of possible sequences that can be generated. Gold codes are generated by carefully selecting certain m-sequences that exhibit a criterion of correlation properties. The maximum number of Gold codes that can be generated for a given length of sequence N is $N + 2$ sequences. This is a definite advantage over m-sequences in a multiuser scenario, when many users are required on the system. On the other hand, Chaos sequences have a far greater amount of possible sequences that can be generated. Because of its unique property of sensitivity to initial conditions and a large number of chaotic waveform equations, the number of chaotic sequence though not infinite, but a much much larger amount compared to m-sequences and even Gold codes. A drawback of this is that this might increase the interference between the different users on the system using chaotic sequences.

2.5 Security

We finally come to the main advantage of chaotic sequences over conventional PN sequences, its high security capability and low probability of interception. When it comes to security of a system in comparing these 3 spreading sequences, chaotic sequences definitely are much more secure than conventional PN sequences. This is mostly because of their aperiodicity and their inherent feature of sensitivity to initial conditions. Figure 2.9 shows the waveform of a first order chaotic dynamical system known as a Logistic Map. We can notice from the figure the noise like characteristics of the chaotic signal. Also, we notice that the signal is bounded within the range [-1, +1]. The figure specifically shows the unique feature of chaotic signals' sensitive dependence on initial conditions. Generating the Logistic Map from two slightly different initial conditions, i.e. (x0 = 0.1, 0.1001) we can notice that after a few iterations the system diverges exponentially.

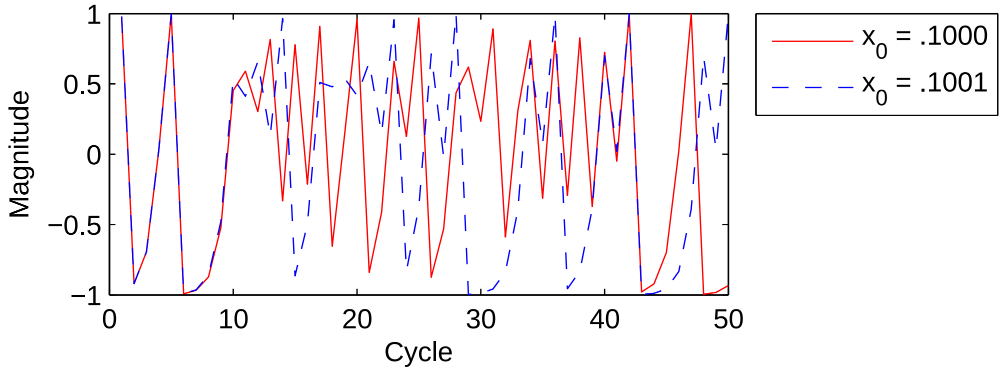

Figure 2.9: Sensitivity to Initial Conditions for Chaos Sequences

The primary reason for choosing chaotic waveform as a means of transmitting data is the high security of chaos sequences and the low probability of interception of these sequences. The fact is that, unless the exact initial condition, and the same chaotic waveform equation is known to the enemy, it is impossible to recover the signal. In Figure **??** we try to decode a signal transmitted using a chaotic waveform. The enemy is assumed to have selected the correct chaotic waveform generator (Logistic Map in this case). Also, the enemy has been able to guess the initial condition only 10^{-10} off from the transmitted chaotic signal. We can see that the enemy is unable to decode the original sequence if he is even off by an ϵ value of 10^{-10}.

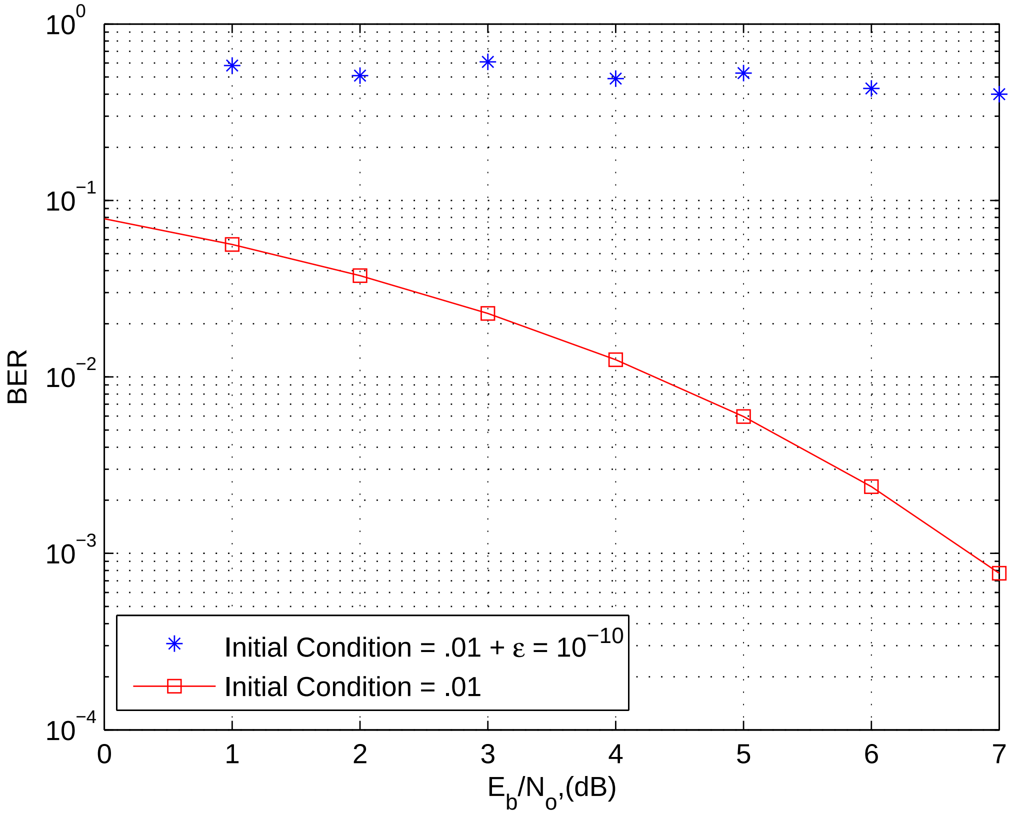

Figure 2.10: High Security Analysis of Chaotic Sequence

We have now compared chaotic spreading sequences to conventional PN sequences using some key measures including, autocorrelation, cross correlation, BER performance, security features, and some other measures. Using chaotic sequence for spectral spreading in a direct-sequence spread-spectrum system has been shown to provide several advantages over conventional PN sequences. One advantage is the availability of an enormous number of different sequences of a given length as compared to the maximal length and Gold code sequences. Generation and regeneration of chaotic sequences is very simple and involves the storage of only a few parameters and functions even for very long sequences. The inherent aperiodic and sensitive initial conditions features in chaotic sequences are definitely properties that can be used to make a system more secure. We can conclude that when security, simple implementation, and many users required on a MC-CDMA communication system are primary design considerations, chaotic sequences are definitely the better choice over conventional PN sequences.

Frequency Domain Based Chaos

3.1 Motivation

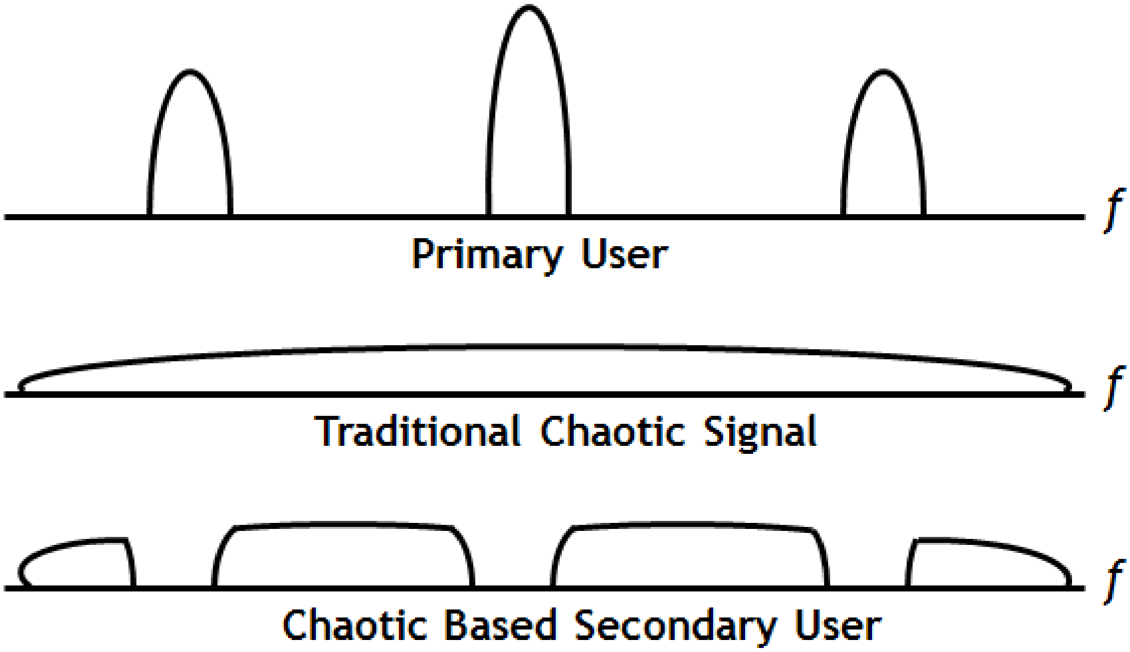

Figure 3.1: (a)Primary User (b)Traditional Chaos (c) NC Chaos

As mentioned before, cognitive radio technology is a paradigm shift in the wireless world that is capable of solving the spectrum congestion problem. Consider Figure 3.1(a) where we have a bandwidth of interest that we are considering to transmit our chaotic waveform over. Traditional chaotic signals, which are generated in the time domain, 3.1(b) cover a contiguous bandwidth in the frequency domain, making it incompatible for cognitive radio technology. We propose to generate the chaotic waveform in the frequency domain that can function over multiple non-contiguous frequency bands. By doing this we will combine the high security benefits of chaos communication systems with the spectral efficiency capability of cognitive radios

3.2 System Description

Figure 3.2 illustrates the proposed chaos cognitive radio communication system. As shown in the figure, the binary data $b(t)$ is multiplied with the chaos waveform $c(t)$ before modulation. At receiver side, a correlator receiver performs correlation of received signal $r(t)$ with the chaos waveform $c(t)$. The uniqueness of this chaos cognitive radio communication system is the frequency domain based chaotic waveform generator.

