DOKUZ EYLÜL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

CHAOTIC MODULATION AND ALPHA-STABLE NOISE PARAMETER MODULATION METHODS IN SPREAD SPECTRUM COMMUNICATION

by

Mehmet Emre ÇEK

August, 2010

İZMİR

CHAOTIC MODULATION AND ALPHA-STABLE NOISE PARAMETER MODULATION METHODS IN SPREAD SPECTRUM COMMUNICATION

A Thesis Submitted to the

Graduate School of Natural and Applied Sciences of Dokuz Eylül University

In partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in

Electrical and Electronics Engineering

by

Mehmet Emre ÇEK

August, 2010

İZMİR

Ph.D. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"CHAOTIC MODULATION AND ALPHA-STABLE NOISE PARAMETER MODULATION METHODS IN SPREAD SPECTRUM COMMUNICATION"** completed by **MEHMET EMRE ÇEK** under supervision of **PROF. DR. FERIT ACAR SAVACI** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.

Prof. Dr. Ferit Acar SAVACI

Supervisor

Prof. Dr. Cüneyt GÜZELİŞ

Thesis Committee Member

Prof. Dr. Saide SARIGÜL

Thesis Committee Member

Assoc. Prof. Dr. Müştak E. YALÇIN

Examining Committee Member

Assist. Prof. Dr. Olcay AKAY

Examining Committee Member

Prof.Dr. Mustafa SABUNCU
Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGMENTS

First of all, I would like to express my sincere gratitude to Prof. Dr. F. Acar SAVACI for his supervision and contributions to my academic background during the completion of my master and doctoral thesis.

I am very grateful to my thesis committee members Prof. Dr. Cüneyt GÜZELİŞ and Prof. Dr. Saide SARIGÜL for their assistance and guidance through my thesis.

I also would like to thank to Dr. Erdal ÖZBEK for his time and help in documentation.

I would like to thank Assist. Prof. Dr. Yalçın İŞLER, Dr. Savaş ŞAHİN, Dr. M. Alper SELVER, Mehmet ÖLMEZ, Aykut KOCAOĞLU and my other colleagues for their encouragement, motivation and support at the rough times.

My special thanks to Ömer KARAL for his helps in the preparation of the final format of this thesis before the deadline.

My sincere thanks to my parents for their everlasting patience, understanding and encouragement.

M. Emre ÇEK

CHAOTIC MODULATION AND ALPHA-STABLE NOISE PARAMETER MODULATION METHODS IN SPREAD SPECTRUM COMMUNICATION

ABSTRACT

With the inspiration from the chaotic communication systems, in which noise like signals, chaotic signals, have been used as carrier signals due to their broad-band frequency spectrum, which have been widely studied in the last twenty years as an alternative to the conventional spread spectrum techniques by the discovery of the synchronization of chaotic dynamical systems. In this thesis, new random communication systems in which noise itself is used as a random carrier instead of using chaotic carrier have been introduced.

Motivation at the beginning stage of this thesis was to develop more secure chaotic communication systems since the security in the existing chaotic communication systems could have been easily broken. With this motivation, at the second chapter of the thesis, after introducing the main ideas of the existing chaotic communication systems, new secure chaotic communication system operating at high frequencies for wireless communication have been introduced.

At the third chapter of the thesis, after introducing the particle filters which was developed to estimate the states of the nonlinear dynamical systems in non-Gaussian environments, by the newly proposed communication schemes, secure recovering of the message signal has been aimed by masking the message carrying chaotic signal with impulsive noise and transmitting it through the Gaussian noise channel and estimating the chaotic signal by using particle filter while achieving synchronization of the receiver with the transmitter.

At the fourth chapter, in the newly proposed random communication schemes, random signals with alpha stable distributions produced in the transmitter part are sent to the receiver through the Gaussian noise channel as random carriers of binary coded message signal. At the receiver part, random carriers mixed with the Gaussian noise are estimated by least squares, correntropy and fractional order moments methods and hence the binary message signal may be recovered. With these newly proposed unique secure random communication schemes of which satisfactory bit error performances have been obtained, triggering of further studies in random communication field is expected.

Keywords: Random Communication, Random Carrier, Alpha Stable Distributions, Detection of Alpha Stable Distributed Signals, Chaotic Communication, Chaotic Carrier, Chaotic Synchronization, Spread-Spectrum Communication, Particle Filters.

GENİŞ BANDLI HABERLEŞMEDE KAOTİK MODÜLASYON VE ALFA-KARARLI GÜRÜLTÜ PARAMERE MODÜLASYONU YÖNTEMLERİ

ÖZ

Bu tezde, geleneksel geniş bandlı haberleşme tekniklerine alternatif olarak, son yirmi yılda kaotik dinamik sistemlerin senkronize edilebilmesiyle birlikte geliştirilen ve gürültü benzeri geniş spektruma sahip kaotik işaretleri taşıyıcı işaret olarak kullanan kaotik haberleşme sistemlerinden esinlenerek, gürültü benzeri kaotik taşıyıcı işaret kullanmak yerine, gürültünün kendisini taşıyıcı işaret olarak kullanan rassal haberleşme sistemleri sunulmuştur.

Bu tezin başlangıç aşamasındaki itilgücü, literatürde var olan kaotik haberleşme sistemlerindeki gizliliğin kırılabilir olmasından dolayı, yüksek frekanslarda çalışabilecek daha güvenli yeni kaotik haberleşme sistemlerini geliştirmek olmuştur. Bu itilgüç ile tezin ikinci bölümünde, literatürdeki kaotik haberleşme sistemleri ana hatları ile sunulduktan sonra, kablosuz haberleşme sistemlerinde kullanılabilecek, kaotik taşıyıcı işareti istenen yüksek frekanslara taşıyan, yeni bir kaotik haberleşme sistemi sunulmuştur.

Üçüncü bölümde ise Gauss olmayan dağılımlara sahip gürültülü ortamlarda doğrusal olmayan dinamik sistemlerin durumlarının kestirilmesi için geliştirilmiş olan parçacık süzgeçleri sunulduktan sonra, yeni önerilen kaotik haberleşme sistemi ile dürtüsel dağılımla maskelenmiş kaotik işaretin Gauss gürültülü kanal boyunca iletildikten sonra alıcı tarafında parçacık süzgeci ile kestirilip alıcı tarafındaki kaotik dinamik sistemin verici tarafındaki kaotik dinamik sistemle senkronize edilmesiyle, ileti işaretinin güvenli bir şekilde tekrardan oluşturulması amaçlanmıştır.

Tezin dördüncü bölümünde literatüre yeni olarak önerilen rassal haberleşme sistemlerinde, iletici kısmında üretilen alfa kararlı dağılıma sahip rassal işaretler, taşıyıcı işaret olarak, ikili kodlanmış ileti işaretini Gauss gürültüsüne sahip kanal boyunca alıcıya iletmektedirler. Alıcı kısmına Gauss gürültüsüyle karışmış olarak ulaşan rassal işaretler, alıcı kısmında önerilen en küçük kareler, özilinti, kesirli düşük mertebeden moment yöntemlerine dayanarak kestirildikten sonra ikili kodlanmış ileti alıcıda tekrardan oluşturulabilmiştir. Tatmin edici bit hata başarımları hesaplanan, bu önerilen ilk rassal haberleşme sistemleri ile, güvenli haberleşme açısından literatürde var olan yöntemler üzerinde güvenilirlik açısından üstünlük sağlanmakta olup, rassal haberleşme alanında daha ileri çalışmaların tetiklenmesi beklenmektedir.

Anahtar Sözcükler: Rassal Haberleşme, Rassal Taşıyıcı, Alfa Kararlı Dağılımlar, Alfa Kararlı İşaretlerin Kestirimi, Kaotik Haberleşme, Kaotik Taşıyıcı, Kaotik Senkronizasyon, Geniş Bandlı Haberleşme, Parçacık Süzgeçleri

CONTENTS

Page

CHAPTER ONE

INTRODUCTION

Developing spectrum spreading techniques have growing interest in signal processing for secure communication. Necessity of spreading the spectrum arose from other reasons such as antijamming and antiinterference, reducing the probability of intercept, performing multiple user access, high resolution ranging and accurate universal timing (Haykin, 1994).

Due to the security requirement in cable or wireless communication, it has been essential to develop several signal processing techniques in last decades. The main purpose is to convert the narrow-band information carrying signal into wide-band through the frequency spectrum. In other words, the communication systems based on frequency spreading has been called as spread-spectrum communication in (Haykin, 1994).

A communication system can be considered as spread-spectrum system if the following conditions are satisfied (Pickholtz et. al.,1982).

- The bandwidth of the transmitted signal must be much greater than the bandwidth of the message signal.
- Second, the transmitted message bandwidth must be achieved by a function which is known by the receiver and it is independent from the message signal.

This function composed by a specified code which converts the narrow-band signal into a wide-band signal is called *spreading code*. Hence, the conventional modulation techniques such as FM and PCM can not be addressed as spread-spectrum although these techniques also spread the spectrum of the information signal, since the second requirement is not satisfied.

1.1 Conventional Spread-Spectrum Techniques

The spread-spectrum systems can be classified in accordance to the modulation types which are direct sequence (Pickholtz et. al.,1982), frequency hopping (Haykin, 1994), time hopping (Win & Scholtz, 2000), chirp (Kowatsch & Lafferl, 1983), and hybrid modulation (Geranoitis, 1985,1986). Among these modulation methods, most frequently used ones are the direct sequence and frequency hopped spread spectrum systems which are explained in the following sections.

1.1.1 Direct-Sequence Spread-Spectrum

In this spread spectrum technique, binary data sequence is modulated by a wide-band code which is called as pseudo-noise (PN) sequence. Figure 1.1 illustrates the block diagram for the direct sequence spread-spectrum binary phase shift keying (BPSK) system. Since the binary message is encoded by generated noise-like sequence directly, the method is called as direct sequence spread-spectrum (DSSS) technique which spreads the frequency content of the message signal.

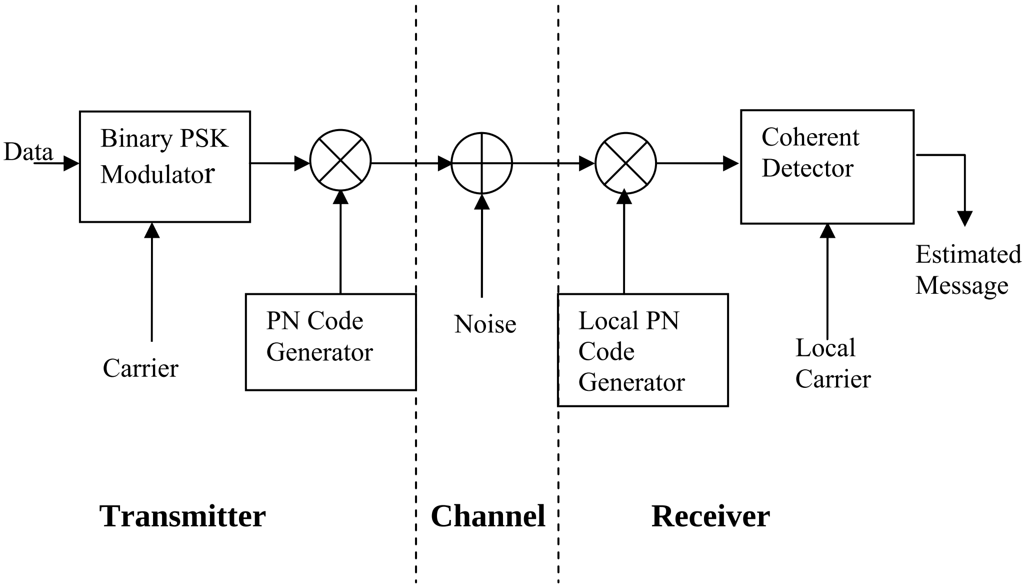

Figure 1.1 Block diagram of the direct sequence spread-binary PSK system.

The resulting wide-band code is modulated by phase shift keying (PSK) as the second stage. The length of the code is determined by the number of feedback shift registers used to generate the PN sequence. When the used memory units increases, then the period of the generated code is also increased. The modulated data with increased period exhibits a noise-like behaviour.

1.1.2 Frequency Hopped Spread Spectrum

The type of spread spectrum in which the carrier hops randomly from one frequency to another is called *frequency-hop spread spectrum*, (Haykin, 1994). M-ary frequency shift keying (MFSK) is the common modulation format for frequency hop systems. The combination of these two techniques is called as FH/MFSK. The block diagram of communication scheme is shown in Figure 1.2. The frequency hopping can be characterized by two sub-classes depending on the rate at which the hops occur. The first one is called as *slow-frequency hopping* in which the symbol rate MFSK signal is an integer multiple of the hop rate. The second method is called as *fast-frequency hopping* in which the hop rate is an integer multiple of the MFSK symbol rate. While several symbols are transmitted on each frequency loop in slow-frequency hopping, the carrier frequency hops several times during the transmission of one symbol.

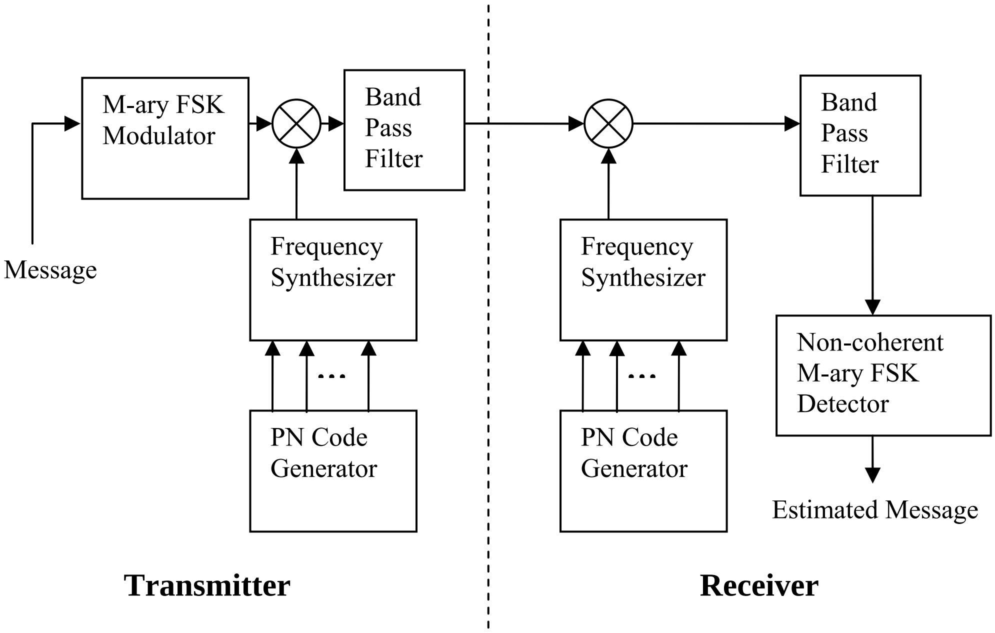

Figure 1.2 Block diagram of the frequency hop M-ary frequency-shift keying.

As described above, the direct-sequence spread spectrum and frequency hopped spread spectrum techniques are both rely on noise-like spreading code called as pseudo-noise (PN) sequence. Although the spread-spectrum systems provide certain advantages such as difficulty of detection, noise performance, short acquisition time and discrimination performance against multipath fading, there are some disadvantages with bandwidth efficiency, sensitivity to the phase distortions, fast code generator and error correction requirements which caused to search alternative methods. Signals exhibiting noise-like behaviour have been considered as possible candidates for spread-spectrum communication. The following subsection involves studies in the literature for chaotic communication as an alternative to the conventional spread-spectrum communication systems.

1.2 Survey on Chaotic Communication Techniques

The chaotic signals have been considered as a candidate tool for the first time for generating noise-like signal in spread-spectrum communication in the middle of 80s (Dmitriev & Kislov, 1985). But it could be possible to use chaotic signals in secure communication after the chaotic synchronization was realized by (Pecora & Caroll, 1990, 1991). The baseband chaotic communication schemes were performed depending on masking or modulating the parameter of the chaotic system (Chua et. al., 1992), (Cuomo & Oppenheim, 1993), (Kolumban et. al., 1998), (Morgül, 2000). A study on the design of non-coherent receiver for chaotic masking scheme was described by (Murali et. al., 2003). The chaotic masking has also been subject of the chaotic communication including observer based synchronization given by (Morgül et. al, 2003), (Li Demin et. al., 2007), (Chen & Min, 2008). Differing from chaotic masking, in another study given by (Savacı et. al., 2003), the periodic message signal has been applied as an input to chaotic dynamical system and the message signal was recovered at the receiver using synchronization. The constraints associated with this method was noted as the frequency of the message signal should not be so close to the fundamental frequency of the chaotic signal and the magnitude of the input signal should be bounded in order to maintain the chaos. In a recent study, the cascaded chaotic systems have been used involving cascaded synchronization (Li C. & Yan, 2006).

In addition to the chaotic masking, different chaotic modulation schemes which are called as chaos-shift keying (CSK) and differential chaos-shift keying (DCSK) was described in (Kolumban et. al., 1998). The types of chaos shift keying can be found in (Lau & Tse, 2003). The chaotic synchronization between linearly coupled systems was involved in (Lü et. al., 2002), (Li Damei, 2005). An application of secure communication scheme which uses generalized synchronization was studied in (Min & Zhang, 2005). In (Li Guo-Hui, 2005), the parameters of the chaotic system were also chosen from another chaotic system and more complex drive-response structure was obtained to improve the security. The improvement of the security has been performed in another study by (Alvarez et. al., 2005a) using a chaotic encryption including ciphertext absolute value. Chaotic secure communication scheme based on impulsive synchronization and impulsive control have been described in (Yang & Chua, 1997), (Xie et. al., 2000), (Yang, 2001), (Yang, 2004) which defines the required conditions for stability of impulsively controlled chaotic systems.

Due to the channel characteristics, the performance is limited of the CSK and DCSK communication systems which have been pointed out by (Kolumban et. al., 2002). Instead of transmitting chaotic signals directly, it is desirable to use constant-envelope signals exhibiting chaotic behavior. One of these methods known as frequency modulated-differential chaos shift keying (FM-DCSK) can be found in (Kennedy et. al., 2000, ch 6). The theory and simulations associated with chaos based FM signals is given by (Callegari et. al., 2003a) and hardware implementation is included in (Callegari et. al., 2003b). The types of other chaotic signal generation and transceiver design techniques have been explained in (Stavroulakis, 2006), comprehensively. As another hardware implementation, architecture of a chaotic PN sequence generator was proposed by (Leon et. al., 2004).

The fundamentals of studying chaos with probability densities were given in (Kennedy et. al., 2000). The statistical approach to the discrete-time nonlinear dynamical systems has been used to characterize the chaotic sources by Perron-Frobenius Operator (PFO) which gives the temporal evolution of the probability densities, used to increase the channel capacity in chaos based DS-CDMA systems (Setti et. al., 2002). The PFO operator in chaotic communication is also applied to increase the security (Abel & Schwarz, 2002).

In addition to the methods given above, spreading the message spectrum was performed by chaotic frequency modulation in some studies (Larger et. al., 2001), (Volkovskii et. al.,1999, 2005) and chaotic pulse-position modulation (Sushchik, et. al., 2000), (Rulkov et. al., 2001) (Fortuna et. al., 2003) which is noted to provide better noise robustness. In (Okamoto & Iwanami, 2006), trellis coded chaotic modulation has been proposed as a secure digital communication scheme which is noted as offering a limited bit error rate performance. The method of multiplying directly the message and the chaotic signal in time domain applied in (Dmitriev et. al., 2004) was called as amplitude modulation of the chaotic carriers where it is assumed that there is no overlap between the frequencies of the message signal and the chaotic carrier. Recently, in a similar study, the message signal is multiplied by the chaotic carrier where the extended Kalman filter (EKF) is designed for synchronization at the receiver part (Fallahi & Leung, 2010).

Differing from the given method in (Dmitriev et. al., 2004), the main contribution of the proposed study is to successfully recover the message signal by properly tuning the frequency of the message signal combining the amplitude modulation using a sinusoidal carrier and the method given in (Savacı et. al., 2003). The aim of the proposed method is to model a chaotic communication scheme which carries the baseband chaotic signal through the high frequencies around the sinusoidal carrier.