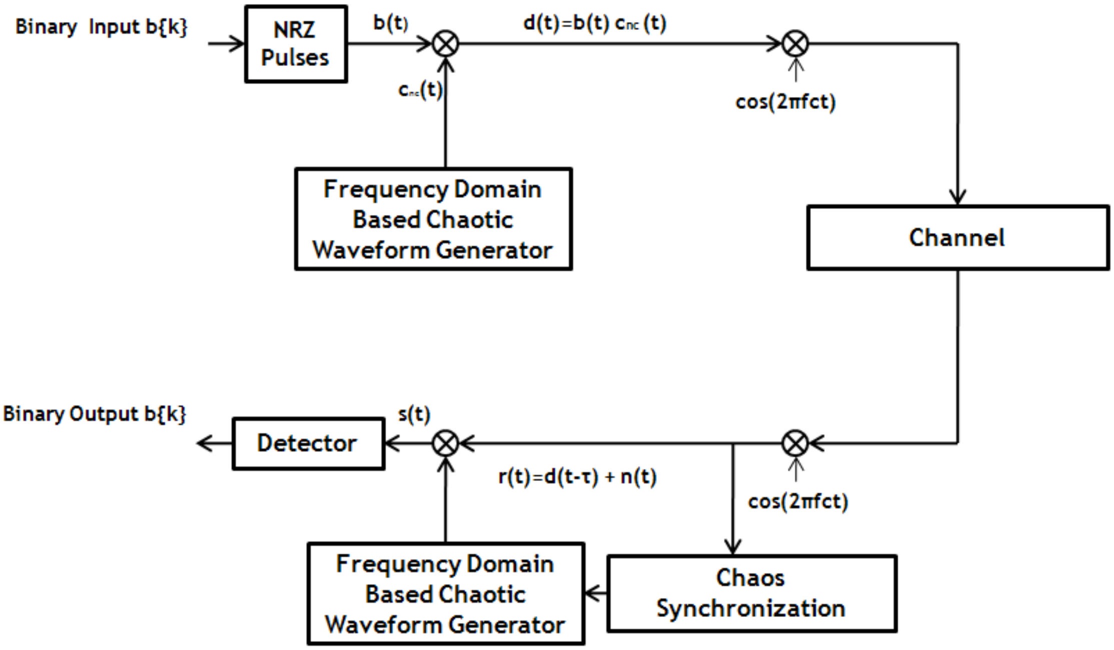

Figure 3.2: Frequency Domain Processing Based Chaos Communication System

Figure 3.3 shows the conceptual model of the frequency domain based chaotic waveform generator. To generate the chaotic sequence, we used a discrete-time representation of an iterative function. This chaotic non-linear dynamical system describes its state variables at one sampling instant in terms of the previous sampling instant, i.e $x_n = f(x_{n-1})$, where x_n is a vector of state variables sampled at the n^{th} sampling instant and f(.) is the iterative function that describe the behavior of the system. A logistic map is used to generate an N length chaotic vector $\overrightarrow{c} = [c_1, c_2, \ldots, c_N]$. The equation for the logistic map is given by,

$$x_n = 1 - 2(x_{n-1})^2 \tag{3.1}$$

The logistic map is one of the simplest dynamical systems capable of exhibiting chaotic behavior that is commonly used in spread spectrum applications. An example of a 512 subcarrier chaotic vector is represented in Figure 3.4.

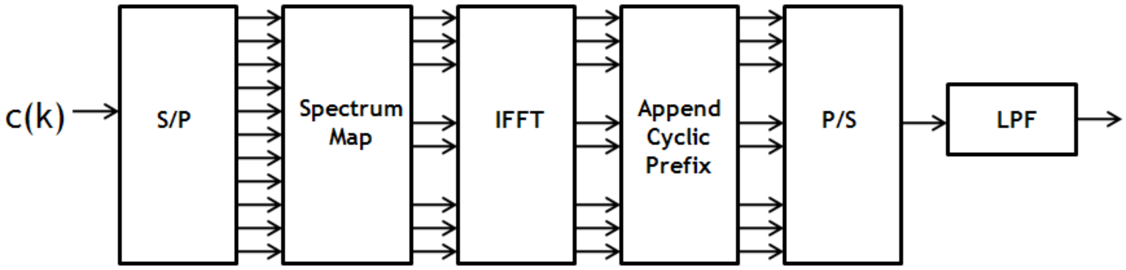

Figure 3.3: Non-Contiguous Chaotic Waveform Generator in Frequency Domain

In cognitive radio and dynamic spectrum access network, a spectrum sensing engine is required to sense the environment and find out the existence and locations of spectrum holes in the band of interest. Subplot (a) in Figure 3.6 shows an example where three primary users with different bandwidth exist in the band of interest. With such spectrum sensing result, we generate a spectrum mask, as shown in Figure 3.6(b), which is essentially a frequency domain window. We then apply this frequency domain window to the frequency domain chaotic signal $\overrightarrow{c}$ to force the frequency samples at frequency bands occupied by the primary users to be zero. As shown in Figure 3.6(c), we obtain a frequency vector $\overrightarrow{C}$

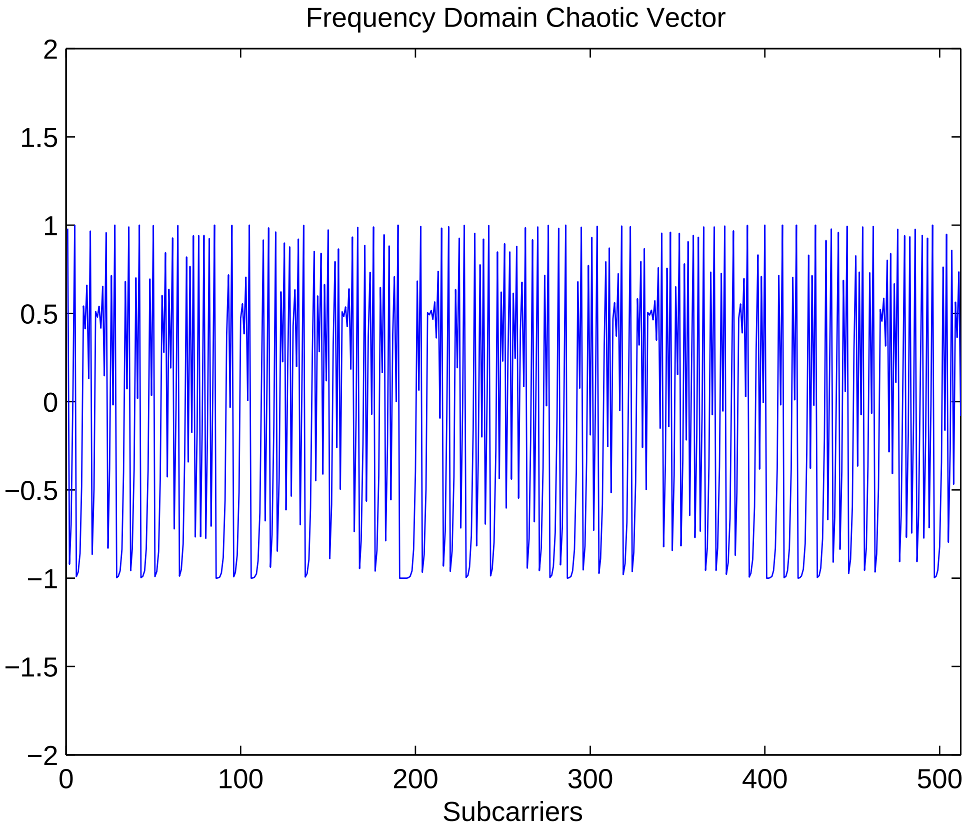

Figure 3.4: Logistic Map: Frequency Domain Sequence

spreads over multiple non-contiguous frequency bands over bandwidth W. By taking the inverse Fourier transform of such vector, we create a discrete chaotic signal $\overrightarrow{C}_{non-contiguous}$ which operates over all available spectrum holes and can be used for cognitive radio. It is evident from Figure 3.6 that the chaotic waveform we create via this frequency domain based non-contiguous chaotic waveform generator generates a chaotic waveform that occupies multiples non-contiguous spectrum bands and is suitable for an overlay cognitive radio system to take advantage of multiple non-contiguous spectrum holes. Another possible method of creating a non-contiguous chaotic waveform, as shown in figure 3.5 is by generating the chaotic vector in the time domain, then taking the FFT to convert it to the frequency domain for notching out the frequencies that are being used by the primary users and then converting it back to the time domain, thus generating the time domain signal of non-contiguous chaotic waveform. In our proposed method shown in figure 3.3 we eliminate the FFT step by simply considering the chaotic waveform as a frequency domain based spreading sequence.

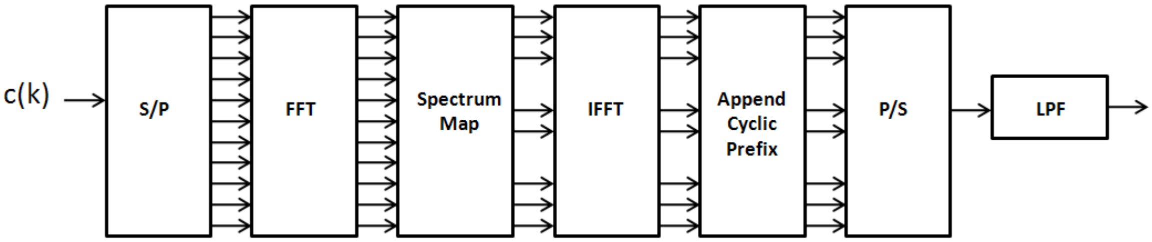

Figure 3.5: Non-Contiguous Chaotic Waveform Generator in Time Domain

After feeding the discrete chaotic signal $\overrightarrow{C}_{non-contiguous}$ through the low pass filter, the continuous chaotic signal $C_{non-contiguous}(t)$ is generated. Employing the continuous chaotic signal $C_{non-contiguous}(t)$, we can now generate a chaos communication system suitable for cognitive radio applications. Specifically, by employing binary chaos shift keying, the transmitted signal corresponds to

$$s(t) = \begin{cases} +C_{non-contiguous}(t) & if \quad b = 1 \\ -C_{non-contiguous}(t) & if \quad b = -1 \end{cases} \tag{3.2}$$

b is the binary digital data.

At receiver side, a chaotic waveform matched filter receiver can be used to decode the digital data modulated on the chaos waveform:

$$\hat{b} = \begin{cases} +1 & if \quad \int r(t) \cdot C_{non-contiguous}(t) > 0 \\ -1 & otherwise \end{cases} \tag{3.3}$$

This non-contiguous chaotic carrier signal as shown in Figure 3.7 will only be transmitted over intended spectrum holes and avoid interference with the primary users.

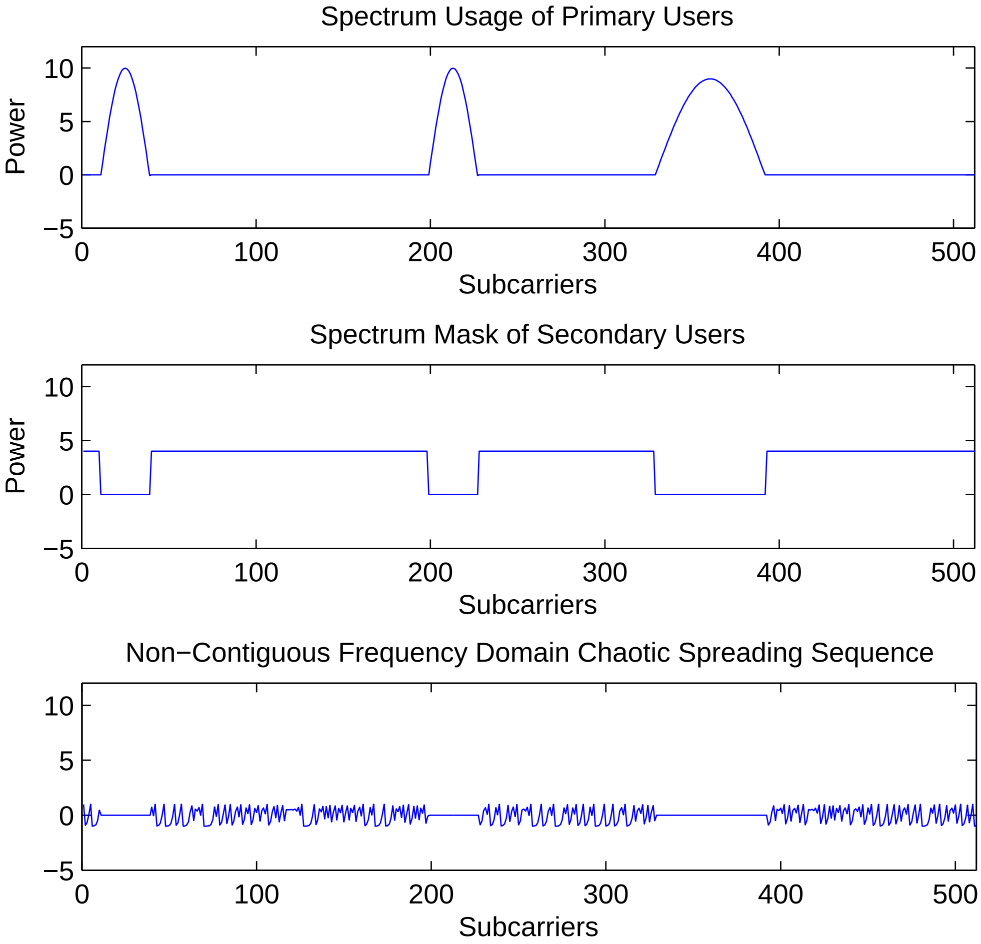

Figure 3.6: Non-Contiguous Frequency Domain Chaotic Signal

3.3 Correlation Analysis

One of the most important characteristics of PN sequences is its auto-correlation properties. At the receiver, the received signal is mixed with a locally generated PN sequence. This must result in maximum auto-correlation, or signal strength at the point of synchronization for the best decision to be made on the incoming signal. Figure 3.8 shows the auto-correlation of a length 512 logistic map chaotic sequence. As shown in the figure, the chaotic waveform provides an auto-correlation close to an impulse. Such auto-correlation make chaotic waveforms ideal for secure spread spectrum communication applications. Another desired property in PN sequences is minimum cross-correlation. In a spread-spectrum system with multiple users, when the received signal is mixed with the locally

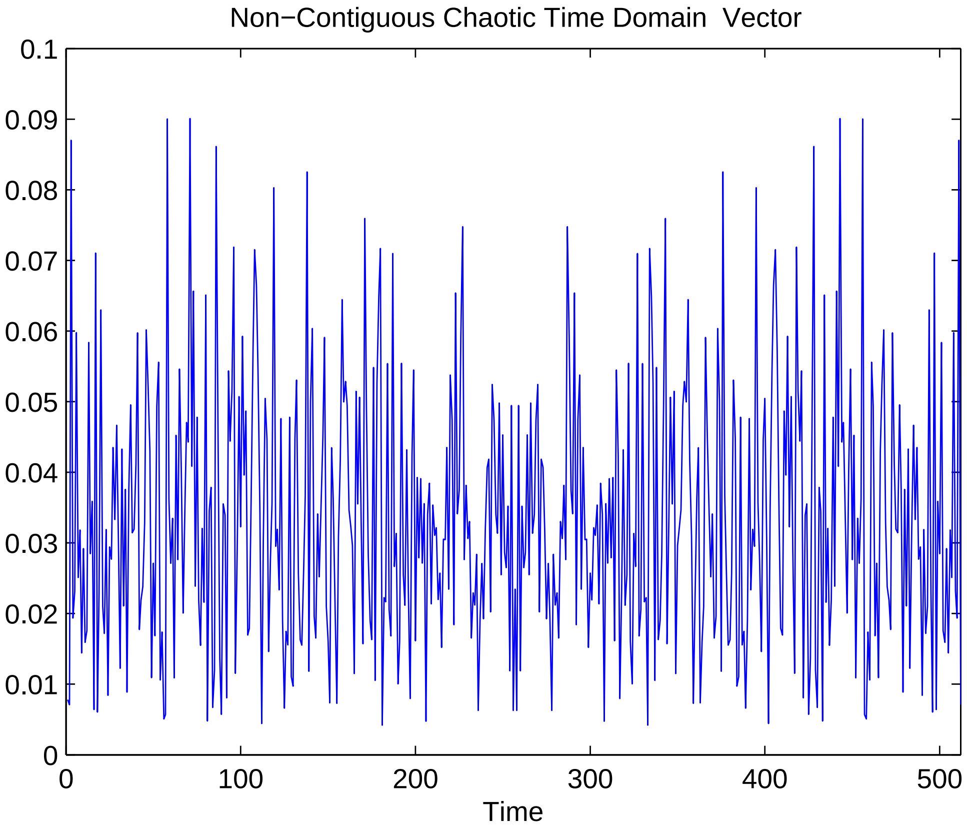

Figure 3.7: Non-Contiguous Chaotic Time Domain Signal

generated PN sequence, it must result in minimum signal strength. This would ensure the receiver would be able to differentiate between the transmitted PN sequence and other PN sequences of other users. Figure 3.8 shows the cross correlation of two separate chaotic sequences is and a cross-correlation close to zero, when using one chaotic map using different initial conditions. In the following section, we demonstrate that the proposed frequency domain processing based chaotic waveforms also maintain these desired auto-correlation and cross-correlation properties.

Figure 3.9 illustrates the auto-correlation and cross-correlation of the same logistic chaotic sequence after the spectrum mask has notched out certain subcarriers which are being used by primary users. Figure 3.10 shows the auto-correlation and cross-correlation of the non-contiguous chaotic waveform after performing the inverse Fourier transform. It is evident from both figures that the desired auto-correlation and cross-correlation properties

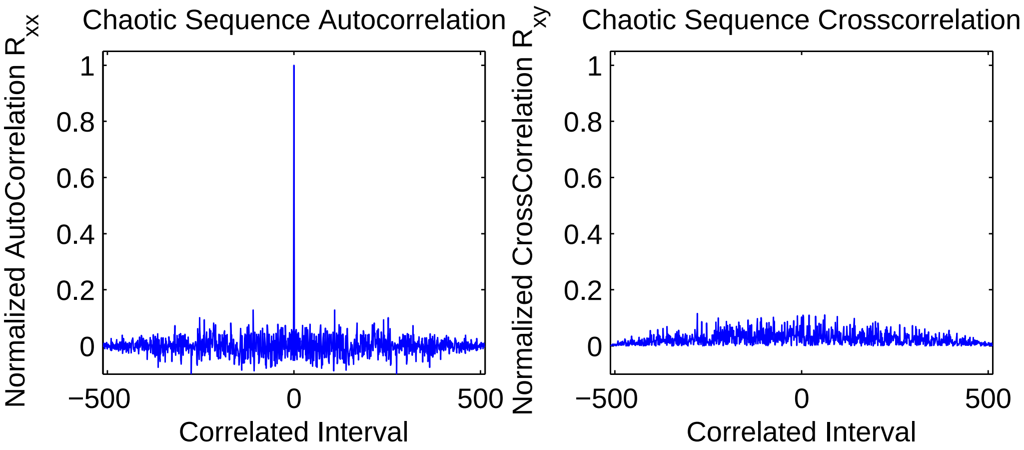

Figure 3.8: Correlation Properties of Logistic Map Chaotic Sequence

are maintained after the conversion from frequency domain back to time domain.

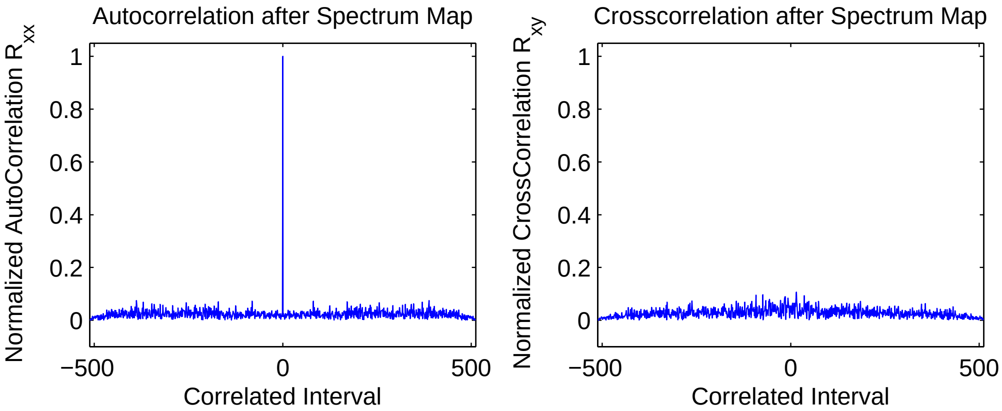

Figure 3.9: Correlation Properties of Non-Contiguous Chaotic Sequence

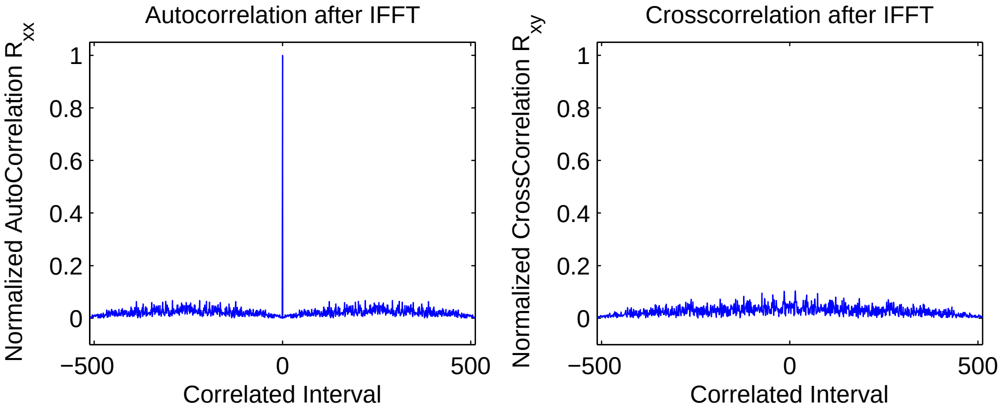

Figure 3.10: Correlation Properties of Non-Contiguous Waveform after IFFT

3.4 BER Analysis

In this section we analyze the BER performance of the proposed non-contiguous chaotic communication system.

3.4.1 BER in AWGN Channel

There are two approaches to calculate the BER performance of chaotic communication system in the literature. The first method employs Gaussian approximation to approximate the power of multiple access interference (MAI) in a multi-user chaotic communication system. Given a chaotic sequence c_t, let $\Psi = [(c_t^i)^2]/E^2[(c_t^{(i)})^2]$, K is the number of users, N is the length of the spreading sequence. Assume all K users have equal average transmit power P_s then $E_b = \beta P_s$ and N_o is the variance of the noise. As stated in [19] [20], the BER performance for a multi-user system using CPSK modulation, in an AWGN Channel is,

$$BER_{CPSK} = \frac{1}{2} erfc\left(\left[\frac{\Psi}{N} + \frac{K-1}{N} + \frac{N_o}{E_b}\right]^{\frac{1}{2}}\right) \tag{3.4}$$

However, when the length of the chaotic sequence employed in the chaotic communication system is small (e.g., less than 10), the Gaussian approximation is not accurate enough. Hence, an exact BER analysis method has been proposed in [6]. First, they obtained an exact Gaussian mean and variance while considering the spreading and the bits used by the other users. Also, the full dynamics of the spreading and on the bits are used to uncondition the result to obtain the exact BER. This is obtained as an N-dimensional integral over independent invariant distributions of the chaotic spreading [14].

Since the non-contiguous chaotic waveform is naturally combined with an overlay cognitive radio, the secondary user employing the non-contiguous chaotic waveform does not cause interference to the primary users, nor experiences interference from the primary users. Hence, the BER performance of the proposed frequency domain based non-contiguous chaotic communication system stays the same as traditional chaotic communication system and both existing methods can be applied depending on the length of the chaotic sequence in the system.