More generally, the types of carrier signals are classified as constant, chaotic and random in spread-spectrum communication methods (Kolumban et. al., 2005). In an earlier study (Minai & Pandian, 1998), combining noise and chaotic signal is considered where the noise has been applied as an input to the chaotic system to generate an encryption model. As a transition from chaotic carrier to random carrier, the alternative methods for generating random numbers from specified explicit functions (Gonzales et. al., 2002) and from standard chaotic maps (Patidar & Sud,

2009) can be used as candidate random carriers. In (Yalçın M. E., 2007) the entropy of the generated random numbers has been increased using n-scroll chaotic attractors to obtain random sequence from deterministic system which can be a proper selection for random secure communication. Instead of modeling random systems using deterministic structures a random signal having α-stable distribution has been considered as a random carrier and used in secure communication (Cek & Savacı, 2009).

On the other hand, there are several studies which breaks the chaotic masking and chaos shift keying using spectrogram (Yang et. al., 1998), generalized synchronization (Tao & Du, 2003) and (Alvarez G. et.al., 2004, 2005b), multiscale wavelets (Fernandez et. al., 2003). Another practical method known as empirical mode decomposition has been the subject of the studies given in (Huang et. al.,1998), (Peng et. al., 2005) that uses mean of the envelopes of the observed signal to decompose into components. Separation of chaotic signals from harmonic signals using empirical mode decomposition has been applied in (Li Guo-Hui, 2006) which is a proper example for chaotic masking. It was shown that the additive periodic signals can be easily distinguished from the chaotic signal. The security of the chaotic masking systems for high dimensional chaotic systems has been discussed in (Alvarez G. et. al., 2005c). To improve the security performance of the chaotic communication the following studies have been proposed.

In (Bu & Wang, 2004), a modulating technique was explained to avoid the attack using phase space reconstruction. In (Li Shujun et. al., 2001), the chaotic encryption method in (Alvarez E. et. al., 1999) is improved with adding an additional encryption block. Since the one dimensional chaotic maps are weak for security, the combination of one dimensional chaotic map has been used to increase the security in (Pareek et. al., 2005).

Although the chaotic signals are said to have broad-band spectrum, it is noted that the power is concentrated mostly on low frequencies (Rasband, 1990) that restricts the security performance of the chaotic communication systems. Even though there was an interest for chaotic communication without synchronization (Kis et. al., 1998), the synchronization of chaotic systems still plays a key role. In such a communication channel including also interference and fading, the maintaining synchronization becomes hard therefore low bit error rate performance is obtained. The findings associated with performance of the chaotic systems in digital communication have been proposed by (Xia et. al., 2004), (Luca et. al., 2005), (Sanhu & Berber, 2005). Ultra-wide-band (UWB) communication scheme using microwave chaotic oscillator has been developed by (Dmitriev, 2006).

1.3 Particle Filtering of The Chaotic Signals in Alpha-Stable Noise Environment

The observed time series from the given states of a dynamical system include noisy measurements in many signal processing applications. The filtering techniques for tracking the states can be classified as optimal filters such as linear Kalman filter and grid-based filters and suboptimal filters including extended Kalman Filter, approximate grid-based filters and particle filters (Arulampalam et. al., 2002).
In chaotic communication, state estimation by using extended Kalman filter has been given in the studies in (Cuomo et. al., 1993), (Sobiski & Thorp, 1998), (Ruan et. al., 2003). The extended Kalman filter has been recently applied by (Hugues & Salas, 2010) to nonlinear time delay systems in observer based chaotic communication system. Nevertheless, extended Kalman filter is not a valid method for the tracking problem in non-Gaussian environments. Therefore, a relatively new tool called particle filters have become significant for estimation problems having especially non-linear system model and non-Gaussian interference.

Particle filters have been used in tracking and navigation problems (Gustafsson et. al., 2002). Particle filters in communication have been applied in (Punskaya et. al., 2001) as demodulator for fading channels where the noise model is assumed as Gaussian mixture which is non-Gaussian. In another study by (Bertozzi et. al., 2004), the particle filter provides tracking of delay time for each path in the frequency selective channels and the bit error rate performance of the spread-spectrum communication system has been improved. The idea of using particle filters for chaotic secure communication has been given in (Zhang et. al., 2006) although they use Gaussian noise as jammer and there is no proposed channel model. The estimation of chaotic states using particle filters without a communication purpose has also been studied in a different study (Zhang et. al., 2007). In (Liu B. et. al., 2008), both the particle filter and Kalman filter have been used to construct a mechanism for filtering the noisy measurements.

Since α-stable distributed noise is a proper member of non-Gaussian noise family, studying particle filters in α-stable noise environment has become a challenging area in signal processing. Tracking the measurements of the autoregressive processes in symmetric α-stable (SαS) noise has been studied in (Gençağa et. al., 2008). Although particle filtering consists of update and prediction stages, in (Mihaylova et. al., 2005), particle filtering with α-stable distributions have been applied using only likelihood function without an update equation by proper selection of the initial densities.

It is noted that the power spectrum of the chaotic signals are concentrated at low frequencies although these signals have a broad-band nature in general (Rasband, 1990). Since the purpose of the spread-spectrum communication systems is to convert the narrow-band message signal into a wideband signal, the whole spectrum has been considered to cover by the transmitted signal by adding α-stable noise signal whose characteristics are known only by the receiver.

In the proposed communication scheme in this thesis, an α-stable distributed noise has been considered as a jammer to improve the security of the system. Then the problem can be defined as filtering and tracking the chaotic states in the non-Gaussian noise environment at the receiver part. Except the channel noise which is assumed to be Gaussian, the received signal also contains non-Gaussian noise having α-stable distribution. Any Kalman filtering method is not valid due to the non-Gaussian noise used for security. The application includes tracking of the chaotic states in impulsive noise environment.

1.4 Digital Communication Systems Using Random Signals with Alpha Stable Distributions

In recent years, the stable distributions have attracted a growing interest. The time series with impulsive character are proper candidates for non-Gaussian stable modelling with a wide variety of areas such as economics, hydrology, physics and telecommunication. Previously, the Gaussian distributions have been mostly preferred method to model the time series but it has been inadequate for the data with large fluctuations. In last decades, the stable distributions defined by a more flexible mathematical formulation have become a proper candidate to describe the random processes with impulsive dynamics.

Extracting information contained in deterministic signals which are contaminated with noise has been widely studied in various signal processing applications. The methods for detecting deterministic signals in Gaussian and Non-Gaussian noise environment can be easily found in the literature such as in (Kay, 1993b) while the detection methods in α-stable (αS) noise environment appear in (Kassam, 1988), (Nikias & Shao, 1995). Optimum receiver has been designed for detection of deterministic signals embedded in impulsive noise (Tsihrintzis & Nikias, 1995). The frequency estimation of the sinusoidal signals in α-stable noise environment has been analyzed in (Altınkaya et. al., 2002). Time-delay estimation of the deterministic signals under both Gaussian and α-stable distributed noise has been explained by (Zhang J, et. al., 2007). In a recent study (Wang et. al., 2008), the binary deterministic signal has been detected using Neyman-Pearson method in both Gaussian and α-stable interference. In signal detection problems the characterization of both impulsive and Gaussian interference can be numerically modeled. As an example in (Li Xutao et. al., 2008), non-Gaussian mixture model including Cauchy and Gaussian distributions has been discussed. Alternative detector models have been introduced in (Kuruoglu et. al., 1998), (Swami & Sadler, 2002) for signal detection problem in Symmetric α-Stable (SαS) distributions. The mutual information and the Correntropy Matched Filter (CMF) have been used to detect the deterministic signals in Gaussian mixture and α-stable noise environment in (Erdogmus et. al., 2005) and in (Pokharel et. al., 2009), respectively.

In Chapter 4, a new random communication system has been proposed in which α-stable random signal whose parameters carry the binary information have been generated by the transmitter and thus the carrier is called as random carrier. In the proposed random communication system (Cek & Savacı, 2009) a random carrier is sent through the AWGN channel, and the parameters of the received signal are estimated by the fractional lower order moment (FLOM) method given in (Kuruoglu, 2001). Alternatively to the FLOM method, the parameters of the received signal for symmetric α-stable random carrier are estimated by least-squares method (Brchich & Zoubir, 1999) in Section 4.2.1 and correntropy based methods (Santamaria et. al., 2006) in Section 4.2.3. Fractional lower order moment method given by (Kuruoglu, 2001) for both symmetric and skewed α-stable carrier signals have been applied for parameter estimation in receiver part in Section 4.2.4.

.

Alternative methods to the conventional digital communication techniques called "Stable Non-Gaussian Noise Parameter Modulation" techniques for encoding the deterministic message in the transmitter part by random signals with SαS distributions have been introduced in Chapter 4. In Section 4.3.1, α-stable random signal has encoded only one bit then it has been called as α-stable ON-OFF keying; in Section 4.3.2, unipodal α-shift keying has been introduced by which the binary message signals "1" and "0" are encoded by the random signals with two different characteristic exponents, if the binary message has been encoded by the skewness parameter then the method has been called antipodal α-shift keying in Section 4.3.3; if α (CE) and β (skewness) parameters have been both used to encode the binary message pair then this method has been called as quadrature α-shift keying in Section 4.3.4. The bit error rate performances of each keying techniques have been also evaluated in corresponding sections of this chapter.

In Section 4.4, the receiver detection performances of the proposed communication schemes have been obtained by applying Neyman-Pearson test through the receiver operating characteristics (ROCs) (i.e., the probability of detection, P_{D} versus the probability of false alarm, P_{FA}). The main contribution of this section is to find the detection probabilities of both symmetric and skewed distributions at the receiver part in the Gaussian noise environment.

CHAPTER TWO

SURVEY ON CHAOTIC COMMUNICATION TECHNIQUES

In recent years, there has been significant growth in personal communications where the aim is to satisfy the huge demand of users. Among the various communication techniques, chaotic communication which is also the major subject of this chapter is an important field in the secure communication field. In this chapter, potential of chaos based communication and fundamentals of chaotic synchronization which constitutes the vital part of the chaotic communication have been explained. In the sequel, conventional chaotic communication schemes and chaotic modulation techniques have been given first and the proposed method based on the chaotic amplitude modulation has been explained in the last section.

2.1 Potential of Chaos in Communications

Since chaotic dynamics have been deeply understood in the last 30 years (Rasband, 1990), (Chua, 1994), (Strogatz, 2001) the idea to exploit chaos in communication applications has appeared due to features of chaotic signals satisfying the requirements of basic communication systems (Lau & Tse, 2003). The basic aspects are briefly given in the following sections.

2.1.1 Broad-Band Aspect

Chaotic signals are aperiodic and posses a continuous wideband frequency spectrum. In Figure 2.1, the frequency spectrum of Lorenz system is shown which is described by the ordinary differential equation given in Eq. 2.1

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz \end{aligned} \tag{2.1}$$

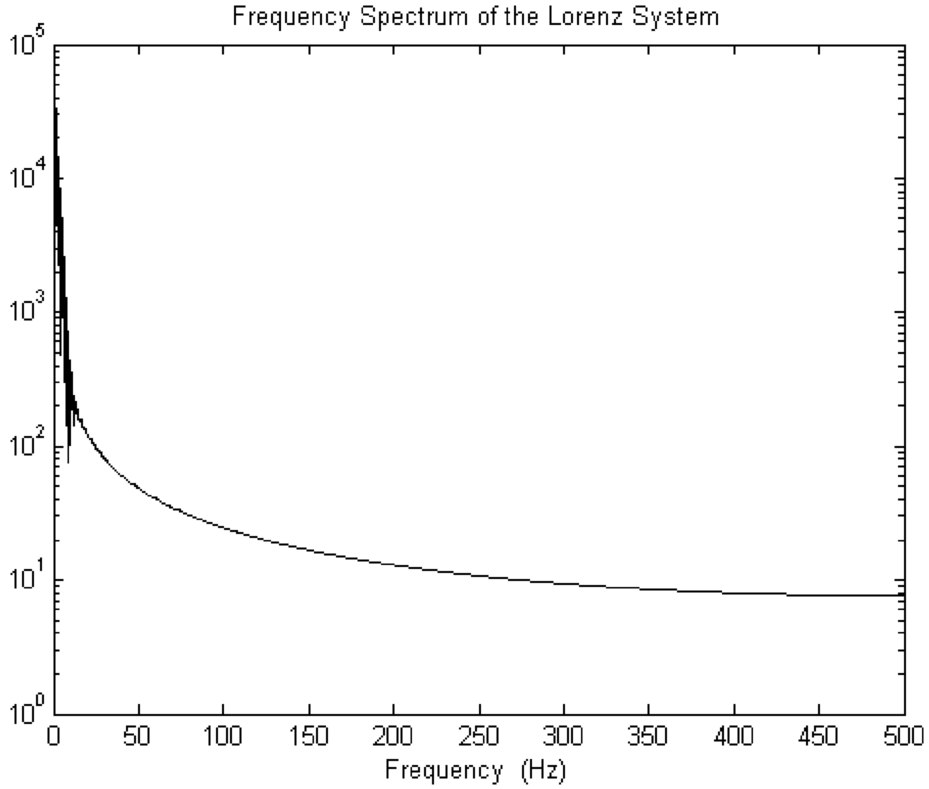

Figure 2.1 Frequency spectrum of Lorenz signal $x(t)$ sampled at 1KHz.

In communications, broad-band signals are used to overcome some problems such as frequency selective fading which occurs when the bandwidth of the channel is narrower than the bandwidth of the transmitted signal. This broad-band property provides the chaotic signals to be candidates for *spread-spectrum* communications (Abel & Schwarz, 2002).

2.1.2 Sensitivity on Initial Conditions

One of the basic properties of chaotic systems is sensitive dependence on their initial conditions. In Figure 2.2, the Lorenz system is shown with different initial conditions. When the initial conditions are slightly disturbed, totally different trajectories are obtained. This makes it difficult to guess the structure of the dynamical system and to predict the signals over long time intervals. These kinds of complex and unpredictable signals are used in *cryptographic applications*, which open another application field of chaos (Abel & Schwarz, 2002). Due to this sensitivity, the auto-correlation of chaotic signals rapidly approaches to zero.

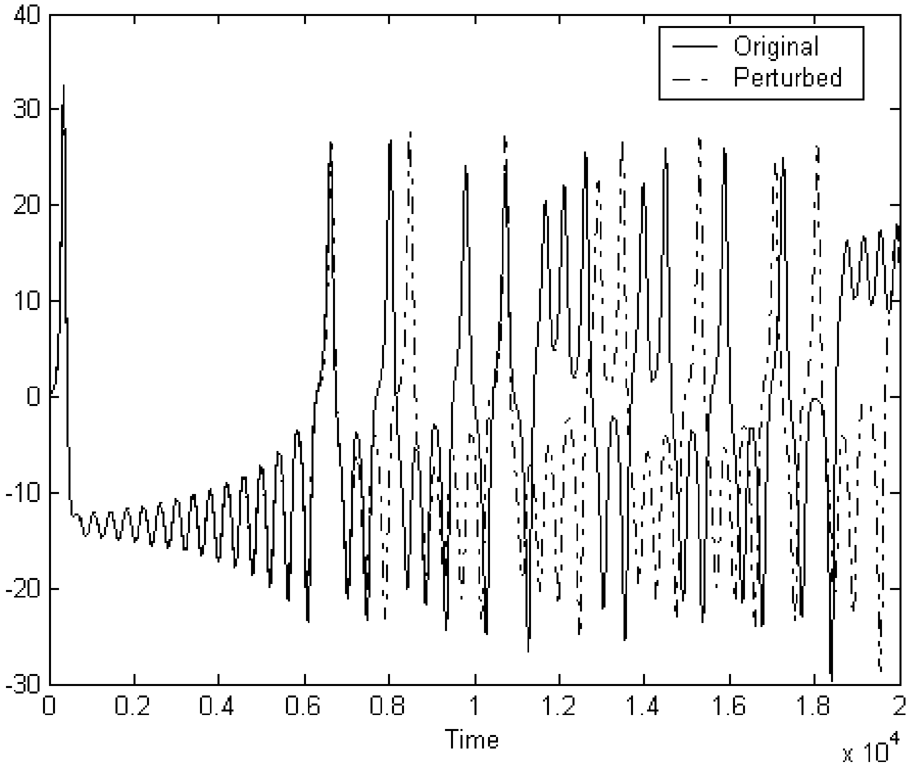

Figure 2.2 Two Lorenz signals $x(t)$ where the initial conditions are perturbed by 0.1.

2.1.3 *Orthogonality Aspect*

Since a physical channel has a limited capacity to transmit messages, an essential part of the communication system design is the sharing of limited resources. The sharing is achieved by using orthogonal signals for each user. The separability of the signals belonging to different users is ensured by the orthogonality which is given in Eq. 2.2 as

$$\int_{-\infty}^{\infty} \mathrm{x}_1(\mathrm{t})\mathrm{x}_2^*(\mathrm{t})\mathrm{dt} = 0 \tag{2.2}$$

where * denotes complex conjugate. Eq. 2.2 implies a vanishing cross-correlation of x_1 and x_2. Due to Parselval's Theorem we have

$$\int_{-\infty}^{\infty} x_1(t)x_2^*(t)dt = \frac{1}{2\pi}\int_{-\infty}^{\infty} X_1(\omega)X_2^*(\omega)d\omega \tag{2.3}$$

where X$_1$(ω) and X$_2$(ω) are Fourier transforms of $x_1(t)$and $x_2(t)$, respectively. According to the relation given in Eq. 2.3, orthogonality in the time domain implies orthogonality in frequency domain and can be achieved in different ways in a multiuser environment.

I. Signals Disjoint in Time

If at any time either x_1(t) or x_2(t) becomes zero, Eq. 2.2 holds trivially. This method is termed as time division multiple access (TDM).

II. Signals Disjoint in Frequency

If at any frequency either X$_1$(ω) or X$_2$(ω) vanishes, the frequency integral in Eq. 2.3 becomes zero. This method is termed frequency division multiple access (FDM).

III. Uncorrelated

Signals generated from different chaotic dynamical systems or same dynamical system with different initial conditions exhibit a vanishing cross-correlation or auto-correlation function which is given in Eq. 2.4

$$C[k] = \sum_n (x[n] - \mu)(x[n+k] - \mu) \tag{2.4}$$

where k is the time lag and μ is the sample mean. The auto-correlation function related with Lorenz system is shown in Figure 2.3. One can derive that samples of chaotic sequences are uncorrelated since the auto-correlation function rapidly vanishes and oscillates near to zero. This property provides the chaotic signals available for *multiuser applications* in communications (Abel & Schwarz, 2002). Eq. 2.2 can hold even if the signals are neither disjoint in time nor in frequency. This can be exploited in code division multiple access (CDMA) techniques.

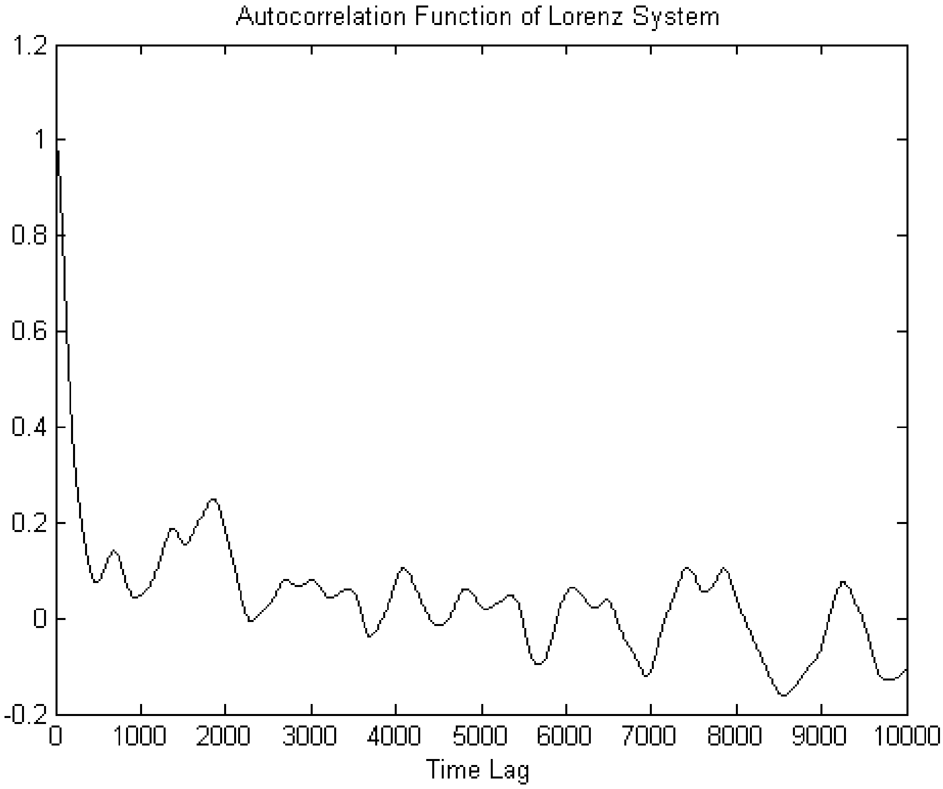

Figure 2.3 Autocorrelation function of Lorenz system with respect to time lag *k*.

2.2 Chaotic Synchronization

In chaotic communication, the class of chaotic systems which possess a self-synchronizing property is used at the transmitter part and the receiver part which is robust to perturbations in most practical applications. A chaotic system is self-synchronizing if it can be decomposed into at least two subsystems which are called as drive system and response subsystem corresponding to a transmitter and receiver in communication scheme respectively (Pecora & Caroll, 1991). The drive and response systems are coupled systems where the behavior of the response is dependent on the behavior of the drive but the drive system is not influenced by the response system and they combine as a compound dynamical system. The mathematical model related with the synchronized systems is given as;

$$\left.\begin{array}{ll}\dot{v} = f(v,u) & v \in \mathrm{R}^{\mathrm{m}} \\ \dot{u} = g(v,u) & u \in \mathrm{R}^{\mathrm{k}}\end{array}\right\} \text{ drive subsystem}$$

$$\dot{u} = g(w,u') \qquad w \in \mathrm{R}^{\mathrm{k}} \qquad \text{response subsystem} \tag{2.5}$$

In (Pecora & Caroll, 1990), it was proven that the subsystems *u* and *u'* would be synchronized if the sub-Lyapunov exponents of the *g*-subsystem are all negative. For Lorenz system, Eq. 2.1 can be considered as the drive system, since its dynamics are independent response system and Eq. 2.6 below represents dynamical response system driven by the state *x*(*t*) of Lorenz system. The eigenvalues of the Jacobian matrix are both negative, thus, $|y_2 - y|$ and $|z_2 - z| \to 0$ as $t \to \infty$. Therefore it can be said that the subsystems are asymptotically stable (Cuomo et. al., 1993).

$$\begin{aligned}\dot{y}_2 &= rx - y_2 - xz_2 \\ \dot{z}_2 &= xy_2 - bz_2\end{aligned} \tag{2.6}$$

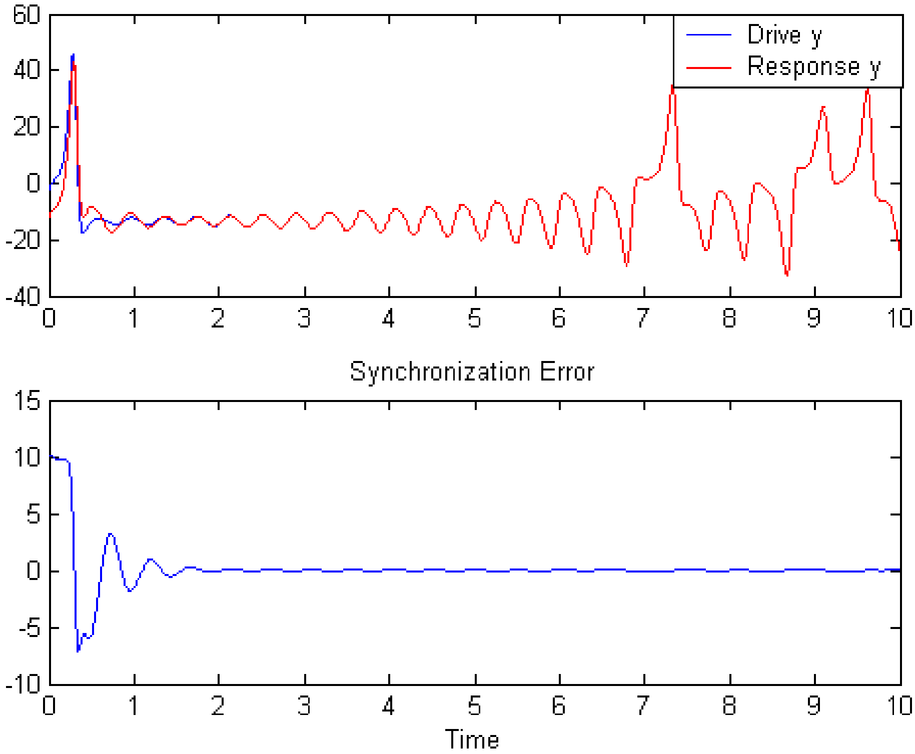

Figure 2.4 Illustration of synchronization for the Lorenz signal *y*(*t*); drive-response system (upper), synchronization error (lower).

In Figure 2.4, convergence of the response $y_2(t)$ to the drive $y(t)$ is illustrated for x driven (y,z) Lorenz subsystem. In Figure 2.4, it is also clearly seen that synchronization error decays to zero in a short time interval. Discovery of chaotic synchronization by (Pecora & Caroll, 1990) triggered to build a chaotic secure communication scheme. In fact, it is the evolution of chaotic synchronization technology to trigger the chaotic secure communication systems.

2.3 Analogue Chaotic Communication Methods

In this section, chaos-based communication systems existing in the literature have been introduced. These techniques involve analogue or digital chaotic modulations which are given in the sequel.

2.3.1 Chaotic Masking

Chaotic masking is obtained by adding the information signal to the noise-like chaotic signal (Cuomo et. al., 1993). The detection is accomplished by regenerating and subtracting the chaotic signal from the received signal. This method is simple to be implemented, but a robust synchronization circuit is required to reproduce the chaotic signal at the receiver. The additive chaos masking scheme shown in Figure 2.5 consists of two identical chaotic systems in both the transmitter and the receiver. The chaotic masking signal $c(t)$ is added into the message signal $m(t)$ and the transmitted signal $s(t)$is produced. Since the chaotic signal $c(t)$is very complex one may expect that the message signal $m(t)$can not be separated from $s(t)$ without knowing the exact $c(t)$ and in order to recover the message signal, chaotic synchronization block is needed in the receiver. It is observed at the receiver side that after a transient time interval where the synchronization error vanishes, synchronization is achieved and a hidden message signal is obtained.

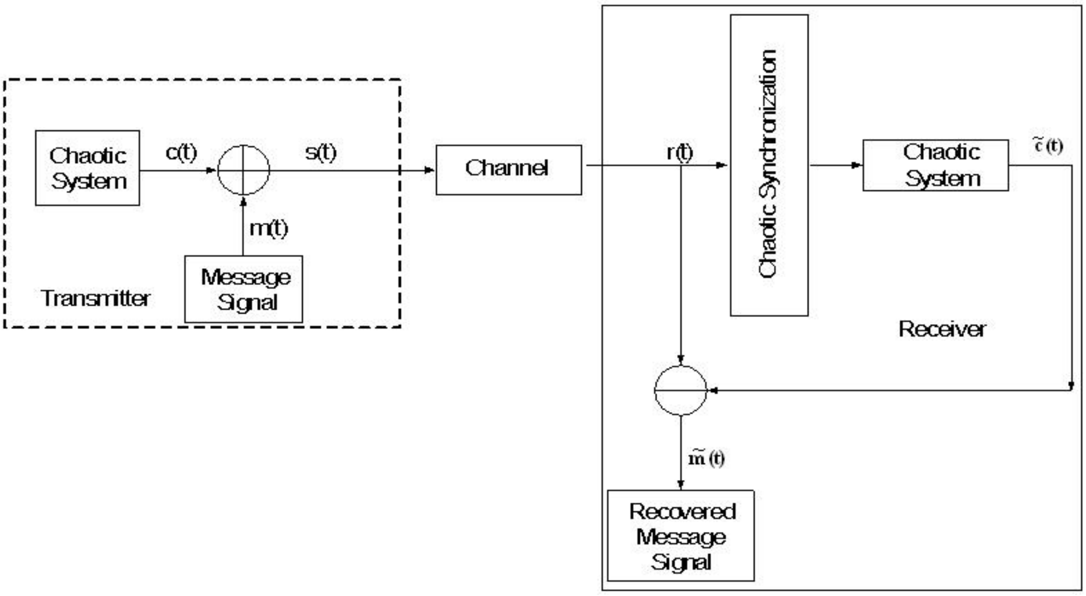

Figure 2.5 Block diagram of basic chaotic masking scheme.

Nevertheless, this scheme can not be used under practical conditions. Because the masking method is very sensitive to channel noise and parameter mismatch between chaotic systems in the transmitter and the receiver which may cause unsynchronization. Furthermore, this scheme has very low degree of security since the message can be obtained by *breaking* methods described in Section 2.6.

2.3.2 Chaotic Communication Using External Input

Steady-state analysis and implementation associated with synchronization of coupled chaotic systems driven by a sinusoidal input has been explained for Chua's circuit (Chua, 1994), (Savacı et. al., 2003). In chaotic communication, this external input can be considered as the information carrying signal. Therefore this master-slave system is one of the chaotic communication schemes.

In this section, sample communication scheme using this method has been generated for the Lorenz system where the dynamics of the transmitter are given as

$$\begin{aligned} \dot{x}_T &= \sigma(y_T - x_T) + m(t) \\ \dot{y}_T &= rx_T - y_T - x_T z_T \\ \dot{z}_T &= x_T y_T - bz_T \end{aligned} \qquad (2.7)$$

The parameters are taken as $\sigma = 16$, $r = 45.6$, $b = 4$ and $m(t)$ represents the message signal. The transmitter signal and its frequency spectrum are shown in Figure 2.6. The receiver dynamics are

$$\begin{aligned} \dot{x}_R &= \sigma(y_R - x_R) \\ \dot{y}_R &= rx_T - y_R - x_T z_R \\ \dot{z}_R &= x_T y_R - bz_R \end{aligned} \tag{2.8}$$

There are some constraints restricting the performance of the proposed communication scheme which are, first, magnitude of the message signal should be small compared to the chaotic signal and second, frequency of the message signal should be high compared to the fundamental frequency of the chaotic signal.

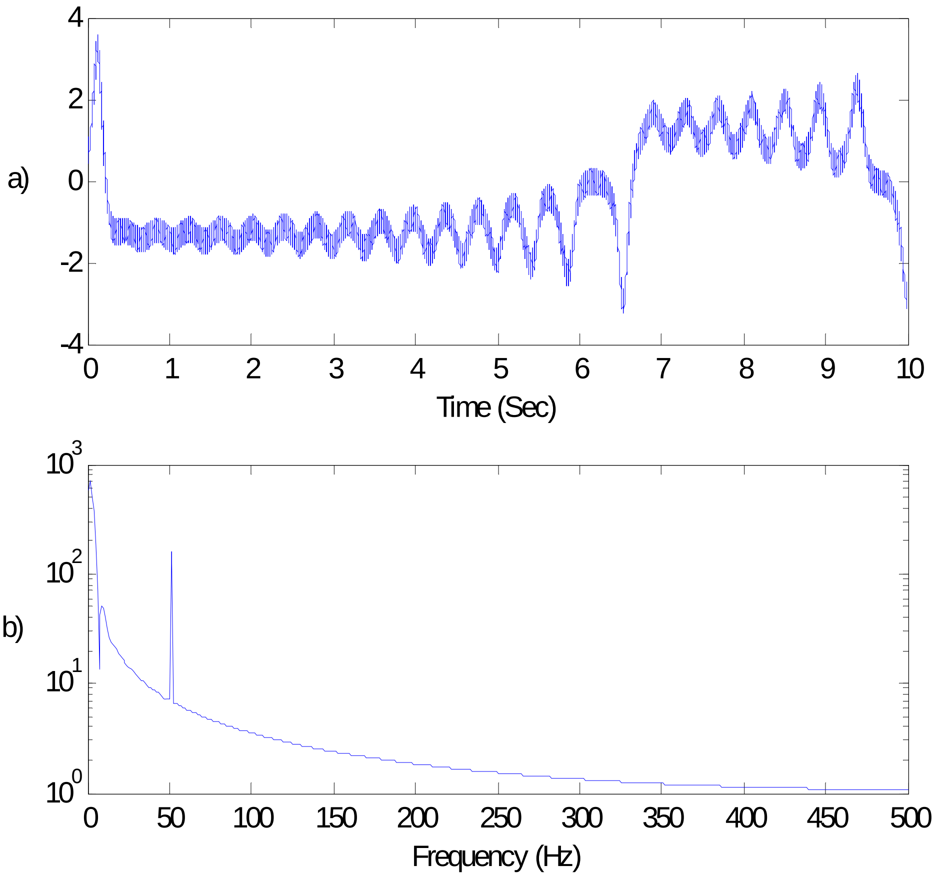

Figure 2.6 a) The chaotic signal carrying message b) Its frequency spectrum.

2.4 Chaotic Digital Modulations

Chaotic digital modulation can be described as mapping of the chaotic signals into binary sequences. There are several techniques for this purpose which are chaos shift keying (CSK) and differential chaos shift keying (DCSK), frequency-modulation DCSK and chaotic phase shift keying. In the sequel these techniques are explained briefly.

2.4.1 Chaos Shift Keying (CSK)

Chaos shift keying is a digital modulation scheme where chaotic signals obtained from different attractors or chaotic signals generated from the same dynamical system with different initial conditions are the basis functions (Kennedy et. al., 2000).

Let $s_m(t)$, m=1,2,…,M denote the elements of the signal set defined by Eq. 2.9

$$s_m(t) = \sum_{\mathrm{j=1}}^{\mathrm{N}} s_{mj} g_j(t), \quad j = 1,2,...,N \tag{2.9}$$

where the basis functions $g_j(t)$ are chaotic waveforms. The composition of CSK signal is illustrated in Figure 2.7-a and the reconstruction of the information signal is seen in Figure 2.7-b.

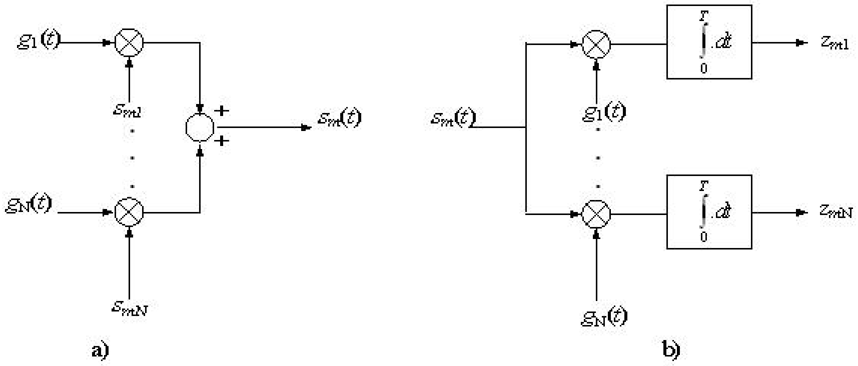

Figure 2.7 a) Generation of the elements of the signal set, b) Determination of the observation signals

Chaotic basis functions are orthonormal in the mean i.e.,

$$\mathrm{E}\left[\int_0^T g_i(t)g_j(t)dt\right]=\begin{cases}1 & \text{if } i=j\\ 0 & \text{otherwise}\end{cases} \tag{2.10}$$

where E[·] denotes the expectation operator and T is the bit duration. The element z_{mi} of the observation vector at the output of the i^{th} correlator, when signal $s_m(t)$ is transmitted, is given as

$$z_{mi}=\int_0^T s_m(t)g_i(t)dt=\int_0^T\left[\sum_{j=1}^N s_{mj}g_j(t)\right]g_i(t)dt=s_{mi}\int_0^T g_i(t)g_i(t)dt=s_{mi} \tag{2.11}$$

The simplest case of chaos shift keying is realized by a single chaotic basis function $g_1(t)$ (i.e., $N=1$), There are three main types of CSK based on a single basis function.

2.4.1.1 Chaotic On-Off Keying (COOK)

In COOK symbol 1 is represented by $s_1(t)=\sqrt{2E_b}\,g_1(t)$ and symbol "0" is given by $s_2(t)=0$. Equivalently, $s_{11}=\sqrt{2E_b}$, $s_{21}=0$ where E_b denotes the average energy per bit.

2.4.1.2 Unipodal CSK

In unipodal CSK, symbol "1" and "0" are distinguished by transmitting bit energies E_{b1} and $E_{b2}=kE_{b1}$, respectively where 0 < k < 1. Symbol 1 is represented by $s_1(t)=s_{11}g_1(t)$ and symbol "0" is given by $s_1(t)=s_{21}g_1(t)$, where $s_{11}=\sqrt{\frac{2E_b}{1+k}}$ and $s_{21}=\sqrt{\frac{2kE_b}{1+k}}$.

2.4.1.3 Antipodal CSK

In antipodal CSK, symbol "1" is represented by $s_1(t)=s_{11}g_1(t)$ and symbol "0" is given by $s_2(t)=s_{21}g_1(t)$, where $s_{11}=\sqrt{E_b}$ and $s_{21}=-\sqrt{E_b}$.

In addition to coherent matched filters, demodulation can be also performed by using coherent correlation receivers and noncoherent receivers as shown in Figure 2.8,

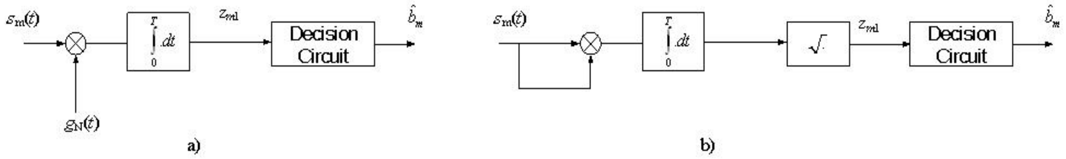

Figure 2.8 a) Coherent Receiver for CSK signal with single basis function b) Noncherent Receiver for CSK signal with single basis function.

where the mathematical expression related with the coherent receiver is given in as

$$z_{m1} = \int_0^T s_m(t) g_1(t)dt = s_{m1}\int_0^T g_1^2(t)dt = s_{m1} \tag{2.12}$$

with $\hat{b}_m$ as the estimated value of the m^{th} binary message bit. The noncoherent demodulator shown schematically in Figure 2.8-b determines the bit energy of the received signal and differs from the previous method such that the received signal is correlated with itself and not with the recovered basis function $g_1(t)$. The demodulator output is given in by

$$z_{m1} = \sqrt{\int_0^T s_m^2(t)dt} = \sqrt{s_{m1}^2 \int_0^T g_1^2(t)dt} = |s_{m1}| \tag{2.13}$$

This receiver structure can be used to demodulate both COOK and Unipodal CSK but because of the | · | function, it can not be used to recover s_{m1}'s of opposite sign and therefore unsuitable for demodulating CSK whereas the coherent correlation receiver can be used for all of these methods.