Figure 3.11 shows the simulated BER performance of a single user system using a Logistic Map with a spreading sequence of 512 in an AWGN channel with three primary users coexisting on the band of interest. The spectrum usage map is shown in Figure 3(a). As expected, the BER performance of the proposed system suffers about 3dB performance loss to a BPSK system in an AWGN channel. This is because chaotic sequences, unlike m-sequences and gold sequences which are binary in nature, are the inherently non-binary sequences. Specifically, this loss in performance is due the fact that in any given bit period the energy per bit could be very low, causing an error in correlation at the receiver. This performance loss can be compensated by employing a normalized chaotic waveform operation which forces the chaotic sequence to $+1$ and -1. This result is confirmed by the simulation shown in Figure 3.12. However, the performance gain shown comes with less security advantage. This loss in security is due to the fact that, after a while an enemy can sense a signal being transmitted with the binary sequence $+1$ and -1. The chaotic sequence loses a little of its noise like properties, thus reducing the security advantage.

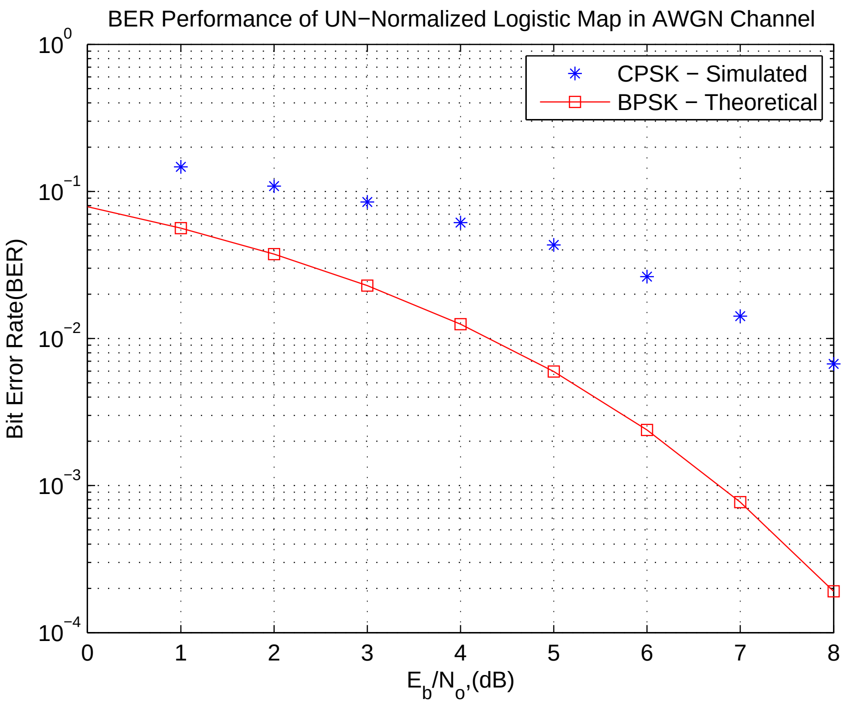

Figure 3.11: BER Performance of Unnormalized CPSK

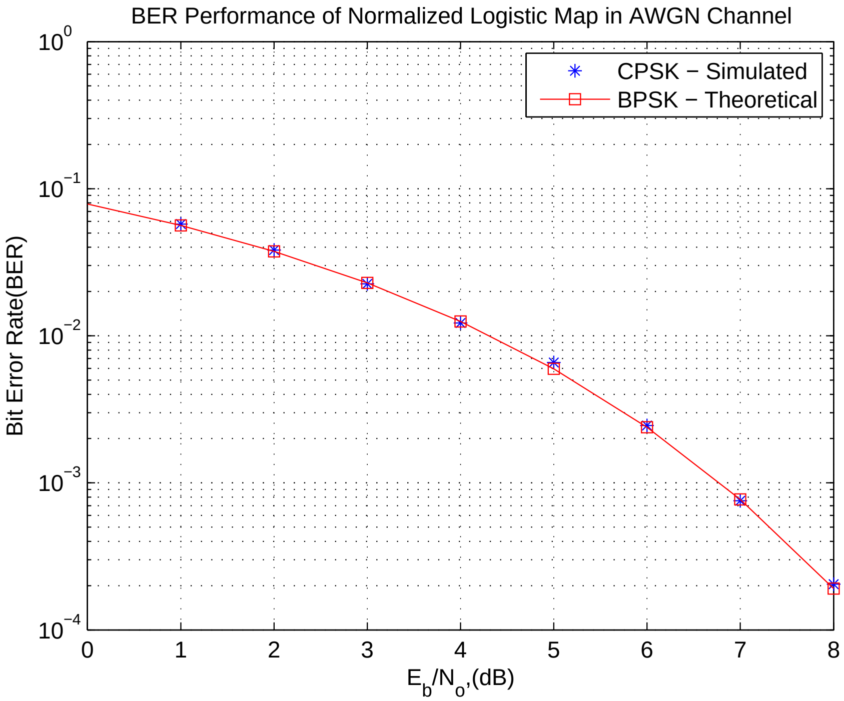

Figure 3.12: BER Performance of Normalized CPSK

3.4.2 BER in Multipath Fading Channel

Here we examine the BER performance of the proposed system in multipath fading channels. The chaos generator is a logistic map with a spreading sequence of length 256. A two-path rayleigh fading channel model is employed where the second path is uniformly distributed among $[0, T]$. The non-contiguous chaotic waveform is generated and a binary chaotic phase shift keying (CPSK) modulation is applied. At receiver side, a Maximum Ratio Combining (MRC) is employed to exploit frequency diversity across all the spectrum holes. The BER versus SNR curves are shown in Figure 3.13. It is evident that the proposed non-contiguous chaotic cognitive radio system is capable of exploiting frequency diversity in a multi-path fading channel and thus offering better BER performance.

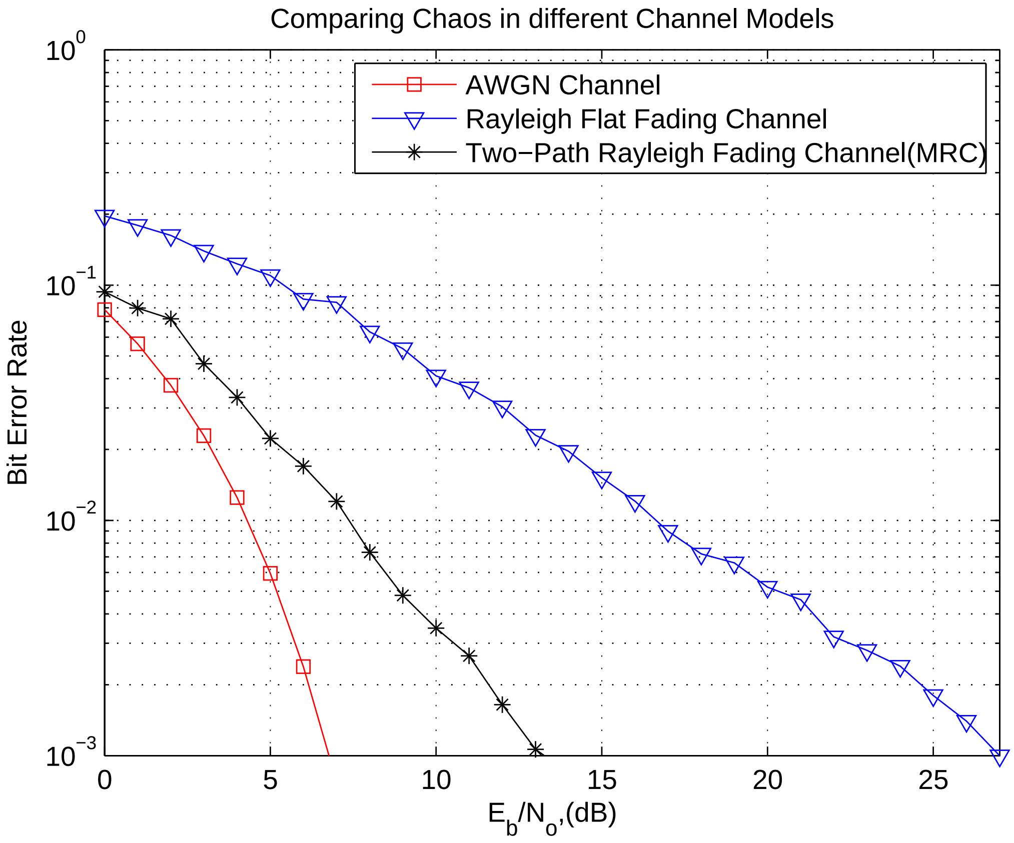

Figure 3.13: BER Performance of Normalized Chaos in different Channels

3.4.3 BER for Multiuser Scenario

Since, chaotic sequences have good auto-correlation and cross-correlation properties, they are good candidates for spread spectrum applications. Specifically, a set of chaotic sequences with good cross-correlation properties can be used in Multi Carrier Code Division Multiple Access (MC-CDMA) systems. We suggested earlier that chaos spreading sequences are ideal for multi-user scenario because of the theoretically infinite sequences that can be generated by just changing the initial condition of the chaotic iterative function. Conventional binary sequences like m-sequences and Gold sequences have only a finite number of separate sequences that can be generated. In a multi-user chaotic system, generation of different spreading sequences would be very easy with just one chaotic function at the transmitter and regenerated at the receiver. Figure 3.14 shows two chaotic sequences generated from one chaotic function using initial conditions very close to each other. We can see that these sequences diverge exponentially after the first few iterations.

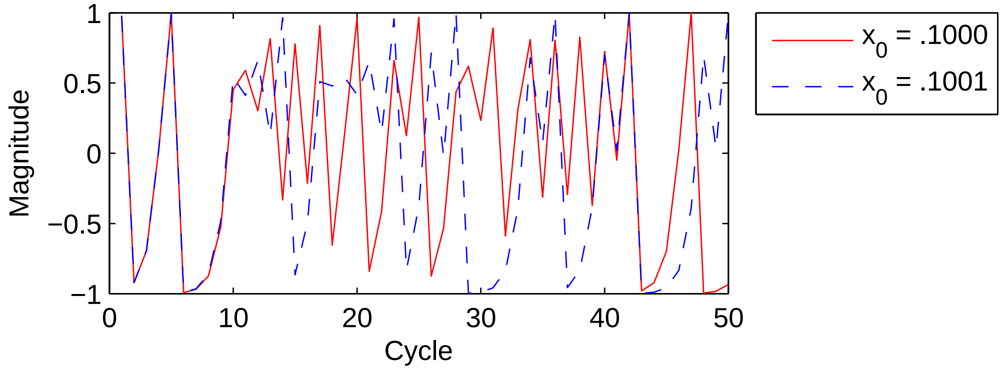

Figure 3.14: Logistic Map: Sensitivity to initial conditions

In Figure 3.15 we have the results of using chaotic spreading sequences in a K user MC-CDMA system. The unique spreading sequences of both users are generated with a Logistic Map with different initial conditions. The non-contiguous chaotic waveform is generated and a binary chaotic phase shift keying (BCPSK) modulation is applied. As illustrated in Figure 3.16, when the number of users on the system increases, the performance degrades. Yet, the possible number of sequences, or users on the system, is infinite with chaotic sequences as compared to a set of orthogonal codes. This gives chaos a much better multi-user capability, when several users are required on the system.