2.4.2 *Differential Chaos Shift Keying (DCSK)*

In binary DCSK, two elements of the signal set are given by

$$s_m(t) = s_{m1}g_1(t) + s_{m2}g_2(t) \tag{2.14}$$

where $(s_{11} \quad s_{12}) = (\sqrt{E_b} \quad 0)$ and $(s_{21} \quad s_{22}) = (0 \quad \sqrt{E_b})$. In the case of DCSK, the basis functions have the special form

$$g_1(t) = \begin{cases} +\dfrac{1}{\sqrt{E_b}} c(t), & 0 \le t < T/2 \\ +\dfrac{1}{\sqrt{E_b}} c(t - T/2), & T/2 \le t < T \end{cases}$$
$$g_2(t) = \begin{cases} +\dfrac{1}{\sqrt{E_b}} c(t), & 0 \le t < T/2 \\ -\dfrac{1}{\sqrt{E_b}} c(t - T/2), & T/2 \le t < T \end{cases} \tag{2.15}$$

where *c*(*t*) is a chaotic waveform and E_b is the energy of each bit. The first half of the basis function is called the reference chip, while the second half is the information-bearing chip. In binary DCSK, bit "1" is sent by transmitting $s_1(t) = \sqrt{E_b}\, g_1(t)$, while for bit "0" , $s_2(t) = \sqrt{E_b}\, g_2(t)$. Figure 2.9 shows a block diagram of a DCSK modulator. The modulation driver, delay circuit and switch are used to generate the appropriate basis functions according to the modulation input b_m.

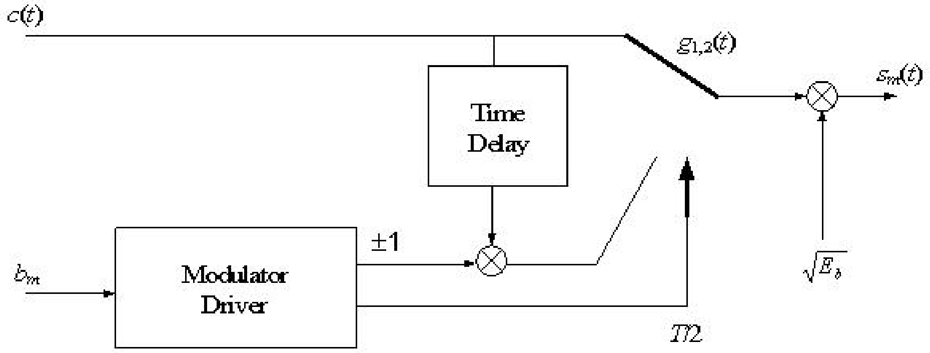

Figure 2.9 Block diagram of DCSK modulator.

Since the DCSK modulation scheme is a variant of CSK with two basis functions, it can be demodulated by a coherent receiver where the signal space diagram for CSK is also valid for DCSK which is the same as in conventional coherent FSK. As another demodulation method, differentially coherent DCSK receiver can be used with the block diagram shown in Figure 2.10. In this technique, the output of the demodulator is found as

$$z_m = \int_{T/2}^{T} r_m(t) r_m(t - T/2) dt = \int_{T/2}^{T} E_b g_m(t) g_m(t - T/2) dt \tag{2.16}$$

and by using the formula $\mathrm{E}\left[\int_{T/2}^{T} g_m^2(t)dt\right] = 1/2$, one has $z_1 \approx +E_b/2$ and $z_2 \approx -E_b/2$. The decision $\hat{b}_m$ as to which symbol was transmitted can be made by a simple level comparator with its threshold set to zero.

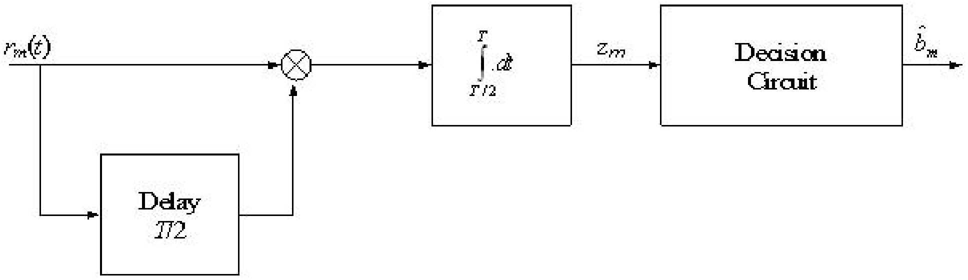

Figure 2.10 Block diagram of differentially coherent DCSK receiver.

2.4.3 *Chaotic Phase Shift Keying (CPSK)*

Due to their wideband nature, chaotic signals are more resistant to multipath propagation compared with sinusoidal functions. Additionally, an advantage of Chaotic Phase Shift Keying (CPSK) is that one chaotic generator can be sufficient for the CPSK scheme whereas, the classical CSK scheme requires two chaotic generators for each of the transmitter and receiver (Sandhu & Berber, 2005). The basic scheme of CPSK system is illustrated in Figure 2.11

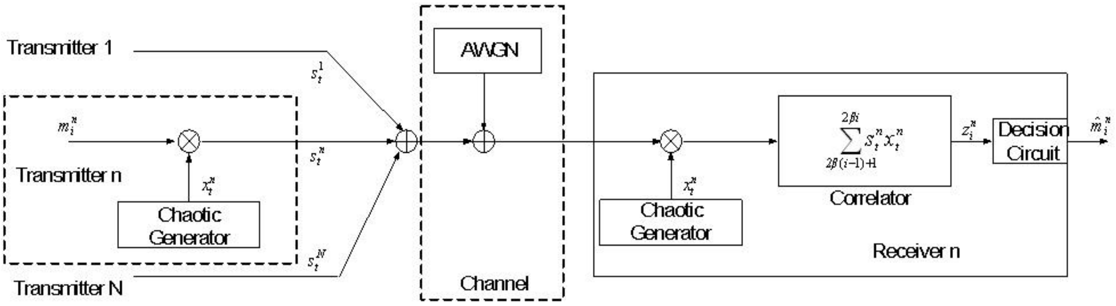

Figure 2.11 A Multiuser CPSK communication system.

Transmitter structure of the CPSK system can be mathematically formulated as follows: Consider a communication system where the zero-mean chaotic sequence generated by the chaos generator is denoted by x_t, m_i is the the i^{th} bit sequence with $m_i \in \{-1,1\}$ and 2β is the number of chaotic samples in each transmitted bit. During the i^{th} bit duration, (i.e., for time $t = 2\beta(i - 1) + 1$, $2\beta(i - 1) + 2$ ......, $2\beta i$), the transmitter's output of the n^{th} user is

$$s_t^n = \begin{cases} +x_t^n & \text{if } m_i = +1 \\ -x_t^n & \text{if } m_i = \text{-}1 \end{cases} \tag{2.17}$$

This scheme is called chaotic phase shift keying because only one generator is needed at the transmitter side, and an 180^{o} phase difference occurs if the transmitted bit is –1 (i.e., multiply by –1) (Sandhu & Berber, 2005). The noisy channel distorts the transmitted signal, and the input of the receiver n at time t is given as

$$r_t = \sum_{n=1}^{N} s_t^n + n_t \tag{2.18}$$

where the first term is the output of the N transmitters at time t, and the second term, n_t is the zero mean AWGN. By assuming that exact synchronized samples are available at the receiver, the output of the correlator of the n^{th} user at the end of the i^{th} bit duration is obtained as

$$z_i^n = \sum_{t=2\beta(\beta-1)+1}^{2\beta\beta} r_t x_t^n \tag{2.19}$$

The demodulating process is then completed by comparing z_i^n to the threshold value of zero.

2.5 Types of Chaotic Analogue Modulations

Baseband chaotic communication systems have been introduced in the previous sections. Although one of the basic features of the chaotic signals is to have broad-band spectrum, it has been noted that the power is concentrated at low frequencies for most of the chaotic systems (Rasband, 1990). Therefore, the noise robustness performance of the baseband chaotic communication schemes becomes poor against realistic channels containing distortions, channel noise and interference. This drawback has been considered to overcome by using modulation techniques including chaotic pulse position modulation (CPPM), chaotic frequency modulation (CFM). In section 2.5.2, chaotic amplitude modulation (CAM) scheme has been newly proposed. In the following, the basic structure of the chaotic frequency modulation from the literature are given briefly. The proposed chaotic amplitude modulation scheme is given in detail as the contribution of the thesis.

2.5.1 Chaotic Frequency Modulation

The CFM is a chaotic communication system which is used for spreading the spectrum. The block diagram of the chaotic frequency modulation is shown in Figure 2.12 below. The voltage controlled oscillator (VCO) generates CFM signal together with chaotic harmonic oscialltor (CHO) where the frequency of VCO is modulated by the message.

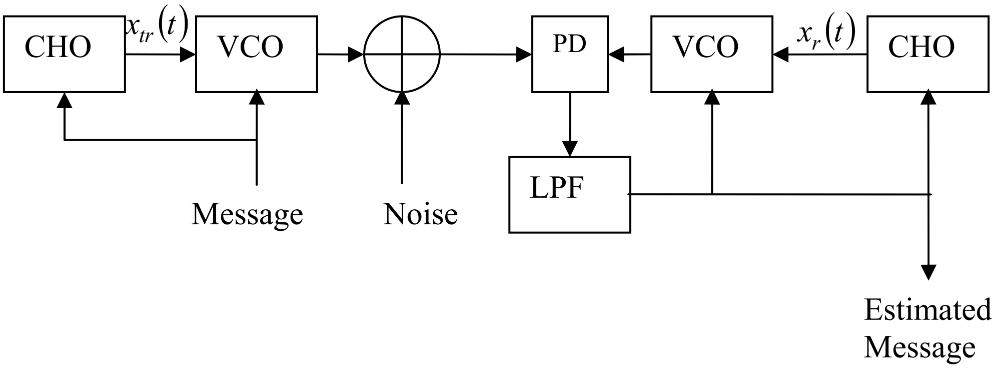

Figure 2.12 Block diagram of the CFM communication Scheme (Volkovskii et al., 2005).

In the receiver part, phase discriminator (PD) generates a signal which is the phase difference between received signal and the local VCO. The synchronization between VCOs at the transmitter and receiver is performed by the Phase Locked Loop (PLL) which is composed by local VCO, PD and the low-pass filter (LPF).

2.5.2 New Chaotic Amplitude Modulation and Demodulation Scheme

In the following, modulation and demodulation schemes of the proposed chaotic amplitude modulation system are explained.

2.5.2.1 Modulation Part

The first stage of the proposed communication scheme consists of chaotic communication based on drive-response system given in (Cuomo & Oppenheim, 1993) where the input signal is embedded into the dynamics of the chaotic system. In this study, Rössler chaotic system is used to hide the narrow-band message signal $m(t)$. The drive system is given as

$$\begin{aligned} \dot{x}_d &= -(y_d - z_d) \\ \dot{y}_d &= x_d + a_1 y_d + m(t) \\ \dot{z}_d &= a_2 + z_d (x_d - a_3) \end{aligned} \tag{2.20}$$

where the constants are $a_1 = a_2 = 0.2$ and $a_3 = 4.7$. Due to their broad-band nature, chaotic signals have frequency components on entire spectrum. In order to avoid the frequency overlapping and to achieve maximum bandwidth efficiency, the chaotic signal $y_d(t)$ is filtered to have frequency spectrum in $[0, \ f_c/2]$ by using a Butterworth low-pass filter $h(t)$ with order of 10 and cut-off frequency of $f_c/2$ where f_c is the carrier frequency. In the following, double sideband-suppressed carrier signal $r(t) = \cos(\omega_c t)$ is multiplied with the filtered chaotic signal $y_d^h(t)$ as

$$c(t) = y_d^h(t)\cos(\omega_c t) \tag{2.21}$$

where ω_c is the carrier frequency and $y_d^h(t)$ is the low-pass filtered signal. The block diagram of the transmitter associated with the proposed communication scheme is shown in Figure 2.13.

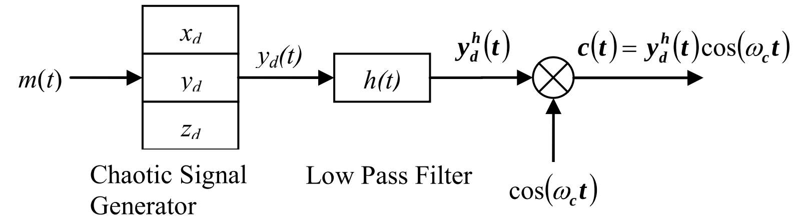

Figure 2.13 Chaotic amplitude modulation transmitter structure.

As a numerical example, the transmitted signal is shown in Figure 2.14, where $m(t) = \cos(2\pi f t)$ with $f_0 = 50\,\text{Hz}$, the carrier frequency $f_c = 200\,\text{Hz}$ and the sampling frequency is $f_s = 2\,\text{kHz}$. The signal $y_d^h(t)$ and the modulated signal $c(t)$

with corresponding frequency spectrums are shown in Figure 2.15a and 2.15b, respectively.

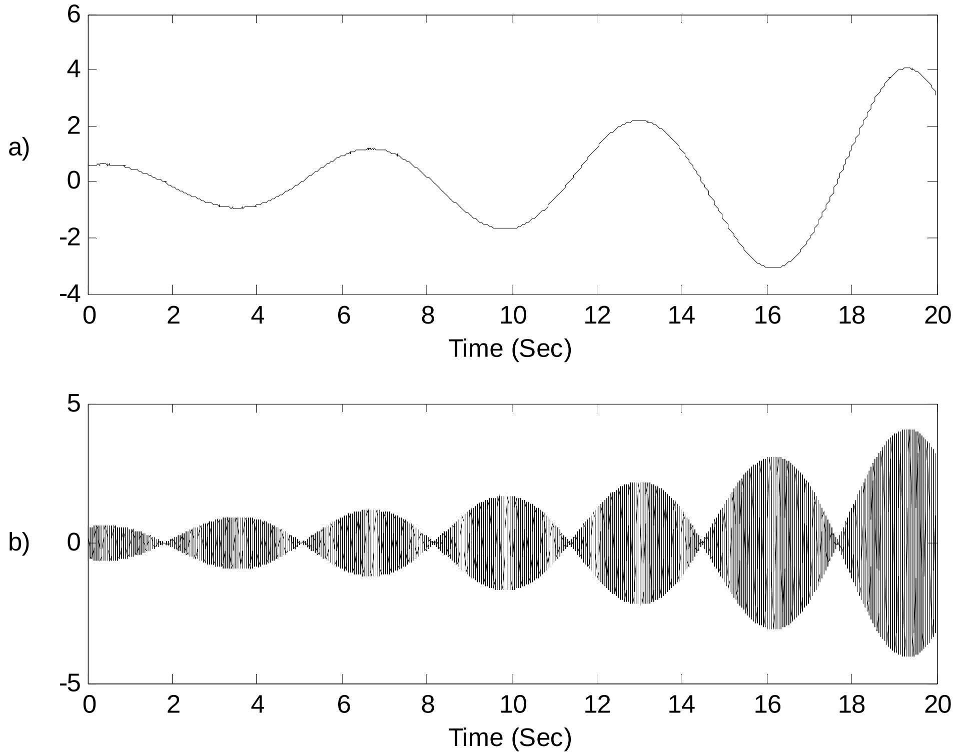

Figure 2.14 a) Low-Pass filtered Chaotic Signal $y_d^h(t)$associated with Rössler system with a cut-off frequency $f_c/2$, b) Amplitude Modulated signal at the transmitter output.

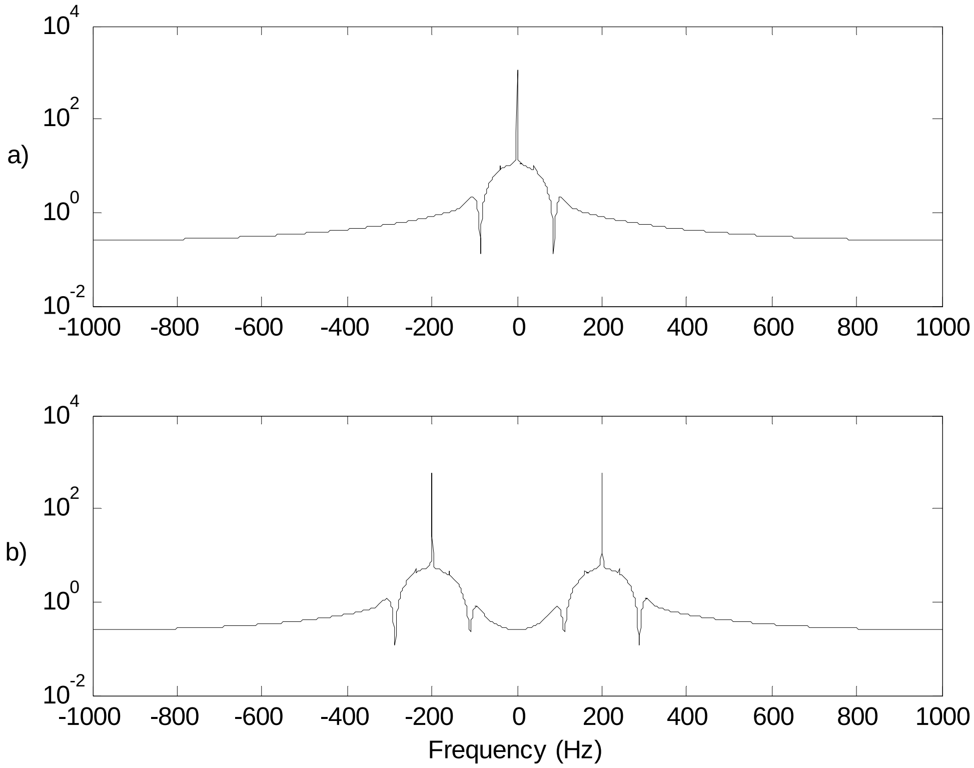

Figure 2.15 Frequency spectrum of a) Low pass filtered signal $y_d^h(t)$ in the transmitter and b) The modulated signal $c(t)$.

In the sequel, the demodulation and an appropriate filtering procedure is explained to estimate the message signal.

2.5.2.2 Demodulation Part

The receiver part shown in Figure 2.16 includes demodulation and low-pass filtering to obtain the estimate of the message signal. The demodulation is expressed as

$$r(t) = c(t)\cos(\omega_c t) \tag{2.22}$$

Since the frequency components of the demodulated signal corresponding to $2\boldsymbol{f_c}$ is filtered by $h(t)$, an estimate of the drive signal can be obtained as

$$\hat{y}_d^{hh}(t) = K \cdot \left(\hat{y}_d^h(t) * h(t)\right) \tag{2.23}$$

where the term * denotes the convolution and K is the empirically determined scale factor.

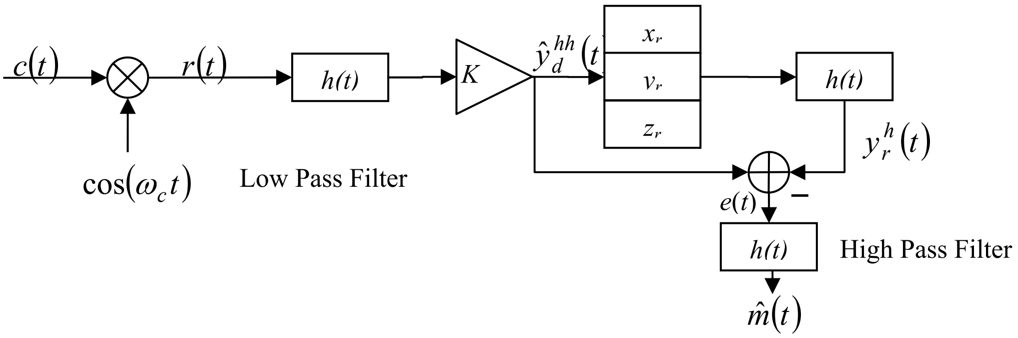

Figure 2.16 The receiver structure of the chaotic amplitude modulation.

The response of system given in Eq. (2.24) can be composed once the approximate of the drive signal $\hat{y}_d^{hh}(t)$ is found

$$\begin{aligned} \dot{x}_r &= -\left(\hat{y}_d^{hh} - z_r\right) \\ \dot{y}_r &= x_r + a_1 y_r \\ \dot{z}_r &= a_2 + z_r\left(x_r - a_3\right) \end{aligned} \tag{2.24}$$

The response signal $y_r(t)$ is filtered to obtain $\hat{y}_r^h(t) = y_r(t) * h(t)$ which has frequency content in $[0,\ \ f_c/2]$. The error between the filtered drive and response signals could be obtained by

$$\hat{e}(t) = \hat{y}_d^{hh}(t) - y_r^h(t) \tag{2.25}$$

The error term involves the synchronization error, noise and the message. Although the complete synchronization can not be achieved, the message signal could be recovered by applying a high-pass filter with 20 Hz cut-off frequency to eliminate the components due to the synchronization error.