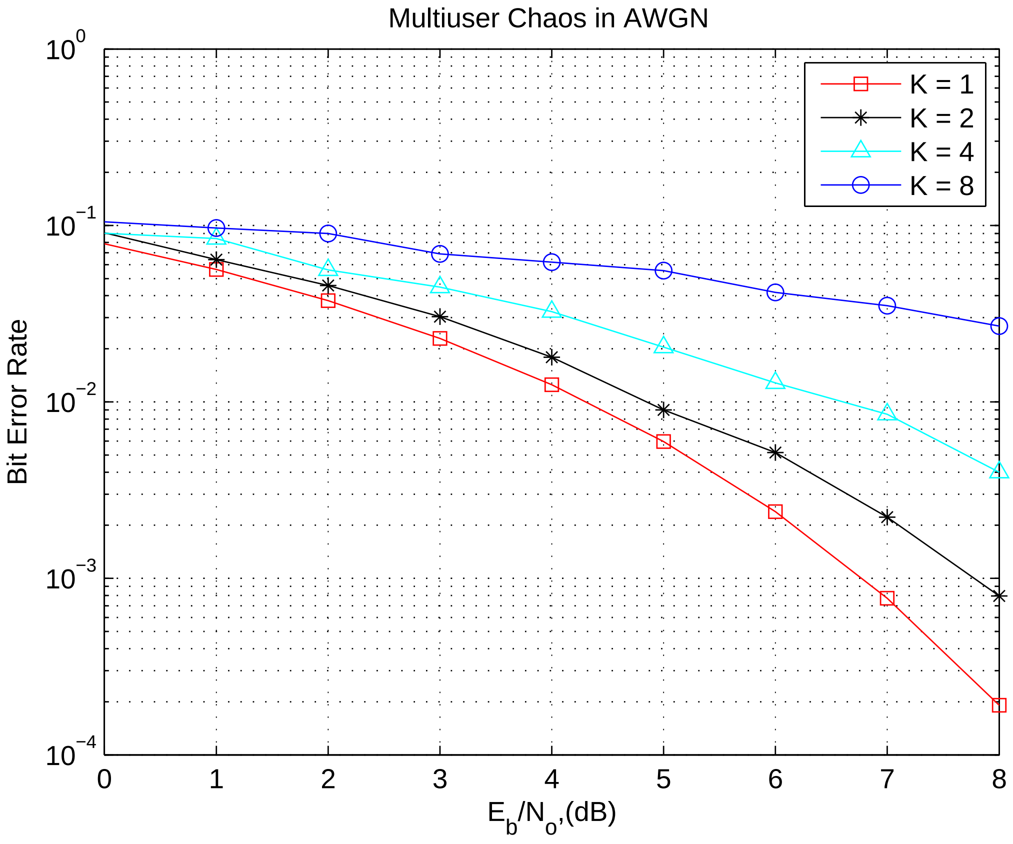

Figure 3.15: BER Performance of Multiuser Chaos in AWGN Channel

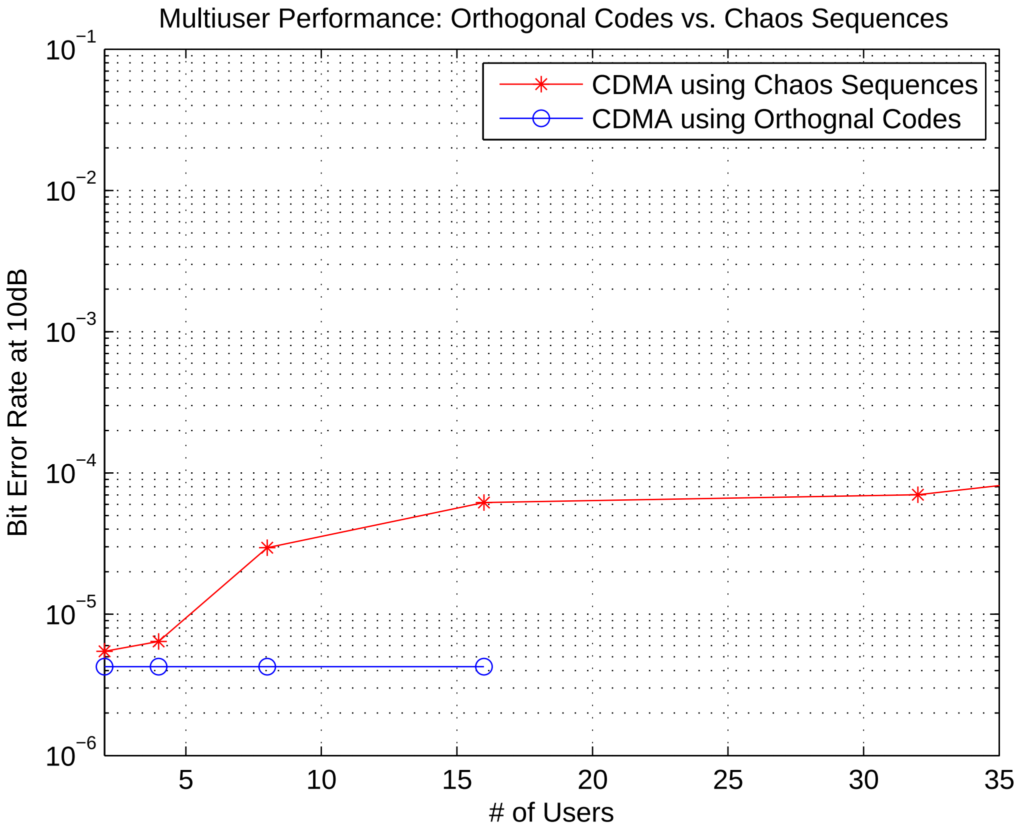

Figure 3.16: Orthogonal Codes vs. Chaotic Sequences using CDMA in AWGN

Polyphase Chaos

4.1 System Description

In this section, we extend our previous work to further enhance the security features of the system. Specifically, by implementing a polyphase carrier interferometry (CI) spreading code set along with chaos sequences, we create a chaos waveform that not only occupies non-contiguous bands but offers more noise like characteristics and lower probability of detection/interception. Simulations show that the proposed system maintains good BER performance under various channel conditions and multiuser scenarios. Furthermore, we demonstrate that the system is more secure and has a lower probability of interception compared with systems with binary chaotic sequences.

We have implemented a Non-Contiguous Polyphase system, in which the k^{th} user's transmission is given by

$$s_k(t) = b_k c_k(t) \tag{4.1}$$

where b_k is the k^{th} user's information symbol (±1), and $c_k(t)$ is the k^{th} user's NC binary chaotic spreading sequence, which is given by

$$c_k(t) = \sqrt{\frac{E_b}{N}} \sum_{i=1}^{N} \beta_k^i e^{j2\pi i \Delta f t} p(t) \tag{4.2}$$

where, N is the length of the chaotic spreading sequence; β_k^i is the i^{th} value of the k^{th}

user's binary chaotic spreading sequence given by (±1); $i\Delta f$ is the frequency position of the i^{th} carrier component usually given by $\Delta f = 1/T_s$, where T_s is the symbol duration to ensure carrier orthogonality; and p(t) is a rectangular waveform of unity height which time-limits the code to one symbol duration T_s.

While this non-contiguous chaotic system has low probability of interception due to the inherited security of the chaotic sequence (since the interceptor needs perfect information on the chaotic signal generator and its initial condition to intercept the signal), the generated chaotic signal has binary phase. To increase the security of the system by making the signal more noise like, we propose to employ a complex polyphase carrier interferometry(CI) spreading sequence instead of binary spreading sequence. By doing so, the newly generated chaotic signal is evenly distributed all over the phase space, making its probability of detection much lower.

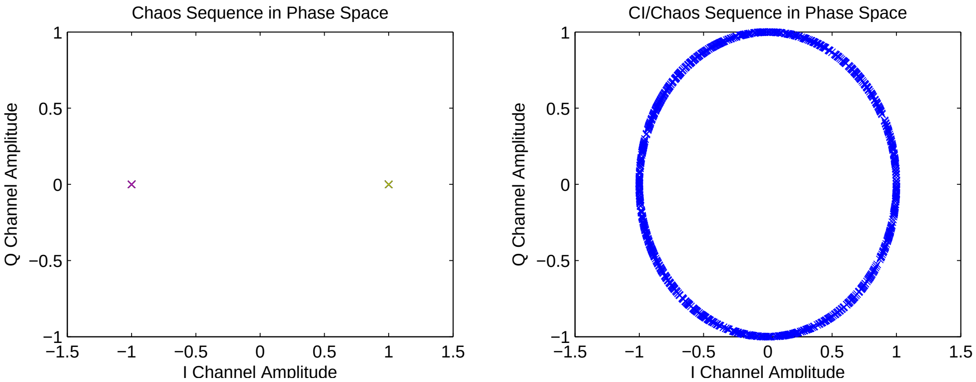

Figure 4.1: Phase Space of Chaos Sequences vs. Polyphase Chaos

This increased security is shown in Figure 4.1 by comparing the signal phase space of original chaotic waveform and that of the proposed polyphase CI chaotic waveform. The k^{th} user's spreading code corresponds to

$$\{\beta_1^{(k)}, \beta_2^{(k)}, .., \beta_N^{(k)}\} = \{e^{j\frac{2\pi}{N}.k.0}, e^{j\frac{2\pi}{N}.k.1}, .., e^{j\frac{2\pi}{N}.k.(N-1)}\} \tag{4.3}$$

Our final transmitted signal of the Polyphase Chaos is given by

$$S(t) = \sqrt{\frac{E_b}{N}} \sum_{k=1}^{K} b_k \sum_{i=1}^{N} c_k e^{j\frac{2\pi}{N}k.i} e^{j2\pi(f_o+f_i)t} p(t) \tag{4.4}$$

Figure 4.2 illustrates the proposed Polyphase Chaotic cognitive radio communication system. As shown in Figure 1, the binary data $b(t)$ is multiplied with the chaos waveform $c(t)$ and CI code $\beta(t)$ before modulation. At receiver side, a correlator receiver performs correlation of received signal $r(t)$ with the chaos waveform $c(t)$ and CI code $\beta(t)$. The uniqueness of this chaos cognitive radio communication system is the frequency domain based chaotic waveform generator.