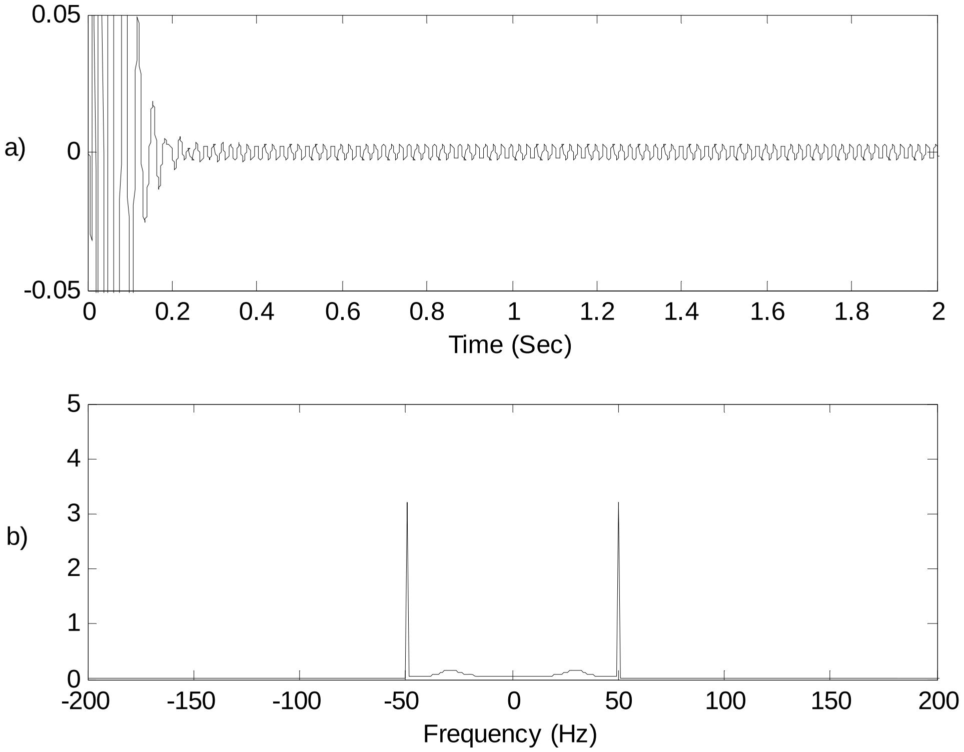

Figure 2.17 a) The error signal given in Eq. 2.25, b) The frequency spectrum of the error signal which includes message.

The error term after high-pass filtering in time domain and its frequency spectrum is illustrated in Figure 2.17. Subsequently, Figure 2.18 illustrates the estimated signal in time domain and its frequency spectrum when a signal to noise ratio of 10 dB is applied.

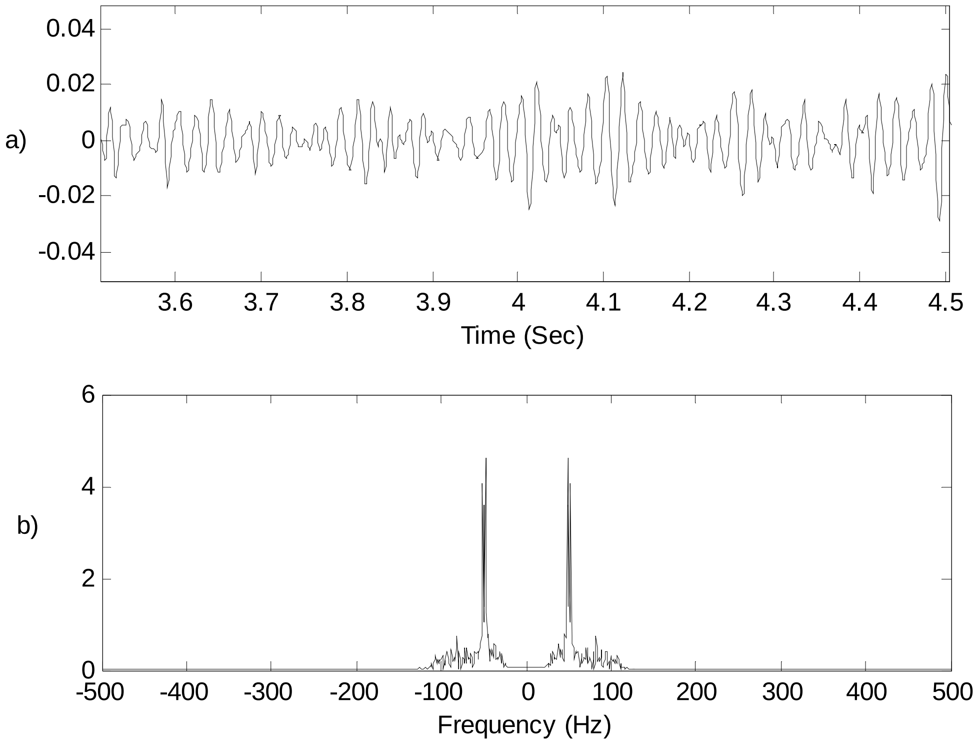

Figure 2.18 a) The error signal given in Eq. 2.25 b) The frequency spectrum obtained by Eq. 2.25 by a high pass filter.

The new chaotic communication method using double sideband-suppressed carrier modulation has been proposed in this section. It has been shown that the message signal can be successfully recovered without any significant distortion or loss. One can conclude that the message signal can be recovered if the frequency spectrum of the synchronization error signal and message signal is separable. Therefore, the frequency of the message signal should be chosen sufficiently high to avoid an interference in the error term. Another critical point is that the scale factor K should be well determined to minimize the synchronization error.

The contribution of the proposed CAM system is to give an alternative modulation method in addition to the existing methods to carry the spectrum of chaotic signals to high frequency bands. Hence, this method can lead to alternative practical implementations for secure communication. The performance of the proposed method has been investigated for noiseless case and under additive white

Gaussian noise (AWGN) channel. It is observed that the frequency of the sinusoidal message signal can be recognizable under channel noise. Further study is needed on analyzing the performance of the proposed method for different channel models.

2.6 Chaotic Breaking Methods

In the following, some of the chaotic breaking methods are described. Using these methods it is shown that chaotic modulation systems including the masking can be broken.

2.6.1 *Breaking Chaotic Communication Using Empirical Mode Decomposition (EMD)*

This practical method decomposes any observed multi-component signal defined by superposition of the mono-component signals which are called as intrinsic mode functions (IMF). This decomposition method is called as the empirical mode decomposition (EMD) (Huang et. al., 1998). Using this method the study on extracting harmonic signal from chaotic interference has been given in (Li Guo-Hui, 2006) by the intrinsic mode functions which satisfy the following two conditions (Huang N. E., 1998):

i. In the whole set, number of extrema and the number of zero crossings must either equal or differ at most by one,
ii. the mean of the local maxima and the local minima is zero in every point of the data.

The empirical mode decomposition procedure can be summarized as follows; the upper and lower envelope signals $x_{up}(t)$ and $x_{low}(t)$ are obtained from the observation signal $x(t)$ using cubic interpolation and the mean is evaluated as

$$m_1(t) = \frac{x_{up}(t) + x_{low}(t)}{2} \tag{2.26}$$

Then the first component $h_1(t)$is computed as

$$h_1(t) = x(t) - m_1(t) \tag{2.27}$$

If $h_1(t)$ is an IMF, then it is the first component of $x(t)$. If $h_1(t)$ is not an IMF then the steps in Eq. 2.26 and Eq. 2.27 are repeated and $h_{11}(t)$ is obtained as $h_{11}(t)=h_1(t)-m_{11}(t)$ until $h_{1k}(t)$ is an IMF. Then the rest of the signal $r_1(t)=x(t)-h_{1k}(t)$ is obtained and the same procedure is repeated iteratively until the residual signal $r(t)$ is mono-component signal from which IMF can not be extracted.

This breaking system has been applied for the chaotic communication scheme given in Section 2.3.2. Figure 2.19 illustrates the chaotic signal carrying a sinusoid as the message with a frequency of 50 Hz. The upper and lower envelopes of the transmitted signal have been found and used to extract the intrinsic mode functions.

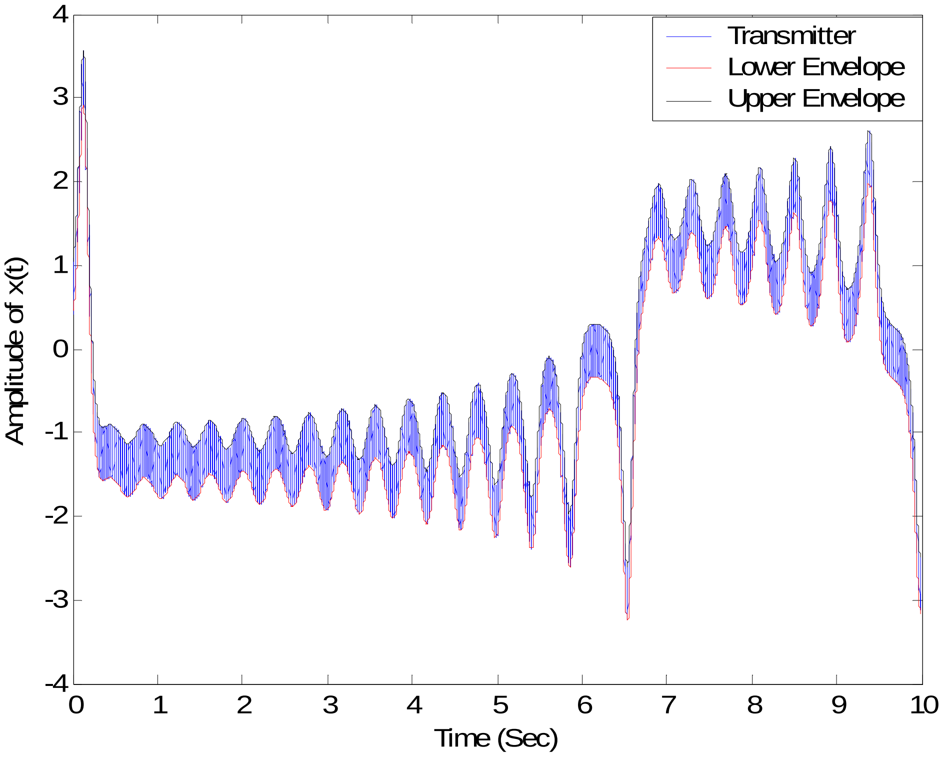

Figure 2.19 Chaotic signal masking a sinusoidal message signal with 50 Hz and its upper and lower envelopes obtained by cubic interpolation.

The decomposition of the transmitter signal with their frequency spectrum are shown in Figure 2.20. The first component directly gives the message signal whose frequency can be easily extracted.

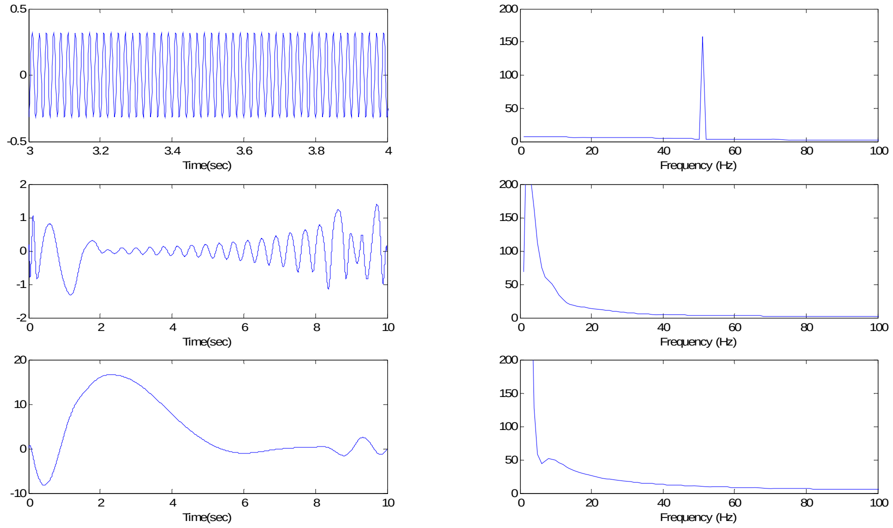

Figure 2.20 The first three intrinsic mode functions and their corresponding frequency spectrums of the of the chaotic transmitter signal shown in Figure 2.19.

This method can break the chaotic communication schemes where the message is directly added or it has been applied as an external input to the dynamics of the system.

2.6.2 Breaking Chaotic Communication Using Spectrogram

The spectrogram has been considered to reveal the time evolution of spectral density of the transmitted signal in order to break the chaotic communication. In chaotic masking schemes, using short time Fourier transforms the message signals can be detected in the broad frequency spectrum of the chaotic signal by evaluating the frequency content of the masked signal in short time intervals. The average power density in equally divided frequency ranges is evaluated and the components in which the power is concentrated are thresholded. Thus, the frequency intervals including the frequency of the message signal is determined by using band-pass filters.

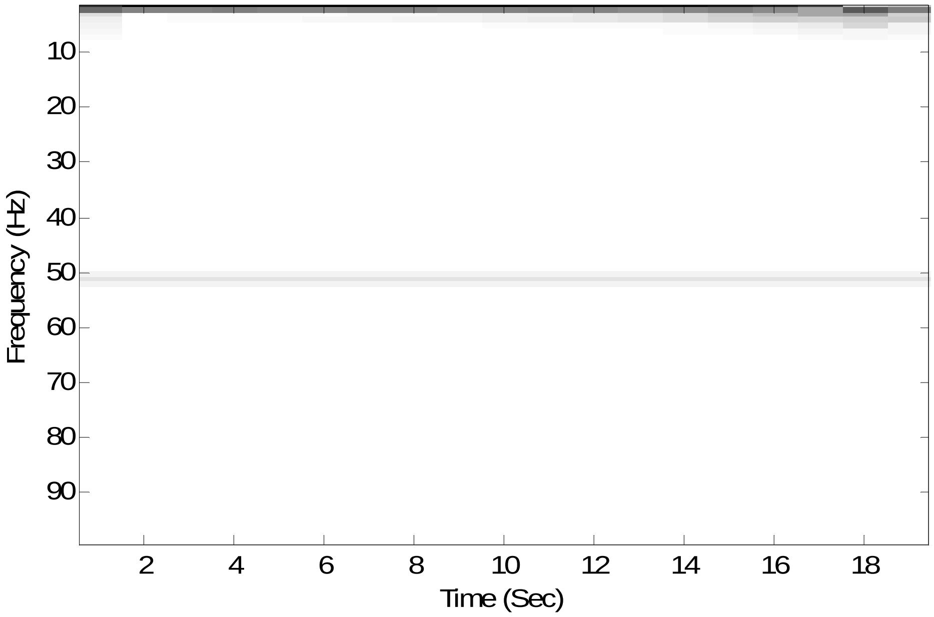

Figure 2.21 The spectrogram of the transmitted Lorenz signal including an analog sinusoidal message signal with a frequency of 50 Hz.

In Figure 2.21 the time-frequency distribution of the chaotic signal with message is shown. As clearly be seen, the message signal can be easily detected using morphological filters described in (Yang et. al., 1998).

CHAPTER THREE
PARTICLE FILTERING OF THE CHAOTIC SIGNALS IN NON-GAUSSIAN ENVIRONMENTS

In recent years, tracking the states of the nonlinear dynamical systems from the noisy measurements has been analyzed in non-Gaussian environments. Many applications require proper filtering techniques to uncover the underlying dynamics of a physical system. This problem can be solved by using optimal and suboptimal Bayesian algorithms. In addition to the optimal methods such as Kalman filtering and Grid-Based filtering, suboptimal methods such as extended Kalman filtering (EKF) and Particle Filtering (PF) have been given in (Arulampalam et. al., 2002). The basic assumptions of the optimal algorithms are that the dynamic systems are linear and both measurement and process noise models are considered as Gaussian. Since the linearity assumptions do not hold in practise the extended Kalman filtering is proposed for estimation of the states of the dynamical system in the Gaussian noise environment. Particle filters are given as a proper filtering method for the nonlinear dynamics in non-Gaussian noise environments. In Section 3.1, the mathematical background related with these filtering methods has been briefly given, including extended Kalman filter in Section 3.1.1, and particle filtering in Section 3.1.2. An application for estimating the nonlinear states and chaotic signal obtained from the Henon map in Cauchy distributed noise environment has been proposed in Section 3.2 and in Section 3.3, respectively. In the following, the nonlinear tracking problem and its Bayesian solution are given briefly. The non-Gaussian noise can be used as jammer in order to improve the security of the chaotic communication schemes explained in Chapter 2.

3.1. Suboptimal Bayesian Filtering Methods

Evolution of the state sequence can be represented by the state vector $\mathbf{x}_k, k \in N$,

$$\mathbf{x}_k = \mathbf{f}_k(\mathbf{x}_{k-1}, \mathbf{v}_{k-1}) \qquad (3.1)$$

where $\mathbf{x}_k \in \Re^{nx}$, $\mathbf{v}_k \in \Re^{nv}$, is an independently identically distributed (i.i.d) noise sequence, $\mathbf{f}_k : \Re^{nx} \times \Re^{nv} \rightarrow \Re^{nx}$ is a function of state vector $\mathbf{x}_{k-1}$ and a process noise vector $\mathbf{v}_{k-1}$, *nx* and *nv* are the dimensions of the state and process noise vectors, respectively. The aim is to estimate the state vector $\mathbf{x}_k$ from the measurements

$$\mathbf{y}_k = \mathbf{h}_k(\mathbf{x}_k, \mathbf{w}_k) \tag{3.2}$$

where $\mathbf{h}_k : \Re^{nx} \times \Re^{nw} \rightarrow \Re^{nx}$ is a function of measurement of state $\mathbf{x}_k$, measurement noise $\mathbf{w}_k$, *nx* and *nw* are the dimensions of the state and measurement noise vectors, respectively.

Bayesian estimation is based on constructing the conditional *posterior* pdf $\boldsymbol{p}(\boldsymbol{x_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}})$ recursively from the previous observations by assuming the *prior* or initial pdf $\boldsymbol{p}(\boldsymbol{x}_0 \mid \boldsymbol{y}_0)$ is known. The prediction of the posterior pdf at time *k* can be obtained by Chapman-Kolgomorov equation as given below

$$\boldsymbol{p}(\boldsymbol{x_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1}) = \int \boldsymbol{p}(\boldsymbol{x_k} \mid \boldsymbol{x}_{\boldsymbol{k}-1})\boldsymbol{p}(\boldsymbol{x}_{\boldsymbol{k}-1} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1})\boldsymbol{d}\boldsymbol{x}_{\boldsymbol{k}-1} \tag{3.3}$$

The Bayesian solution can be obtained by the prediction step given in Eq. 3.3 and the update step which is obtained via Bayes' rule

$$\boldsymbol{p}(\boldsymbol{x_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}}) = \frac{\boldsymbol{p}(\boldsymbol{y_k} \mid \boldsymbol{x_k})\boldsymbol{p}(\boldsymbol{x_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1})}{\boldsymbol{p}(\boldsymbol{y_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1})} \tag{3.4}$$

where the normalizing constant term $\boldsymbol{p}(\boldsymbol{y_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1})$ is obtained as

$$\boldsymbol{p}(\boldsymbol{y_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1}) = \int \boldsymbol{p}(\boldsymbol{y_k} \mid \boldsymbol{x_k})\boldsymbol{p}(\boldsymbol{x_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1})\boldsymbol{d}\boldsymbol{x_k} \tag{3.5}$$

In general, the recursive solution of the posterior pdf given in Eq. 3.4 can not be obtained analytically. Therefore, optimal algorithm which is Kalman filter or suboptimal algorithms such as Extended Kalman Filter (EKF) and Particle Filters (PF) can be applied to approximate the optimal Bayesian solution. Since the state evolution function given in Eq. 3.1 is non-linear in chaotic systems, the nonlinear Bayesian filters EKF and PF will be described in Section 3.1.1 and 3.1.2, respectively.