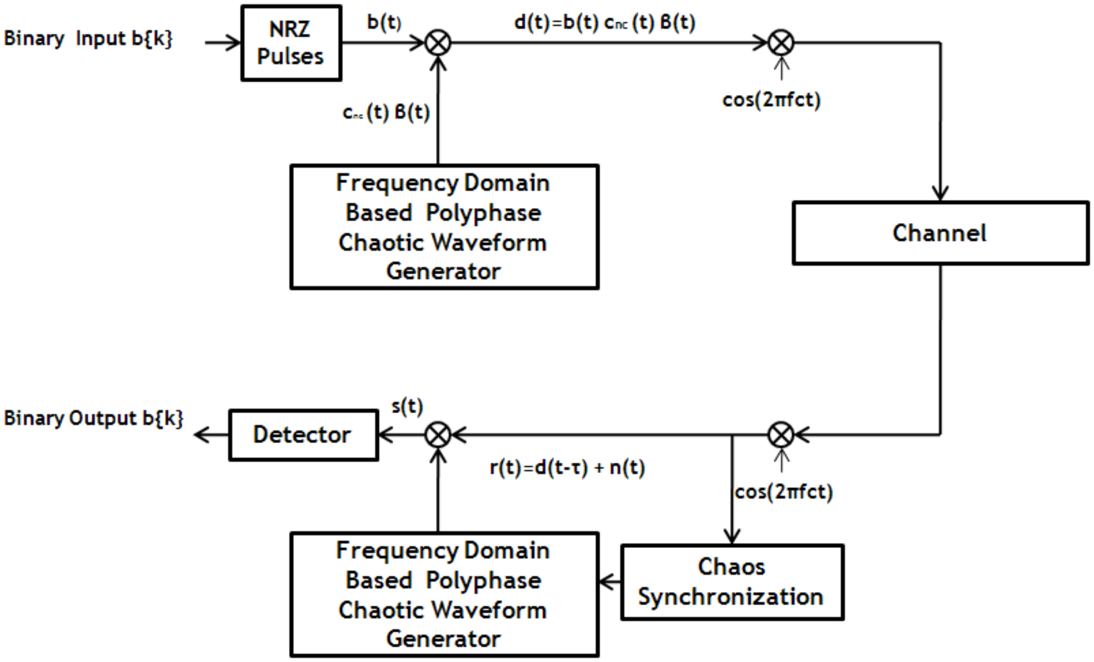

Figure 4.2: Frequency Domain Processing Based Polyphase Chaotic System

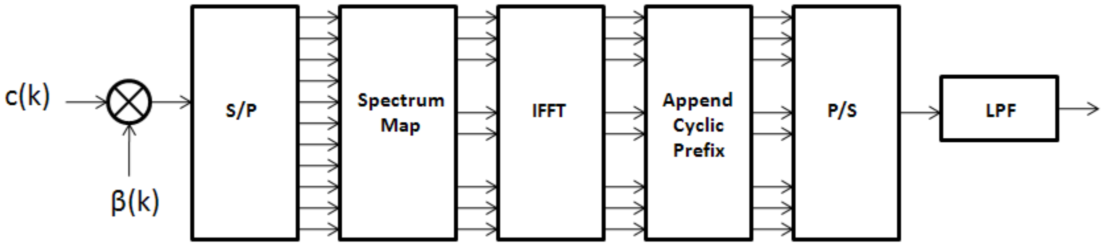

Figure 4.3: NC Polyphase Chaotic Waveform Generator

4.2 Correlation Analysis

As we stated earlier, one of the most important characteristics of PN sequences is its auto-correlation properties. At the receiver, the received signal is mixed with a locally generated PN sequence. This must result in maximum auto-correlation, or signal strength at the point of synchronization for the best decision to be made on the incoming signal. Another desired property in PN sequences is minimum cross-correlation. In a spread-spectrum system with multiple users, when the received signal is mixed with the locally generated PN sequence, it must result in minimum signal strength. This would ensure the receiver would be able to differentiate between the transmitted PN sequence and other PN sequences of other users.

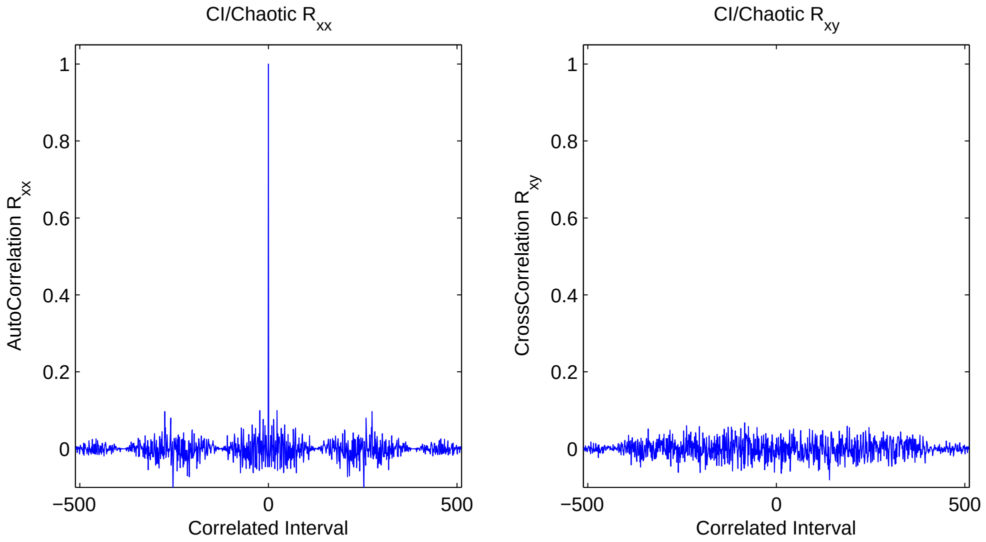

Figure 4.4: Correlation Properties of NC Polyphase Chaotic Sequence

Figure 4.4 shows the auto-correlation and cross-correlation of the NC-Polyphase Chaotic waveform. As shown, the Polyphase Chaotic waveform provides a auto-correlation close to an impulse and a cross-correlation close to zero. The cross-correlation shown is that of two separate chaotic sequences from one chaotic map using different initial conditions.

Figure 4.5 illustrates the auto-correlation and cross-correlation of the same Polyphase Chaotic Sequence after the spectrum mask has notched out certain subcarriers which are being used by primary users, as well as performing the inverse Fourier transform. It is evident from both Figures that the desired auto-correlation and cross correlation properties are maintained after the conversion from frequency domain back to time domain. It is evident from both Figures that the desired auto-correlation and cross-correlation properties of proposed frequency domain processing based Polyphase waveforms are maintained after the conversion from frequency domain back to time domain.

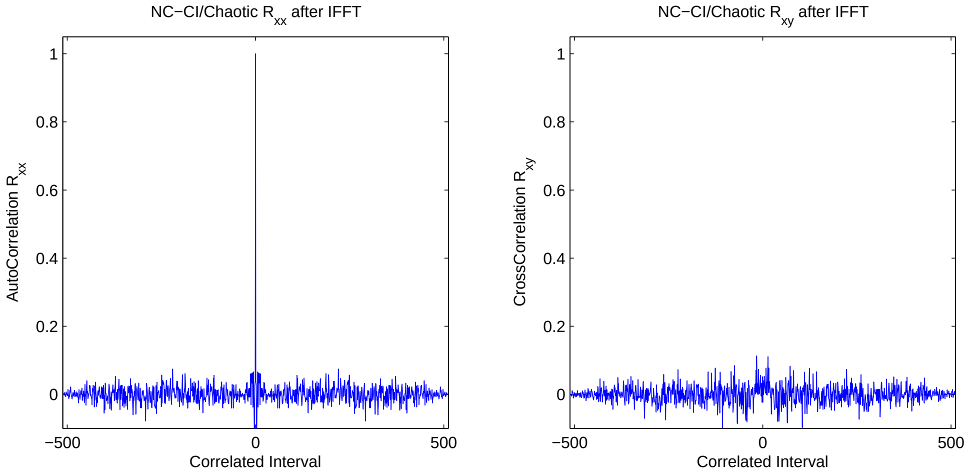

Figure 4.5: Correlation Properties of NC Polyphase Chaotic Waveform after IFFT

4.3 Bit Error Rate Performance

In this section we analyze the BER performance of the proposed non-contiguous chaotic communication system.

4.3.1 BER in AWGN Channel

The CI spreading code is simple a DFT matrix, which are orthogonal spreading codes, i.e.,

$$\Re\left[\frac{\int c_k(t)c_l(t)dt}{\int c_k(t)c_k(t)dt}\right] = \Re\left[\sum_{i=1}^{N} e^{j(\frac{2\pi}{N}k.i-(\frac{2\pi}{N}l.i)}\right] \tag{4.5}$$

$$\delta_{k,l} = \begin{cases} 1 \quad if \quad b = l \\ 0 \quad if \quad b \neq 1 \end{cases} \tag{4.6}$$

Since the non-contiguous Polyphase Chaotic waveform is naturally combined with an overlay cognitive radio, the secondary user employing the non-contiguous waveform does not cause interference to the primary users, nor experiences interference from the primary users. Hence, the BER performance of the proposed frequency domain based non-contiguous Polyphase Chaotic communication system stays the same as a contiguous Polyphase Chaotic communication system and both existing methods can be applied depending on the length of the chaotic sequence in the system. This result is confirmed by the simulation shown in Figure 4.6.

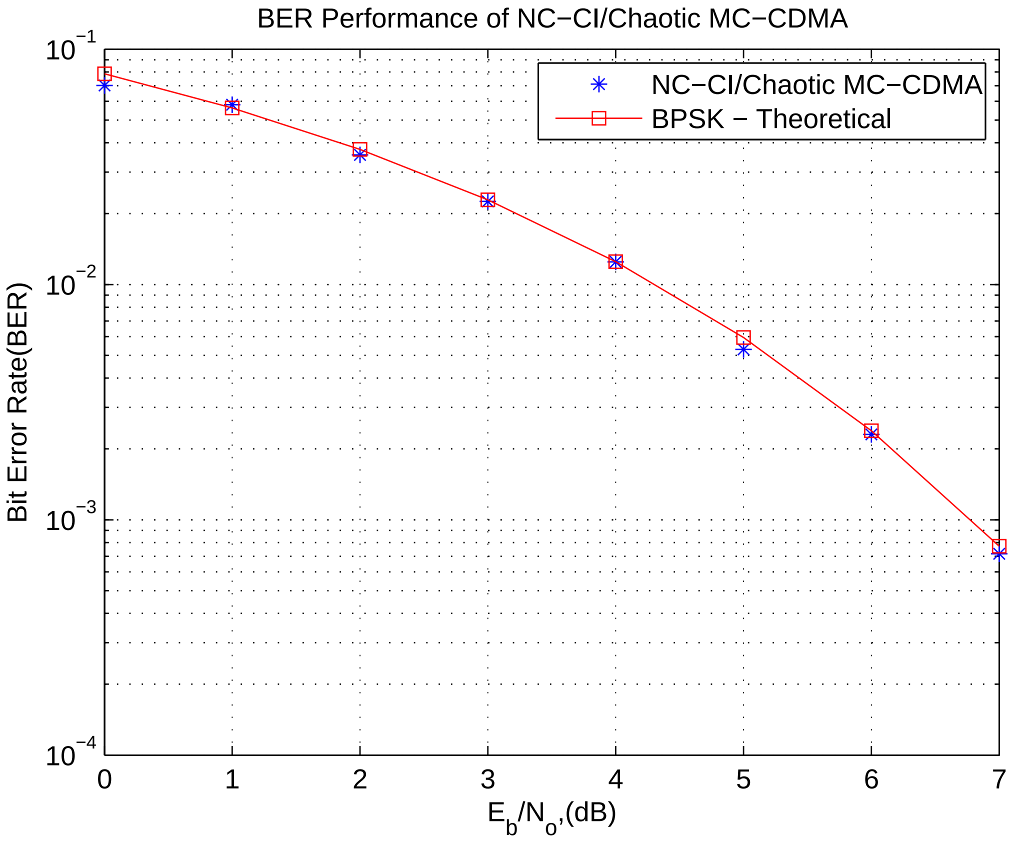

Figure 4.6: BER Performance of Single User Polyphase Chaos in AWGN Channel

4.3.2 BER in Multipath Fading Channel

Here we examine the BER performance of the proposed system in multipath fading channels. The chaos generator is a logistic map with a spreading sequence of length N = 32. A two-path rayleigh fading channel model is employed where the second path is uniformly distributed among $[0, T]$. The non-contiguous chaotic waveform is generated and a binary chaotic phase shift keying (CPSK) modulation is applied. At receiver side, a Maximum Ratio Combining (MRC) is employed to exploit frequency diversity across all the spectrum holes. The BER versus SNR curves are shown in Figure 4.7. It is evident that the proposed non-contiguous CI/Chaotic cognitive radio system is capable of exploiting frequency diversity in a multi-path fading channel and thus offering better BER performance.