3.1.1. Extended Kalman Filter

Linear Kalman filter and extended Kalman filter assume that the process noise and the measurement noise is Gaussian distributed. If the state and measurement equations given in Eq. 3.1 or Eq. 3.2 are nonlinear, then local linearizations can be used to model the nonlinearity. The required posterior density $\boldsymbol{p}(\boldsymbol{x_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}})$ is approximated by EKF using Gaussian densities given in the following equations (Arulampalam et. al., 2002),

$$\boldsymbol{p}(\boldsymbol{x}_{\boldsymbol{k}-1} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1}) \approx \mathrm{N}(\boldsymbol{x}_{\boldsymbol{k}-1}; \boldsymbol{m}_{\boldsymbol{k}-1|\boldsymbol{k}-1}, \boldsymbol{P}_{\boldsymbol{k}-1|\boldsymbol{k}-1}) \tag{3.6}$$

$$\boldsymbol{p}(\boldsymbol{x_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1}) \approx \mathrm{N}(\boldsymbol{x_k}; \boldsymbol{m}_{\boldsymbol{k}|\boldsymbol{k}-1}, \boldsymbol{P}_{\boldsymbol{k}|\boldsymbol{k}-1}) \tag{3.7}$$

$$\boldsymbol{p}(\boldsymbol{x_k} \mid \boldsymbol{y}_{1:\boldsymbol{k}}) \approx \mathrm{N}(\boldsymbol{x_k}; \boldsymbol{m}_{\boldsymbol{k}|\boldsymbol{k}}, \boldsymbol{P}_{\boldsymbol{k}|\boldsymbol{k}}) \tag{3.8}$$

where N denotes the Gaussian distribution. The update equations associated with mean $\boldsymbol{m}_{\boldsymbol{k}-1}$ and covariance $\boldsymbol{P}_{\boldsymbol{k}-1}$ are given as

$$\boldsymbol{m}_{\boldsymbol{k}|\boldsymbol{k}-1} = \mathbf{f}_{\boldsymbol{k}}(\boldsymbol{m}_{\boldsymbol{k}-1|\boldsymbol{k}-1}) \tag{3.9}$$

$$\boldsymbol{P}_{\boldsymbol{k}|\boldsymbol{k}-1} = \boldsymbol{Q}_{\boldsymbol{k}-1} + \hat{\boldsymbol{F}}_{\boldsymbol{k}} \boldsymbol{P}_{\boldsymbol{k}-1|\boldsymbol{k}-1} \hat{\boldsymbol{F}}_{\boldsymbol{k}}^{\boldsymbol{T}} \tag{3.10}$$

$$\boldsymbol{m}_{\boldsymbol{k}|\boldsymbol{k}} = \boldsymbol{m}_{\boldsymbol{k}|\boldsymbol{k}-1} + \boldsymbol{K_k}(\boldsymbol{y_k} - \mathbf{h}_{\boldsymbol{k}}(\boldsymbol{m}_{\boldsymbol{k}|\boldsymbol{k}-1})) \tag{3.11}$$

$$\boldsymbol{P}_{\boldsymbol{k}|\boldsymbol{k}} = \boldsymbol{P}_{\boldsymbol{k}|\boldsymbol{k}-1} - \boldsymbol{K_k} \hat{\boldsymbol{H}}_{\boldsymbol{k}} \boldsymbol{P}_{\boldsymbol{k}|\boldsymbol{k}-1} \tag{3.12}$$

The functions $\mathbf{f}_{\mathrm{k}}(\cdot)$ and $\mathbf{h}_{\mathrm{k}}(\cdot)$ are nonlinear and their local linearizations $\hat{\boldsymbol{F}}_{\boldsymbol{k}}$ and $\hat{\boldsymbol{H}}_{\boldsymbol{k}}$ are given as

$$\hat{\boldsymbol{F}}_{\boldsymbol{k}} = \left.\frac{\boldsymbol{d}\mathbf{f}_{\boldsymbol{k}}(\boldsymbol{x})}{\boldsymbol{dx}}\right|_{x=\boldsymbol{m}_{\boldsymbol{k}-1|\boldsymbol{k}-1}} \tag{3.13}$$

$$\hat{\boldsymbol{H}}_{\boldsymbol{k}} = \left.\frac{\boldsymbol{d}\mathbf{h}_{\boldsymbol{k}}(\boldsymbol{x})}{\boldsymbol{dx}}\right|_{x=\boldsymbol{m}_{\boldsymbol{k}|\boldsymbol{k}-1}} \tag{3.14}$$

$$\boldsymbol{S_k} = \hat{\boldsymbol{H}}_{\boldsymbol{k}} \boldsymbol{P}_{\boldsymbol{k}|\boldsymbol{k}-1} \hat{\boldsymbol{H}}_{\boldsymbol{k}}^{\boldsymbol{T}} + \boldsymbol{R_k} \tag{3.15}$$

$$\boldsymbol{K_k} = \boldsymbol{P}_{\boldsymbol{k}|\boldsymbol{k}-1} \hat{\boldsymbol{H}}_{\boldsymbol{k}}^{\boldsymbol{T}} \boldsymbol{S}_{\boldsymbol{k}}^{-1} \tag{3.16}$$

Above equations are obtained from Taylor series expansion of the nonlinear functions. In the next Section particle filtering method is explained which can be used for estimating the nonlinear states in non-Gaussian noise environment.

3.1.2. Particle Filtering

Particle filtering is a sequential Monte Carlo (MC) method which represents posterior density using a set of random samples which are also called as *particles* and the corresponding normalized weights. There are several particle filtering methods explained in (Arulamplam et. al., 2002). In the sequel, sampling importance sampling (SIS) particle filter is defined briefly. The estimated value from the noisy measurement y_k at time instant k can be found by the particles $\boldsymbol{x}_{0:\boldsymbol{k}}^{\boldsymbol{i}}, \boldsymbol{i} = 1, \cdots, \boldsymbol{N_s}$ where N_s is the selected number of the particles and the normalized weights $\boldsymbol{w}_{\boldsymbol{k}}^{\boldsymbol{i}}$. Then the posterior probability associated with the states $\boldsymbol{x}_{0:\boldsymbol{k}}$ up to time k can be found as

$$p(x_{0:k} \mid y_{1:k}) \approx \sum_{i=1}^{N_s} w_k^i \delta\left(x_{0:k} - x_{0:k}^i\right) \tag{3.17}$$

According to the SIS algorithm, the weights are determined by using the importance density abbreviated as $\boldsymbol{q}$ and shown below

$$\boldsymbol{w}^{\boldsymbol{i}} \propto \frac{\pi\left(\boldsymbol{x}^{\boldsymbol{i}}\right)}{\boldsymbol{q}\left(\boldsymbol{x}^{\boldsymbol{i}}\right)} \tag{3.18}$$

where the density $\pi(\boldsymbol{x})$ is proportional density to the density $\boldsymbol{p}(\boldsymbol{x})$ and $\pi(\boldsymbol{x})$ can be evaluated.

$$\boldsymbol{w}_{\boldsymbol{k}}^{\boldsymbol{i}} \propto \frac{\boldsymbol{p}\left(\boldsymbol{x}_{0:\boldsymbol{k}}^{\boldsymbol{i}} \mid \boldsymbol{y}_{1:\boldsymbol{k}}\right)}{\boldsymbol{q}\left(\boldsymbol{x}_{0:\boldsymbol{k}}^{\boldsymbol{i}} \mid \boldsymbol{y}_{1:\boldsymbol{k}}\right)} \tag{3.19}$$

$$\boldsymbol{q}(\boldsymbol{x}_{0:\boldsymbol{k}} \mid \boldsymbol{y}_{1:\boldsymbol{k}}) = \boldsymbol{q}(\boldsymbol{x}_{\boldsymbol{k}} \mid \boldsymbol{x}_{0:\boldsymbol{k}-1})\boldsymbol{q}(\boldsymbol{x}_{0:\boldsymbol{k}-1} \mid \boldsymbol{z}_{1:\boldsymbol{k}-1}) \tag{3.20}$$

$$\boldsymbol{p}(\boldsymbol{x}_{0:\boldsymbol{k}} \mid \boldsymbol{y}_{1:\boldsymbol{k}}) = \frac{\boldsymbol{p}(\boldsymbol{y}_{\boldsymbol{k}} \mid \boldsymbol{x}_{\boldsymbol{k}})\boldsymbol{p}(\boldsymbol{x}_{\boldsymbol{k}} \mid \boldsymbol{x}_{\boldsymbol{k}-1})}{\boldsymbol{p}(\boldsymbol{y}_{\boldsymbol{k}} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1})} \boldsymbol{p}(\boldsymbol{x}_{0:\boldsymbol{k}-1} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1}) \tag{3.21}$$

$$\propto \boldsymbol{p}(\boldsymbol{z}_{\boldsymbol{k}} \mid \boldsymbol{x}_{\boldsymbol{k}})\boldsymbol{p}(\boldsymbol{x}_{\boldsymbol{k}} \mid \boldsymbol{x}_{\boldsymbol{k}-1})\boldsymbol{p}(\boldsymbol{x}_{0:\boldsymbol{k}-1} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1}) \tag{3.22}$$

Using the equations (3.20) and (3.22), the weights are expressed as

$$\boldsymbol{w}_{\boldsymbol{k}}^{\boldsymbol{i}} \propto \frac{\boldsymbol{p}\left(\boldsymbol{y}_{\boldsymbol{k}} \mid \boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}}\right)\boldsymbol{p}\left(\boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}} \mid \boldsymbol{x}_{\boldsymbol{k}-1}^{\boldsymbol{i}}\right)\boldsymbol{p}\left(\boldsymbol{x}_{0:\boldsymbol{k}-1}^{\boldsymbol{i}} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1}\right)}{\boldsymbol{q}\left(\boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}} \mid \boldsymbol{x}_{0:\boldsymbol{k}-1}^{\boldsymbol{i}}, \boldsymbol{y}_{1:\boldsymbol{k}}\right)\boldsymbol{q}\left(\boldsymbol{x}_{0:\boldsymbol{k}-1}^{\boldsymbol{i}} \mid \boldsymbol{y}_{1:\boldsymbol{k}-1}\right)} \tag{3.23}$$

If the importance function is taken as $\boldsymbol{q}\left(\boldsymbol{x}_{\boldsymbol{k}} \mid \boldsymbol{x}_{0:\boldsymbol{k}-1}^{\boldsymbol{i}}, \boldsymbol{y}_{1:\boldsymbol{k}}\right) = \boldsymbol{q}\left(\boldsymbol{x}_{\boldsymbol{k}} \mid \boldsymbol{x}_{\boldsymbol{k}-1}, \boldsymbol{y}_{\boldsymbol{k}}\right)$, then the importance density is dependent on only $\boldsymbol{x}_{\boldsymbol{k}-1}$ and $\boldsymbol{y}_{\boldsymbol{k}}$. In that case the weights are expressed as in Eq. (3.24)

$$\boldsymbol{w}_{\boldsymbol{k}}^{\boldsymbol{i}} = \boldsymbol{w}_{\boldsymbol{k}-1}^{\boldsymbol{i}} \frac{\boldsymbol{p}\left(\boldsymbol{y}_{\boldsymbol{k}} \mid \boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}}\right)\boldsymbol{p}\left(\boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}} \mid \boldsymbol{x}_{\boldsymbol{k}-1}^{\boldsymbol{i}}\right)}{\boldsymbol{q}\left(\boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}} \mid \boldsymbol{x}_{0:\boldsymbol{k}-1}^{\boldsymbol{i}}, \boldsymbol{y}_{1:\boldsymbol{k}}\right)} \tag{3.24}$$

when the importance function is chosen as $\boldsymbol{q}\left(\boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}} \mid \boldsymbol{x}_{0:\boldsymbol{k}-1}^{\boldsymbol{i}}, \boldsymbol{y}_{1:\boldsymbol{k}}\right) = \boldsymbol{p}\left(\boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}} \mid \boldsymbol{x}_{\boldsymbol{k}-1}^{\boldsymbol{i}}\right)$ then the weights for each particle becomes

$$\boldsymbol{w}_{\boldsymbol{k}}^{\boldsymbol{i}} = \boldsymbol{w}_{\boldsymbol{k}-1}^{\boldsymbol{i}} \boldsymbol{p}\left(\boldsymbol{y}_{\boldsymbol{k}} \mid \boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}}\right) \tag{3.25}$$

After the values of the weights have been determined, the estimated value of the state can be found as

$$\hat{\boldsymbol{x}}_{\boldsymbol{k}} = \sum_{\boldsymbol{i}} \boldsymbol{x}_{\boldsymbol{k}}^{\boldsymbol{i}} \boldsymbol{w}_{\boldsymbol{k}}^{\boldsymbol{i}} \tag{3.26}$$

In the next Section, the particle filtering has been applied to the nonlinear dynamical system in Cauchy distributed noise environment as the impulsive noise in the measurements.

3.2. Particle Filtering Application for Tracking under Impulsive Noise

In this Section, an application on the analysis of tracking the nonlinear states under impulsive noise has been performed. Consider the nonlinear discrete time dynamical system given as

$$x_{k+1} = \frac{1}{2}x_k + 25\frac{x_k}{1+x_k^2} + 8\cos(1.2k) + v(k) \tag{3.27}$$

$$y_{k+1} = x_{k+1} + w_{k+1} \tag{3.28}$$

where the process noise $\boldsymbol{v}_{\boldsymbol{k}}$ is a Gaussian and the measurement noise w_k is a Cauchy noise whose density $f(w)$ is given as

$$f(w) = \frac{2\sigma}{\pi\left((w-\mu)^2 + 4\sigma^2\right)} \tag{3.29}$$

with scale parameter σ and the shift μ. In the application, the Cauchy noise has the pdf with $\sigma = 1$ and $\mu = 0$. The process noise has a density $\boldsymbol{N}(0,0.5)$ and the initial density of particles has been chosen as $N\left(0,\frac{1}{32}\right) + N(8,0.5) + N(-8,0.5)$.

Initial density for the generated particles is heuristically chosen based on the estimated pdf (histogram) of the observed states.

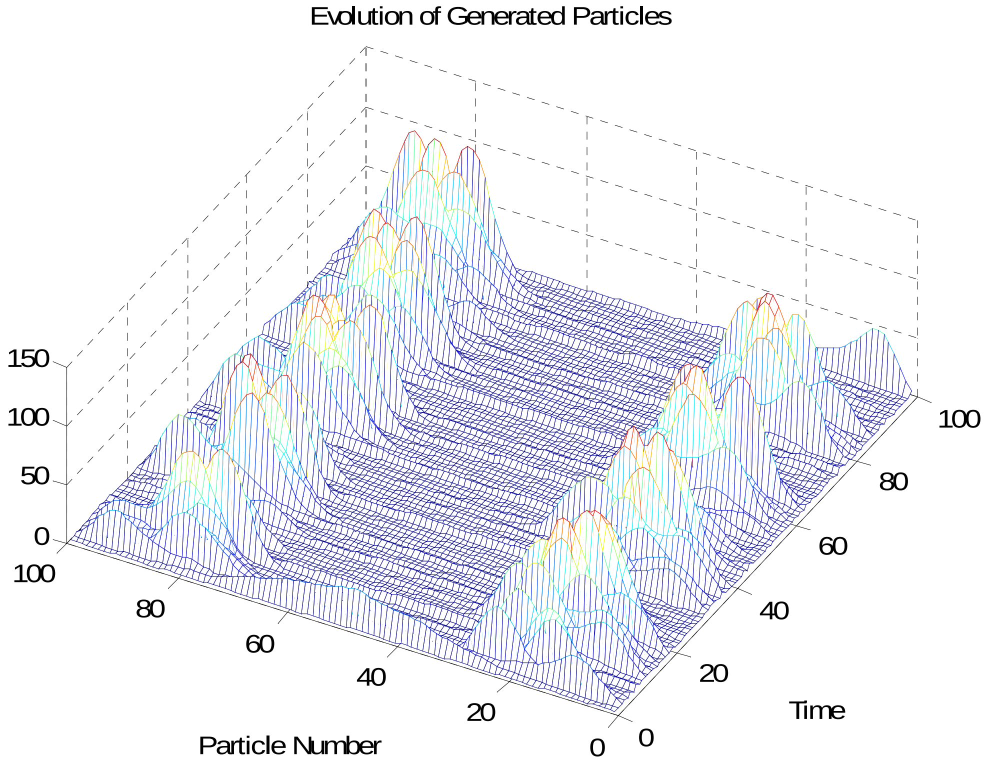

Figure 3.1 Time evolution of particles under the mapping given in Eq. 3.27.

Figure 3.1 indicates the time evolution of the generated particles which depends on the state dynamics. The filtered signal is shown in Figure 3.2 together with noisy and actual measurements. It can be clearly seen that reasonable filtering performance has been achieved.

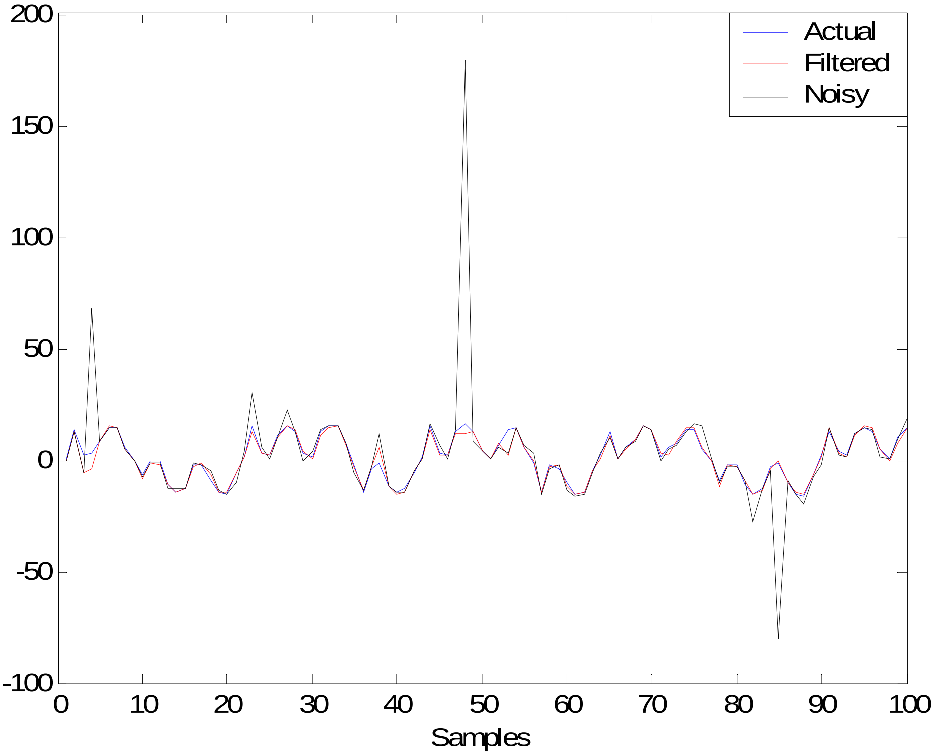

Figure 3.2 Noisy, clean and filtered signal sequences.