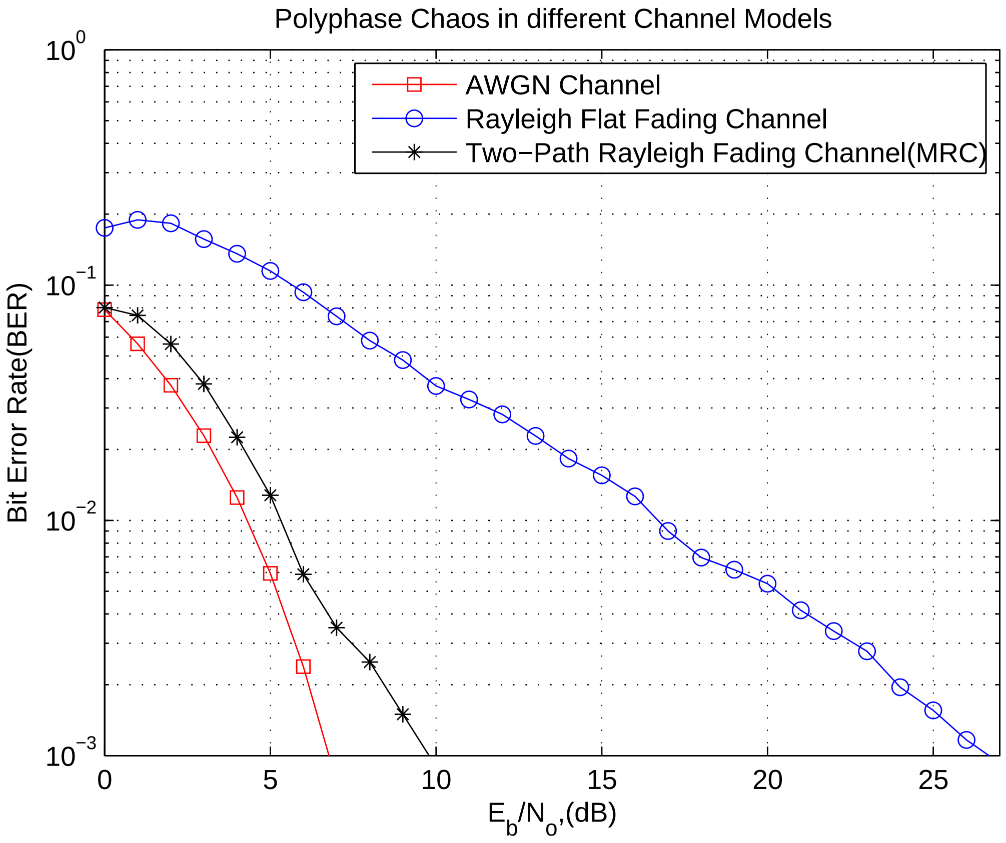

Figure 4.7: BER Performance of Normalized Chaos in different Channels

4.3.3 BER for Multiuser Scenario

For multiuser communication there are two separate the Polyphase Chaos sequences were implemented. In the first method, each user transmits on the same band at the same time but are distinguished by a different code sequence. By this we mean that each user is using a different chaotic sequence, generated by the Logistic Map, using different initial conditions, combined with the CI code from the DFT matrix, where each user's code is a row of the DFT matrix.Figure 4.8 shows the performance of this method Polyphase Chaotic in a multiuser scenario.

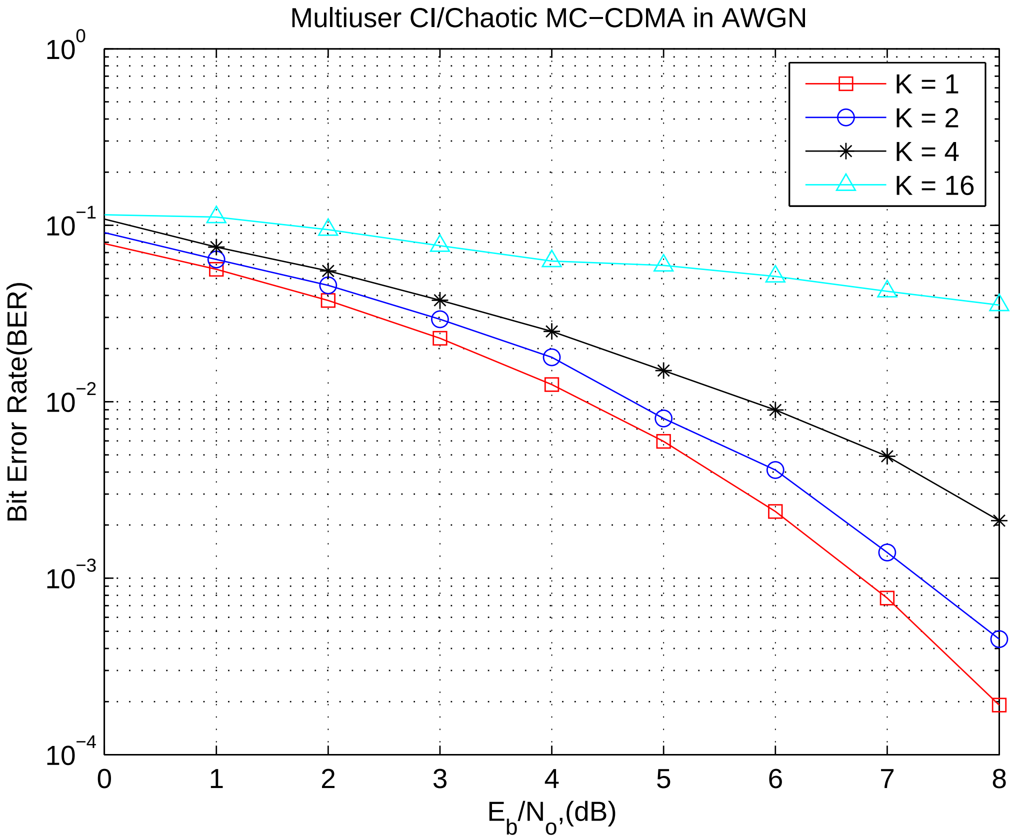

Figure 4.8: Method 1: Multiuser Polyphase Chaos in AWGN Channel

Figure 4.9 compares Polyphase Chaos method one, with regular Chaos spreading sequences for K = 2 and 4. We can see a slight improvement of about 0.5dB with the Polyphase Chaos. This is another added advantage from the previous section.

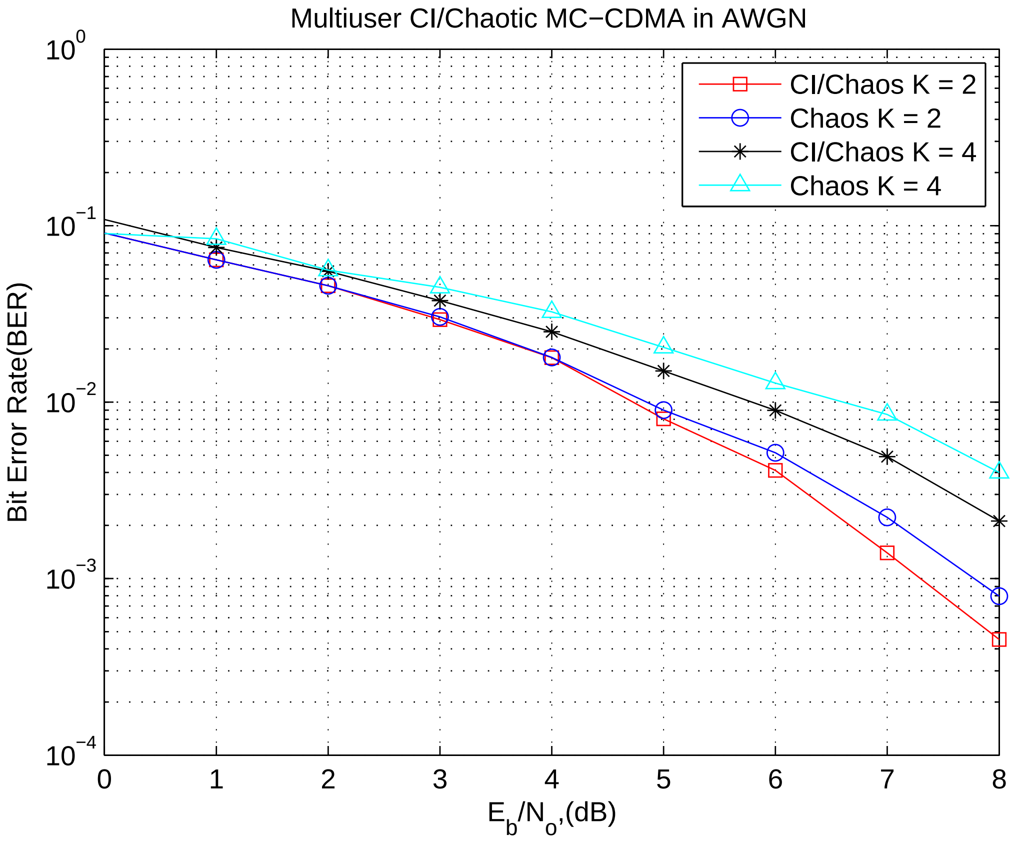

Figure 4.9: Multiuser BER Comparison of Polyphase Chaos vs. Chaos in AWGN

Another method that we implemented, uses the same chaotic sequence for each user on the system and a different CI code layered on top. Since CI codes are orthogonal, we can force this Polyphase Chaos code to be orthogonal as well. By doing this, we maintain the security features of method one, while dramatically improving the BER performance of the Polyphase Chaos system. Figure 4.10 shows the performance of the Polyphase Chaos using method two. We can see that the performance of the users does not change, because of the orthogonal nature of the Polyphase Chaos codes.

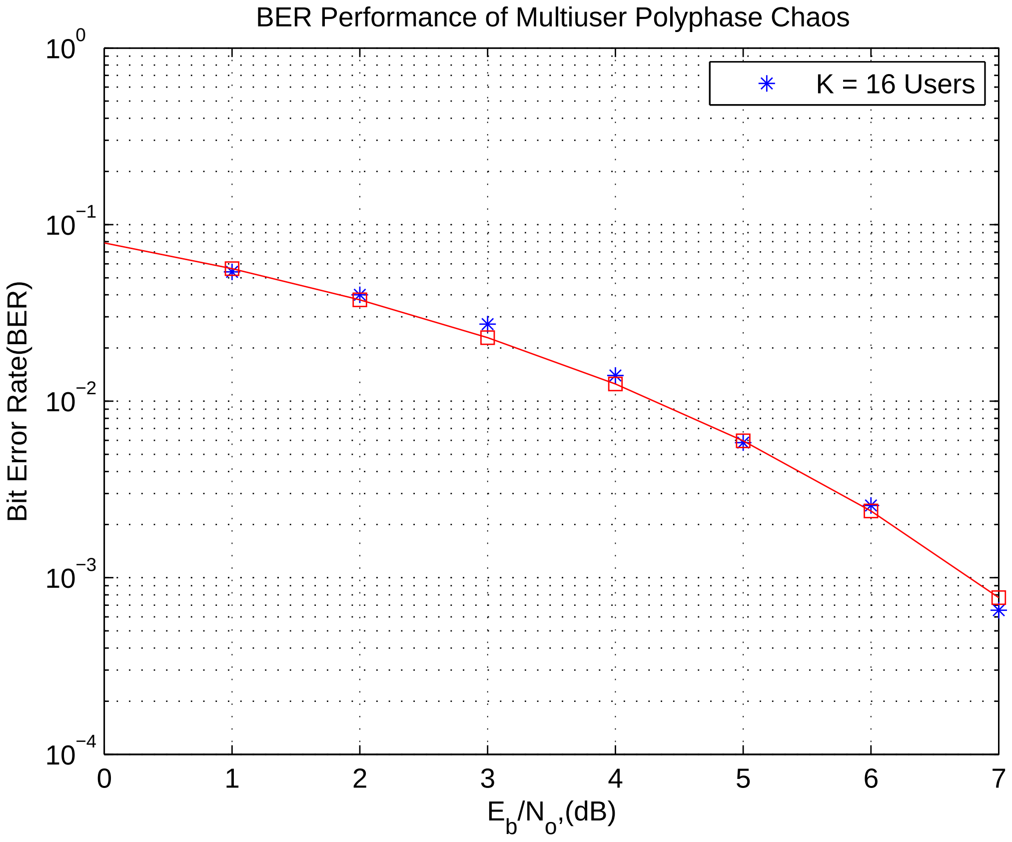

Figure 4.10: Method 2: Multiuser Polyphase Chaos in AWGN Channel

4.4 High Security Analysis

In our previous work, we mentioned the security advantages of using chaos spreading sequences. We can also now claim that adding a phase shift to the noise-like chaotic behavior, we can increase the security much further. We have done so using CI codes in this paper. We can show this increased security by trying to decode our signal using a set of Hadamard-Walsh codes.