3.3. Particle Filtering The Chaotic Signals Under Impulsive Noise

In this Section the tracking problem of the chaotic trajectory in impulsive noise contamination has been analyzed. Differing from the signal processing application given in the previous Section, the process noise is not added since the dynamics of the system is assumed exactly known. The Henon map expressed in one dimensional space has been used as state model given in (3.30)

$$x_{k+1} = 1 - ax_k^2 + bx_{k-1} \tag{3.30}$$

$$y_{k+1} = x_{k+1} + w_{k+1} \tag{3.31}$$

The measurement noise w has the scale parameter $\sigma = 1$ and the shift parameter $\mu = 0$. In Figure 3.3 the filtered signal versus noisy and clean signal is illustrated. As clearly be seen, the particle filter can estimate the actual signal with a small error. The performance of the filter has also been indicated by the phase space reconstruction shown in Figure 3.4

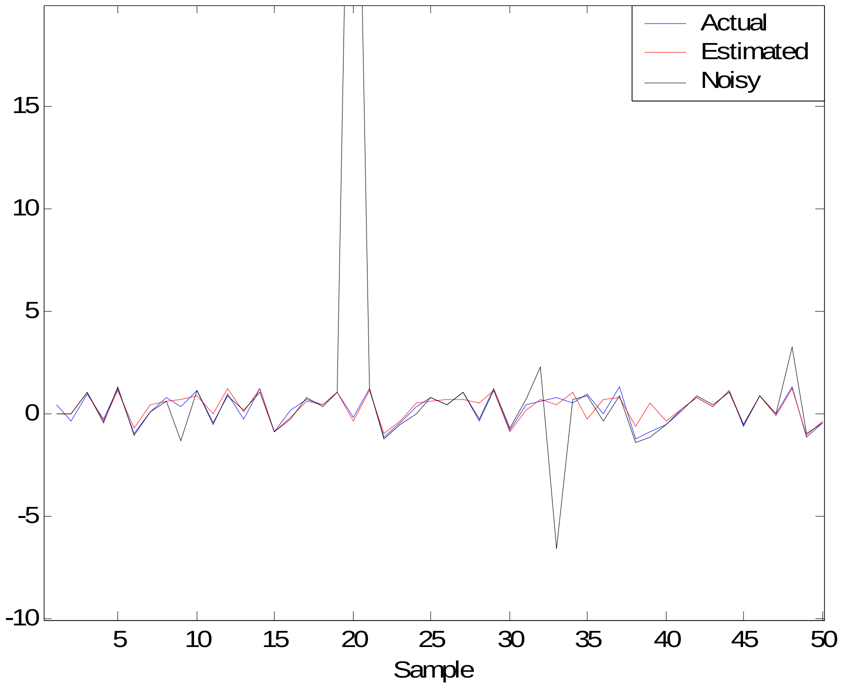

Figure 3.3 Noisy, clean and filtered signal sequences for the chaotic system given in Eq. 3.30.

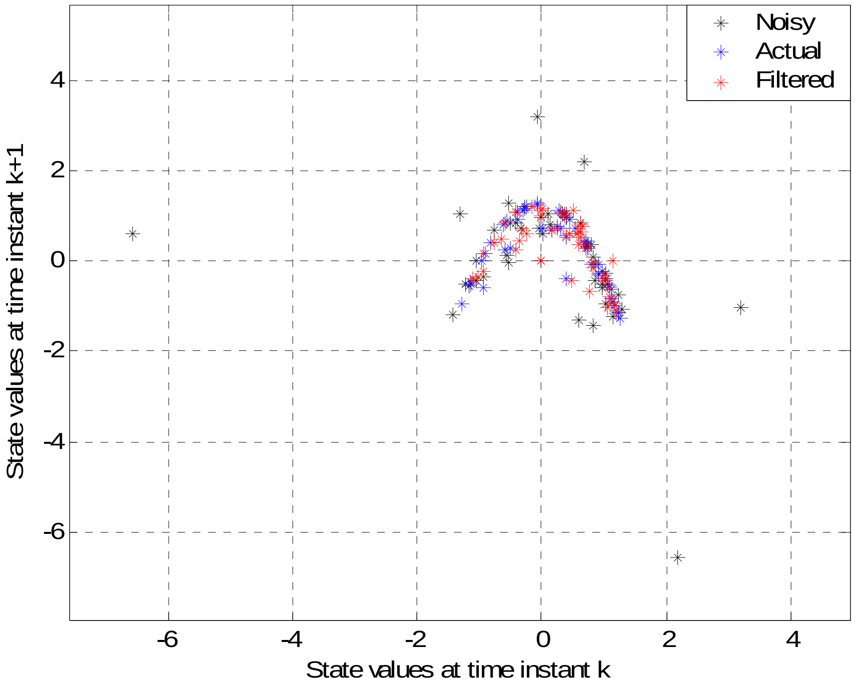

Figure 3.4 Phase space of the noisy, clean and filtered signal sequences for the chaotic system given in Eq. 3.30.

According to the obtained results, it can be said that particle filtering has a certain filtering effect but can not provide a satisfactory estimating performance in the chaotic dynamics. This is due to proper selection of the prior densities in the chaotic dynamics associated with the weights and the generated particles and there is not such a rule for determining the initial density in the particle filtering method.

3.4. Particle Filters in Chaotic Communication System

In this Section, the new chaotic secure communication system has been described. The block diagram of this communication system is shown in Figure 3.5 and it can be described as

i. the message signal $m(t)$ drives the chaotic signal generator (chaotic dynamical system),

ii. impulsive noise $r(t)$ is used for masking the output of the chaotic dynamical system $c(t)$,

iii. the masked signal $c_m(t) = c(t) + r(t)$ is sent through the AWGN channel,

iv. particle filtering is used to filter the masking signal $r(t)$ to obtain estimated output signal $\hat{c}(t)$. At this stage, since the initial density of the particles is estimated by the histogram of the dynamical system in the transmitter it can be used as a key in the receiver part to filter the masking signal. The receiver chooses particles from the initial density of the dynamical system in the transmitter accordingly and then evaluates the likelihood $p\left(c_k^r \mid x_k^i\right)$ where c_k^r is the incoming signal to the receiver. Since the density of the impulsive noise $r(t)$ is only known by the transmitter and the receiver, therefore an intruder can not filter the masking signal $r(t)$. Thus, secure chaotic communication system can be achieved.

v. The filtered signal $\hat{c}(t)$ is applied to the identical chaotic dynamical system in the receiver to synchronize the receiver with the transmitter to estimate the message signal.

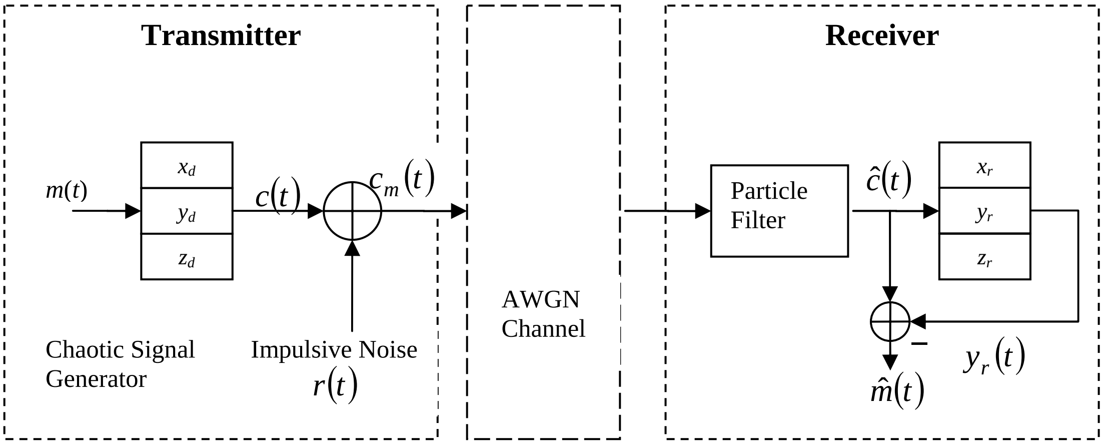

Figure 3.5 The block diagram of the chaotic secure communication system.

CHAPTER FOUR

DIGITAL COMMUNICATION SYSTEM USING RANDOM SIGNALS WITH ALPHA STABLE DISTRIBUTIONS

In this chapter, the new random secure communication scheme is introduced in which a message signal is hidden in the parameters of random carriers which have α-stable distributions. After the definitions and the basic properties of the stable distributions are given in Section 4.1, the proposed digital communication system is described and its performance in AWGN channel is studied. In Section 4.2, three receiver models based on the least-squares estimation method, the moment type method, the fractional lower order moment method (FLOM) are given.

In Subsection 4.3.1, the bit error rate performance of the communication system which is composed of the proposed α-stable ON-OFF keying transmitter and the FLOM based receiver model in the AWGN channel have been analyzed. In Subsection 4.3.2, the proposed transmitter model “unipodal α-stable keying” is given and the bit error rate performances have been analyzed for each three receiver models which are based on the least-squares method, the correntropy method and the FLOM based method, respectively. In Subsection 4.3.3, the transmitter model “antipodal α-stable keying” is proposed and its bit error rate performance is given by FLOM based receiver model; In Subsection 4.3.4, the transmitter model “quadrature α-stable keying” is described and the bit error rate performance for FLOM based receiver model is evaluated. In Subsection 4.3.5, the transmitter model “antipodal α-stable keying with random parameters” is proposed and then bit error rate performance for the FLOM based receiver model is given.

4.1 Alpha-Stable Distributions (αS)

Most of the physical and financial data have an impulsive nature which can be described by α-stable distributions. Stable distributions construct a family of distributions with the property of skewness and heavy tailness. αS distributions include well known distributions as Gaussian, Cauchy and Lévy distributions.

Definition 4.1.1 (Samorodnitsky, 1994):

A random variable X is said to have a stable distribution if for any positive real numbers A and B, there are positive real numbers C and D such that

$$AX_1 + BX_2 \overset{d}{=} CX + D \tag{4.1}$$

where X_1 and X_2 are independent realizations of X and the term "$\overset{d}{=}$" denotes equality in distribution.

The following definition states that stable distributions can be found as limits of normalized sums of independently identically distributed (i.i.d.) random variables.

Definition 4.1.2 (Samorodnitsky, 1994): A random variable X is said to have a stable distribution if it has a domain of attraction, i.e., if there is sequence of i.i.d. random variables $Y_1, Y_2, \cdots$ and sequences of positive numbers $\{d_n\}$ and real numbers $\{a_n\}$, such that

$$\frac{Y_1 + Y_2 + \cdots + Y_n}{d_n} + a_n \overset{d}{\Rightarrow} X \tag{4.2}$$

where the notation "$\overset{d}{\Rightarrow}$" denotes convergence in distribution.

The characteristic function of a stable random variable is defined as:

Definition 4.1.3 (Samorodnitsky, 1994): A random variable X is said to have stable distribution if there are parameters $0 < \alpha \leq 2$, $\sigma \geq 0$, $-1 \leq \beta \leq 1$ and $-\infty < \mu < \infty$ such that its characteristic function can be expressed as below:

$$\varphi(\omega) = \begin{cases} \exp\left\{ -\sigma^{\alpha} |\omega|^{\alpha} \left(1 - i\beta (sign\,\omega) \tan \frac{\pi\alpha}{2} \right) + i\mu\omega \right\} & \text{if } \alpha \neq 1 \\ \exp\left\{ -\sigma|\omega| \left(1 + i\beta \frac{2}{\pi} (sign\,\omega) \ln \omega \right) i\mu\omega \right\} & \text{if } \alpha = 1 \end{cases} \tag{4.3}$$

where the function $sign\,\omega$ is defined as $sign\,\omega = \begin{cases} 1 & if\omega > 0 \\ 0 & if\omega = 0 \\ -1 & if\omega < 0 \end{cases}$

Univariate stable distributions are characterized with their four parameters. The stability index which is a measure of impulsiveness in the random sequence is called as characteristic exponent and denoted by α. Impulsiveness of the random data causes heavy tails in its distribution. The skewness parameter β indicates the symmetry, the scale σ or the dispersion parameter $\gamma = \sigma^{\alpha}$ is analogous to the variance of the distribution and the parameter μ denotes the amount of the shift.

The stable random variable X can be simply denoted as $X \sim S_{\alpha}(\sigma, \beta, \mu)$ and symmetric α-stable distribution is also denoted as $S\alpha S$ when $\beta = \mu = 0$. The probability density function (pdf) of X can be found by evaluating the Fourier transform of the characteristic function (Janicki & Veron,1994)

$$f(x) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \varphi(\omega) e^{-i\omega x} d\omega \tag{4.4}$$

The main problem with the stable distributions is that except for few values of four parameters describing their characteristic functions, their probability density functions can not be expressed analytically. These exceptions are the following distributions:

I. **Gaussian distribution** (**α=2**), $S_2(\sigma, 0, \mu)$,

$$f(x) = \frac{1}{2\sigma\sqrt{\pi}} \exp\left\{-\frac{(x-\mu)^2}{4\sigma^2}\right\} \tag{4.6}$$

II. **Cauchy distribution**, (**α=1**), $S_1(\sigma, 0, \mu)$,

$$f(x) = \frac{2\sigma}{\pi\left((x-\mu)^2 + 4\sigma^2\right)} \tag{4.7}$$

III. **Lévy distribution**, (**α=1/2**), $S_{1/2}(\sigma, 1, \mu)$,

$$f(x) = \left(\frac{\sigma}{2\pi}\right)^{1/2} (x-\mu)^{-3/2} \exp\left(-\frac{\sigma}{2(x-\mu)}\right) \tag{4.8}$$

Using the numerical approximations of the formula in Eq. 4.4, one is able to construct α-stable density and cumulative distribution function (*cdf*) for various values of α, β and σ which are illustrated in Figures 4.1-4.6. The shift parameter μ is taken as $\mu = 0$ for all cases.

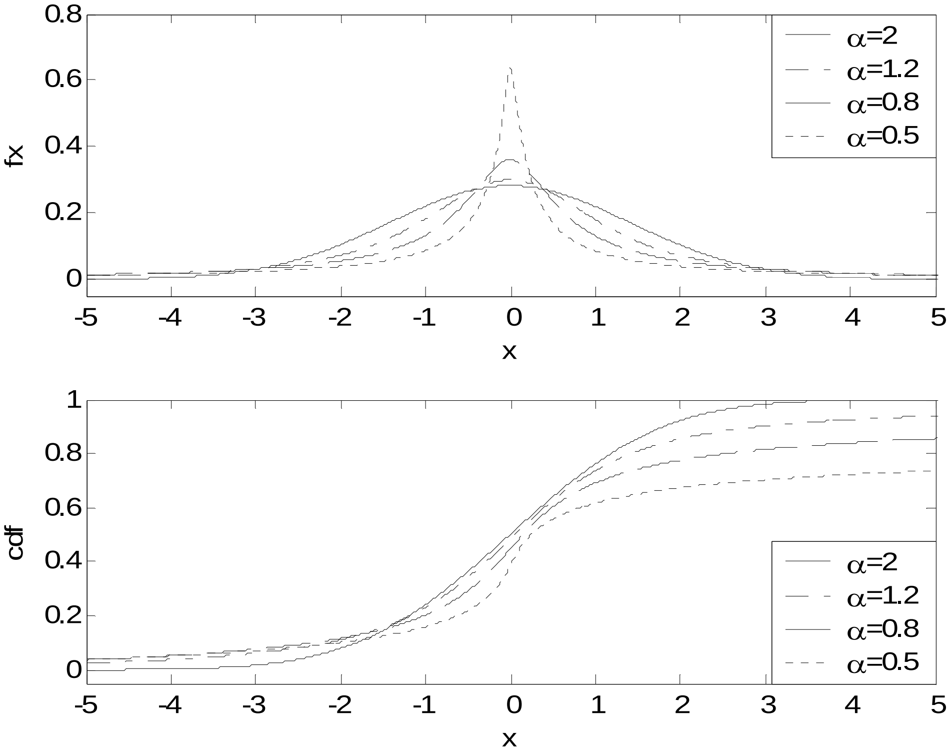

Figure 4.1 Pdf illustrated as $f(x)$ and $cdf(x)$ are shown for $\beta = 0$, $\sigma = 1$.

From Figure 4.1, while increasing the impulsiveness of the data, and hence the probability density distribution (i.e., by decreasing α), the tails of the distribution becomes heavier. For the same characteristic exponent as increasing the scale parameter σ the distribution becomes more flat which is shown in Figure 4.2. The effect of the characteristic exponent for the skewed distributions is shown in Figure 4.3 and Figure 4.4. It can be said that for lower characteristic exponent the distribution is sharper and has a non-symmetric structure. The effect of skewness parameter β for different values of characteristic exponent parameter is illustrated in Figure 4.5 and Figure 4.6. One can observe that the non-symmetric behavior increases when α decreases and β gets near to ±1.

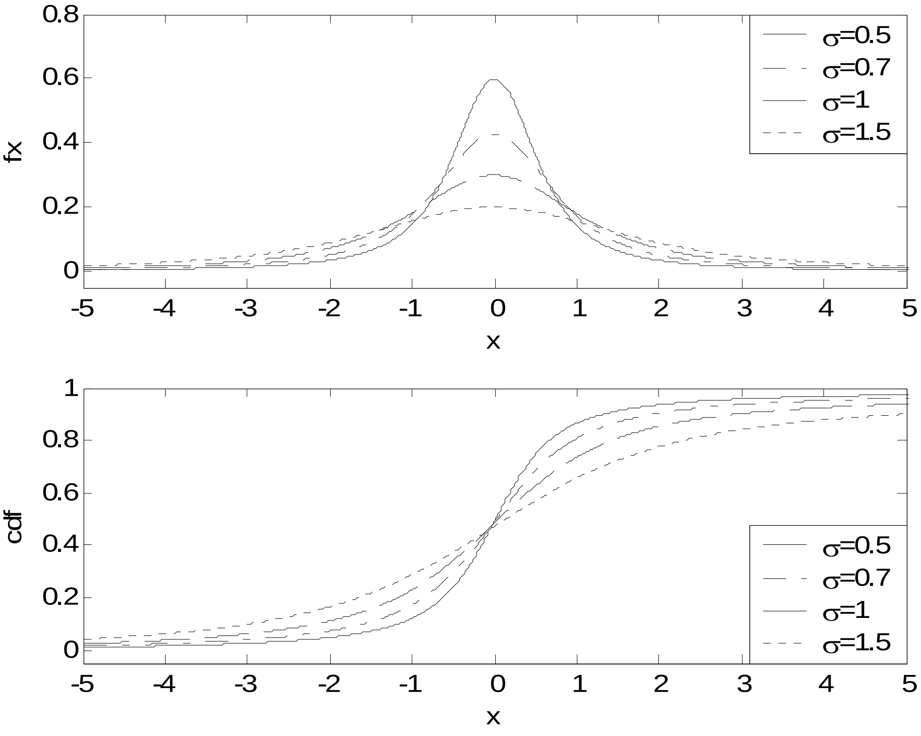

Figure 4.2 Pdf illustrated as $f(x)$ and $cdf(x)$ are shown for $\alpha = 1.2$, $\beta = 0$.

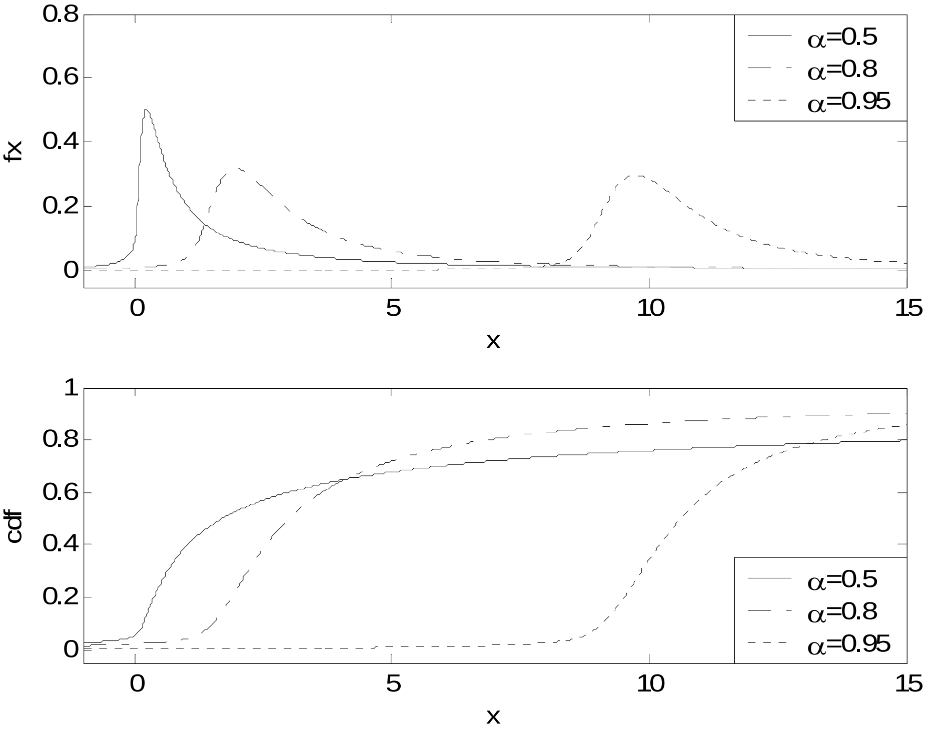

Figure 4.3 Pdf illustrated as $f(x)$ and $cdf(x)$ are shown for $\beta = 0.8$, $\sigma = 1$.