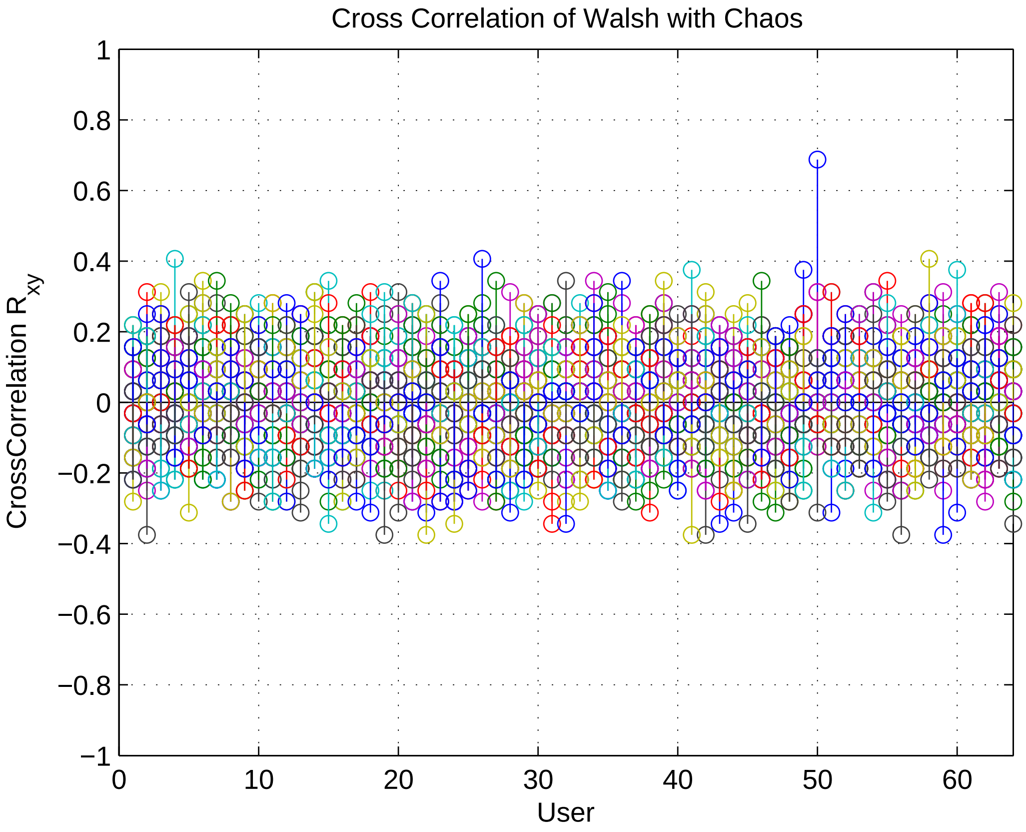

Figure 4.11: Cross Correlation of Walsh with Chaos

Using length N = 64 Hadamard-Walsh Codes, we found all the possible cross-correlations with a length N = 64 and K = 64 users on the system. We can see in Figure 4.11, that the cross-correlations of all the possibilities are below 0.4 except for one possible user with a high correlation of 0.7. Now, implementing the CI code along with the Chaotic sequence,

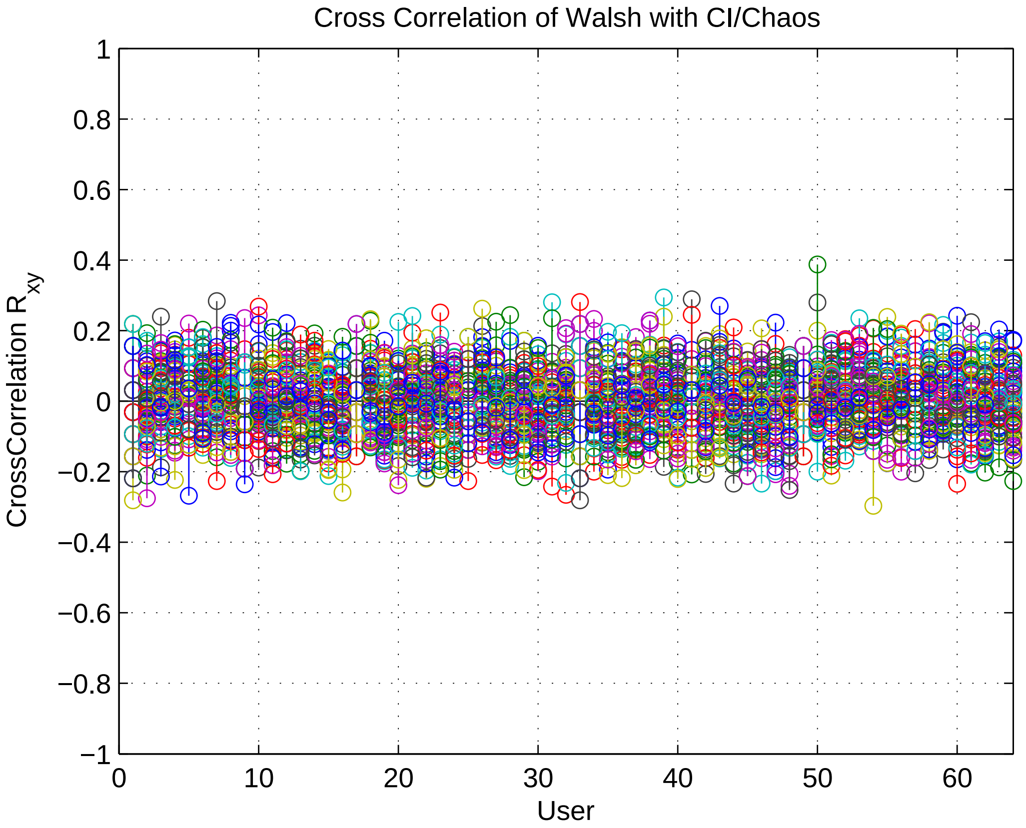

Figure 4.12: Cross Correlation of Walsh with Polyphase Chaos

as shown in Figure 4.12, we see that all the possible cross-correlations reduce to below 0.4. This increase in the security of the system and much harder for the enemy to decode the signal.

	$Mean$	Var	Max
Chaos	0.0020	1.0938	0.6875
CI/Chaos	0.0020	0.6847	0.3878

CONCLUSION

In this thesis, we combined the benefits of a chaos communication system with the benefits of cognitive radio technology to create a robust, highly secure, and flexible chaotic cognitive radio system. We first begin with a short survey of chaotic communication and cognitive radio technology. Then we compare chaotic waveforms to other conventional PN sequences and show its superiority in security and multiuser capabilities. We then propose a novel frequency domain based chaos communication system that is capable of operating over multiple non-contiguous frequency bands. Furthermore, we analyze the performance of this system in different channel models and in multiuser scenarios. Finally, we implement carrier-interferometry sequences along with the chaos sequence to increase the security and performance of the system. Simulation results over various channel conditions confirm the effectiveness of the proposed system.

Bibliography

[1] P. Stavroulakis, *Chaos Applications in Telecommunications.* CRC Press, 2006.

[2] Anjam Riaz, Maaruf Ali, ed., *Chaotic Communications, their Applications and Advantages over Traditional Methods of Communication*, 2008.

[3] A.S. Dmitreiv, M. Hasler, A.I. Panas, K.V. Zakharchenko, "Basic principles of direct chaotic communications," *Nonlinear Phenomena in Complex Systems*, vol. 1, p. 14, 2002.

[4] A. Abel and W. Schwarz, "Chaos communications - principles, schemes, and system analysis," *Proceedings of IEEE Trans. Circuits Syst. I*, vol. 90, no. 5, pp. 691–710, May 2002.

[5] F.C.M. Lau, C.K. Tse, *Chaos-Based Digital Communication Systems.* Springer-Verlag, 2003.

[6] V. Chakarvarthy, X. Li, Z. Wu, F. Garber and M. Temple, "Novel overlay/underlay cognitive radio waveforms using sd-smse framework to enhance spectrum efficiency - part i," *IEEE Transactions on Communications*, vol. 57, December 2009.

[7] S. Hijazi, B. Natarajan, M. Michelini, Zhiqiang Wu, C.R. Nassar, "Flexible spectrum use and better coexistence at the physical layer of future wireless systems via a multicarrier platform," *IEEE Wireless Communications*, vol. 11, pp. 64–71, April 2004.

[8] Joseph Mitola III, *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*. Ph.d. dissertation, Royal Institute of Technology (KTH), Sweeden, 2000.

[9] F.C.M. Lau, C.K. Tse, M. Ye and S.F. Hau, "Coexistence of chaos-based and conventional digital communication systems of equal bit rate," *IEEE Trans. Circuits Syst. I*, vol. 51, pp. 391–408, Feb 2004.

[10] Lei LiHua, Shi Huli, Ma GuanYi, "Caps sattellite spread spectrum communication blind multi-user detecting system based on chaotic sequences," *Physics, Mechanice & Astronomy*, vol. 52, pp. 339–345, Mar 2009.

[11] Gobindar S. Sandhu and Stevan Berber, "Theoretical model, simulation results and performances of a secure chaos-based multi-user communication system," *International Journal of Network Security*, vol. 8, pp. 25–30, Jan 2009.

[12] C. M. G. Heidari, "Chaotic sequences for spread spectrum: An alternatice to pn-sequences," *Proc. IEEE ICWC-92*, p. 437440, 1992.

[13] Y. J.Tou, P and H. Leung, "Spread-spectrum signals," *Circuits Systems and Signal Processing*, vol. 18, pp. 59–73, 1999.

[14] A. E. M.I. Youssef, M.Zahara and M. A. ElGhany, "Chaotic sequences implementation on residue number spread spectrum systems," *International Journal of Communications*, vol. 2, pp. 143–154, 2008.

[15] O. P. M. Mike B. Reynen, Ahmed H. Osman, "Using gold sequences to improve the performance of correlation based islanding detection," *Electric Power Systems Research*, p. 6, 2009.

[16] D. R. P. C. Georges Kaddoum, Martial Coulon, “Performance of multi-user asynchronous chaos-based communication system through m-distributed fading channel,” in *17th European Signal Processing Conference*, 2009.

[17] S. K. P. Ipsita Bhanja, “Performance comparison of various spreading codes in spread spectrum modulation,” *Proceedings of National Conference on Rage Technology*, pp. 30–35, 2006.

[18] H. Z. J. Y. Lin Wang, Mu Wei, “Performance comparison between q-cdma and chaotic spreading spectrum cdma communication system over saleh indoor channel,”

[19] Yuu-Seng and Zahir M. Hussain, “A new approach in chaos shift keying for secure communication,” in *Third International Conference on Information Technology and Applications*, 2005.

[20] Wai M. Tamm, Francis C.M. Lau, Chi K. Tse, Anthony Lawrence, “Exact analytical bit error rates for multiple access chaos-based communication systems,” *IEEE Transcations on Circuits and Systems*, vol. 51, pp. 473–481, September 2004.