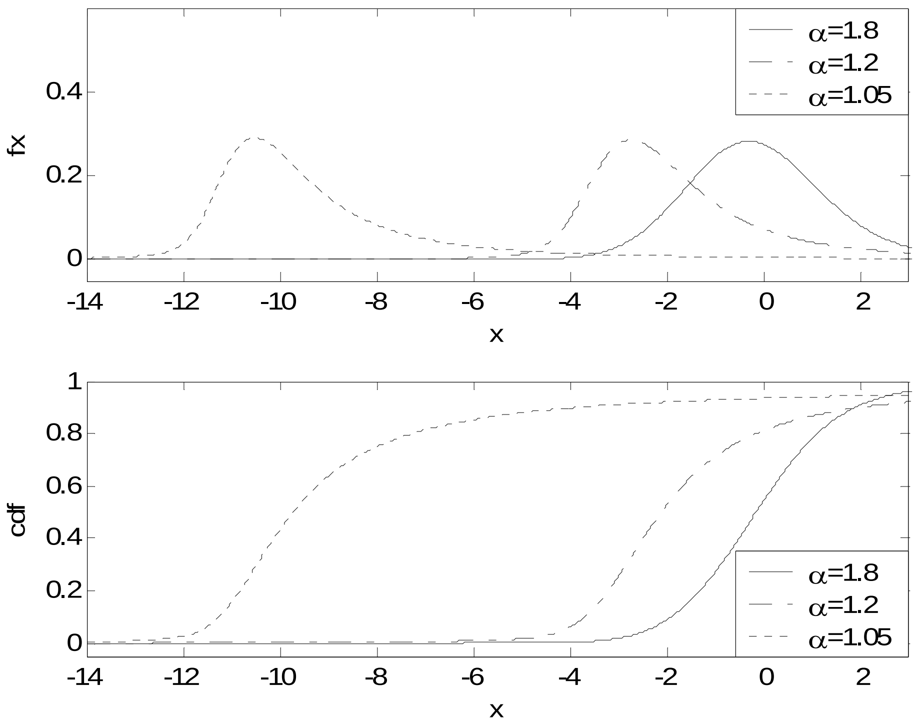

Figure 4.4 Pdf illustrated as $f(x)$ and $cdf(x)$ are shown for $\beta = -0.8$, $\sigma = 1$.

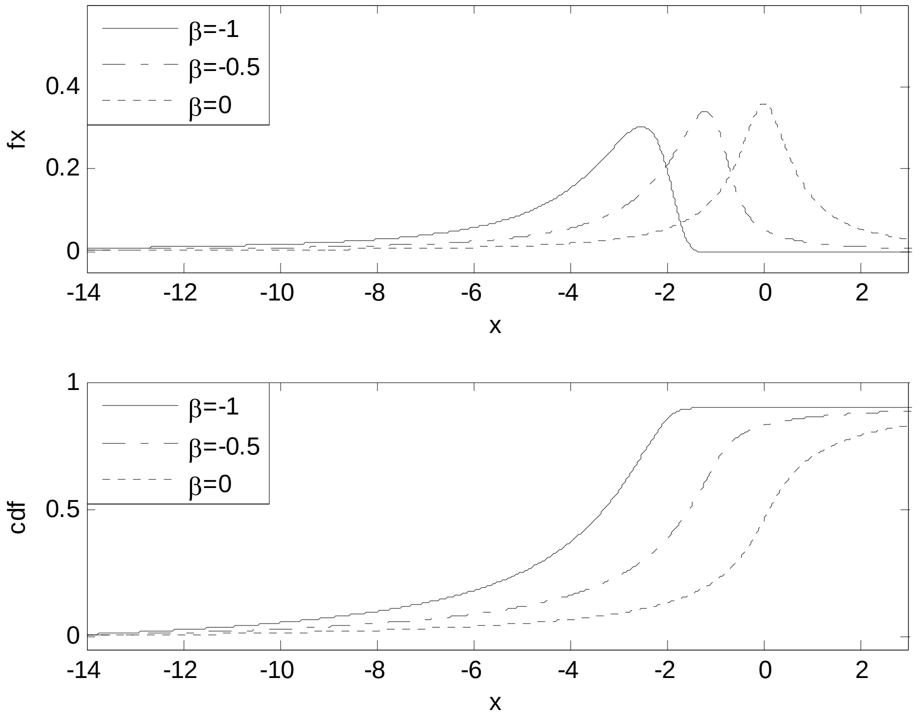

Figure 4.5 Pdf illustrated as $f(x)$ and $cdf(x)$ are shown for $\alpha = 0.8$, $\sigma = 1$.

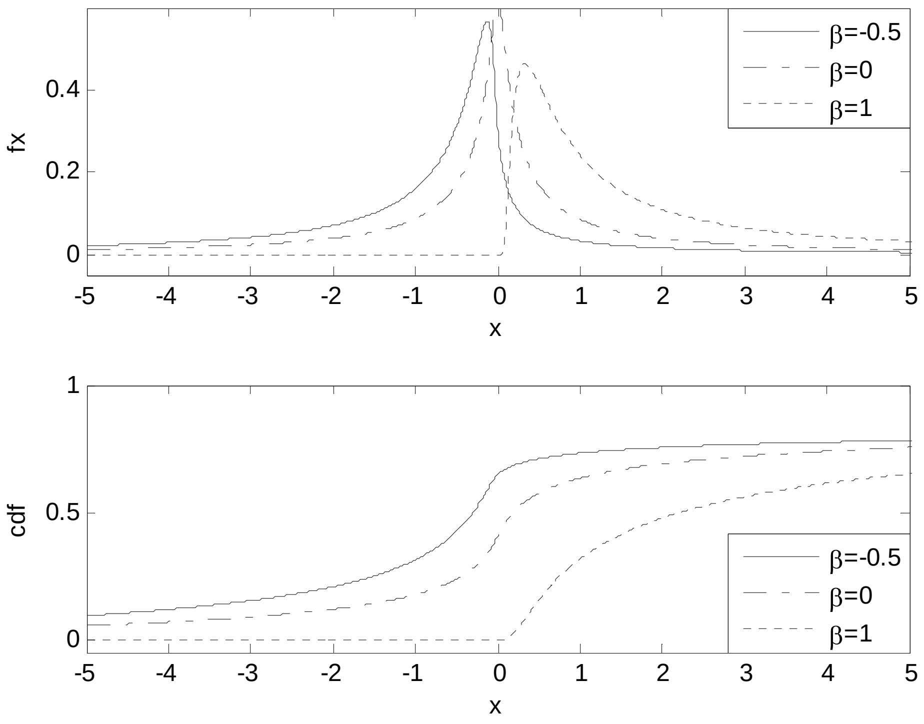

Figure 4.6 Pdf illustrated as $f(x)$ and $cdf(x)$ are shown for $\alpha = 0.5$, $\sigma = 1$.

4.1.1 Properties of α-Stable Distributions

Among all of the properties given by (Samorodnitsky, 1994), some of the most important ones are described in the following sequel:

Property 4.1.1.1 (**Addition**) Let $X_1 \sim S_\alpha(\sigma_1, \beta_1, \mu_1)$and $X_2 \sim S_\alpha(\sigma_2, \beta_2, \mu_2)$ to be independent random variables. Then $X_1 + X_2 \sim S_\alpha(\sigma, \beta, \mu)$

$$\sigma^\alpha = \left(\sigma_1^\alpha + \sigma_2^\alpha\right),\ \beta = \frac{\beta_1\sigma_1^\alpha + \beta_2\sigma_2^\alpha}{\sigma^\alpha},\ \mu = \mu_1 + \mu_2 .$$

Property 4.1.1.2 (**Shifting**) If $X \sim S_\alpha(\sigma, \beta, \mu)$ and *c* is a non-zero real constant, the density function of the random variable $X + c$ is $X + c \sim S_\alpha(\sigma, \beta, \mu + c)$.

Property 4.1.1.3 (**Scaling**) If $X \sim S_\alpha(\sigma, \beta, \mu)$ and *c* is a non-zero real constant, the density function of the random variable cX is expressed as

$$
\begin{array}{ll}
cX \sim S_\alpha\left(|c|\sigma, \operatorname{sgn}(c)\beta, c\mu\right) & \text{if } \alpha \neq 1 \\
cX \sim S_\alpha\left(|c|\sigma, \operatorname{sgn}(c)\beta, c\mu - \frac{2}{\pi}c\left(\ln|c|\sigma\beta\right)\right) & \text{if } \alpha = 1
\end{array}.
$$

Property 4.1.1.4 (**Mirror**) For any $0 < \alpha < 2$

$X \sim S_\alpha(\sigma, \beta, 0) \Leftrightarrow -X \sim S_\alpha(\sigma, -\beta, 0)$.

Property 4.1.1.5 (**Symmetry**) $X \sim S_\alpha(\sigma, \beta, \mu)$ is symmetric if and only if $\beta = 0$ and $\mu = 0$. The distribution is called as *symmetric about* μ if and only if $\beta = 0$.

Property 4.1.1.6 (**Finiteness of the moments**) Let $X \sim S_\alpha(\sigma, \beta, \mu)$ with $0 < \alpha < 2$. Then

$E|X|^p < \infty$ for any $0 < p < \alpha$,

$E|X|^p = \infty$ for any $p \geq \alpha$.

Note that α-stable random variables with α<2 have an infinite second and higher order moments and also when $\alpha \leq 1$, $\boldsymbol{E}|\boldsymbol{X}| = \infty$.

4.1.2 Generation of α-Stable Random Variables

Any symmetric α-stable random variable $X \sim S_\alpha(1,0,0)$ with $\alpha \in (0,2]$ can be obtained by the following transformation (Janicki, Veron 1994)

$$
X = \frac{\sin(\alpha V)}{\{\cos(V)\}^{1/\alpha}} \cdot \left\{\frac{\cos(V - \alpha V)}{W}\right\}^{(1-\alpha)/\alpha} \tag{4.9}
$$

where $V \sim U(-\pi/2, \pi/2)$ and W has an exponential distribution with mean 1. The skewed stable random variable $Y \sim S(1, \beta, 0)$ with $\alpha \in (0,1) \cup (1,2]$ and $\beta \in [-1,1]$ can be generated using the random variables V and W and by applying the following transformation

$$
Y = D_{\alpha,\beta} \cdot \frac{\sin\left(\alpha\left(V + C_{\alpha,\beta}\right)\right)}{\{\cos(V)\}^{1/\alpha}} \cdot \left\{\frac{\cos\left(V - \alpha\left(V + C_{\alpha,\beta}\right)\right)}{W}\right\} \tag{4.10}
$$

where the constants $C_{\alpha,\beta}$ and $D_{\alpha,\beta}$ are given as

$$
\boldsymbol{C}_{\alpha,\beta} = \frac{\arctan\left(\beta \tan(\pi\alpha/2)\right)}{1 - |1 - \alpha|} \tag{4.11}
$$

$$\boldsymbol{D}_{\alpha,\beta} = \{\cos(\arctan(\beta\tan(\pi\alpha/2)))\}^{-1/\alpha} \tag{4.12}$$

After giving the fundamentals of α-stable distributions, another important topic named as *covariation* (corresponds to the covariance for the Gaussian distributions) describing the correlation between the samples of the stable random process is explained in the following Section.

4.1.3 Covariation

The covariance function defines how much two random variables are correlated with each other (i.e., how similar they are). Since the covariance is used in the analysis of Gaussian random variables (i.e., α=2), the interaction between random variables with $1 < \alpha < 2$ is expressed by the analogous term *covariation.* More conveniently, the covariation could be obtained by set of observations using fractional lower order statistics (FLOS) and rewritten as (Miller, 1978),

$$[X,Y]_\alpha = \frac{E\left[XY^{<p-1>}\right]}{E\left[|Y|^p\right]}\gamma_Y \tag{4.13}$$

where $1 \le p < \alpha$ and $< \cdot >$ denotes signed power $\boldsymbol{x}^{<\boldsymbol{p}>} = |\boldsymbol{x}|^{\boldsymbol{p}}\,\mathrm{sgn}(\boldsymbol{x})$. $\gamma_{\boldsymbol{Y}}$ is the dispersion parameter of *Y.* The expectations including the fractional lower order moments (FLOM) from a set of observations X_{n} and Y_{n}, $n = 1,\cdots N$ can expressed as

$$\boldsymbol{E}\left[|\boldsymbol{X}|^{\boldsymbol{p}}\right] = \frac{1}{\boldsymbol{N}}\sum_{\boldsymbol{n}=1}^{\boldsymbol{N}}|\boldsymbol{X}_{\boldsymbol{n}}|^{\boldsymbol{p}} \tag{4.14}$$

and

$$E\left[|X|^{<p>}\right] = \frac{1}{N}\sum_{n=1}^{N}|X_n|^p \cdot \mathrm{sgn}(X_n) \tag{4.15}$$

Some properties related with covariation are given by (Nikias & Shao, 1995) as below:

Property 4.1.3.1 (**Independence**) If *X* and *Y* are independent and jointly SαS then

$$[X,Y]_\alpha = 0\,. \tag{4.16}$$

Property 4.1.3.2 (**Symmetry**) If *X* and *Y* are jointly Gaussian (i.e., α=2) random variables with zero mean, the covariation of *X* with *Y* is expressed as the covariance between *X* and *Y* which is symmetric.

$$[X,Y]_2 = [Y,X]_2 = E[XY] \tag{4.17}$$

Property 4.1.3.3 (**Linearity**) If X_1, X_2 and *Y* are jointly SαS and *a* and *b* real constants then the covariation $[X,Y]_\alpha$ is said to be linear in *X* as given below

$$[aX_1 + bX_2, Y]_\alpha = a[X_1,Y]_\alpha + b[X_2,Y]_\alpha \tag{4.18}$$

Property 4.1.3.4 The Cauchy-Schwarz inequality given below holds by any jointly SαS random variables X and Y.

$$\left|[X,Y]_\alpha\right| \le \|X\|_\alpha \|Y\|_\alpha^{<\alpha-1>} \tag{4.19}$$

where $\|X\|_\alpha = \left([X,X]_\alpha\right)^{1/\alpha} = \gamma_X$ and γ_X is the dispersion parameter of *X*. The asymmetric definition associated with the covariation coefficient of *X* with *Y* is expressed by (Nikias & Shao, 1995)

$$\lambda_{X,Y} = \frac{[X,Y]_\alpha}{[Y,Y]_\alpha} \tag{4.20}$$

In general it is difficult to obtain analytic expression associated with covariation between stable random variables. Using Eq. 4.13, the expression associated with asymmetric, unbounded covariation coefficient becomes

$$\lambda_{X,Y} = \frac{[X,Y]_\alpha}{[Y,Y]_\alpha} = \frac{E\left[XY^{<p-1>}\right]}{E\left[|Y|^p\right]} \tag{4.21}$$

Unlike the correlation coefficient obtained from the covariance, asymmetric and unbounded structure of the covariation coefficient makes it useless for a proper tool in most practical applications. In recent studies, the symmetric and bounded covariation coefficient has been given by (Garel et. al., 2004) and (Garel & Kodia, 2009)

$$\rho(X,Y) = \lambda_{X,Y} \cdot \lambda_{Y,X} = \frac{[X,Y]_\alpha}{[Y,Y]_\alpha} \cdot \frac{[Y,X]_\alpha}{[X,X]_\alpha}. \tag{4.22}$$

Using (4.22) the covariation coefficient can be used as a measure of interactions between the random processes having stable distributions. In digital communication the covariation is considered to be essential tool for the design of receivers under different channel models involving different fading channel types.

4.2 Proposed Receiver Models for Random Communication Systems

In this thesis, covariation has been considered as a tool for a receiver design in white Gaussian noise environment. When the received signal is defined as

$$Y = X + N \tag{4.23}$$

where the transmitted signal $X \sim S_\alpha(\gamma,0,0)$ carries the information in the Gaussian channel where $N \sim S_2(\gamma_G,0,0)$ and $\boldsymbol{\gamma_G}$ denotes channel noise variance. The covariation ρ between the estimated signal $\hat{X}$ and the received signal Y can be used to estimate the characteristic exponent of the information carrying signal X (i.e., random carrier).

Since in the proposed communication system an information carrying signal is a random signal, the ratio of the energies of the stable and the Gaussian distributed random signals (DR) can be defined as

$$DR = 10\log\left(\frac{\gamma}{\gamma_G}\right) \tag{4.24}$$

In Figure 4.7, the mean value of the Monte Carlo simulation of 100 realizations associated with the covariation for the model defined in Eq. 4.23 is illustrated with respect to the characteristic exponent α and the dispersion ratio (DR) which is used as analogous to the signal to noise ratio (SNR).

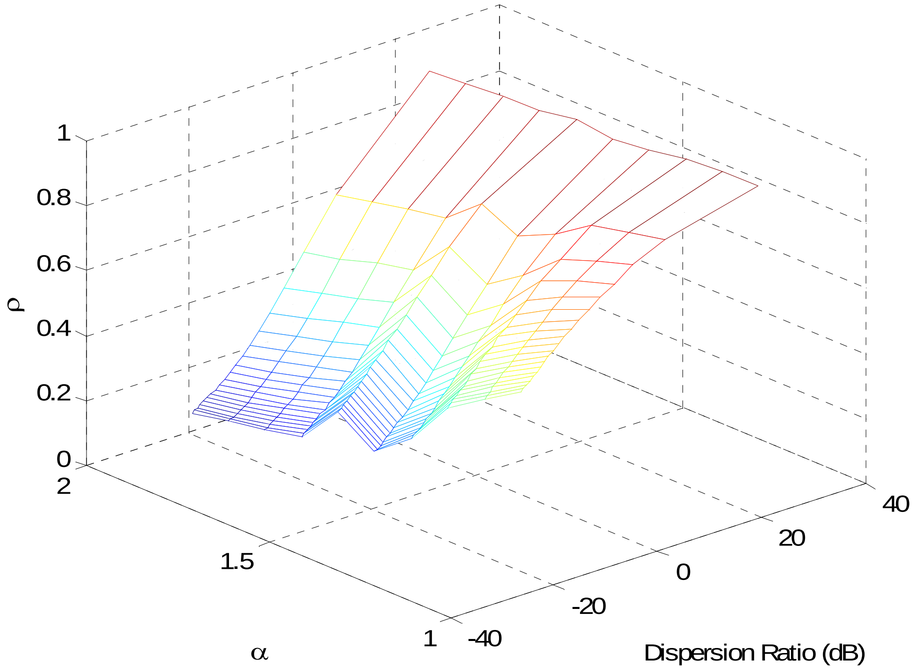

Figure 4.7 Covariation ρ of the stable distribution given in Eq. 4.23 with respect to α and dispertion ratio (DR) in dB.

As seen from Figure 4.7, one can conclude that the covariation increases when the dispersion ratio is increased. This is because, the energy of the noise in the channel comparatively becomes low. Another critical point is that when α gets closer to two, i.e., Gaussian, then the covariation decreases for the same dispersion ratio. It can be concluded that by choosing smaller α (i.e., by choosing more impulsive carrier signal), better covariation between the random carrier and received signal can be obtained.

On the other hand, the standard deviation of the Monte Carlo simulation with respect to the characteristic exponent α and the dispersion ratio (DR) illustrated in Figure 4.8 indicates that the probability of error in estimating the covariation increases when α gets closer to two, especially for low dispersion ratios. These findings can be a guide to design a receiver using covariation.

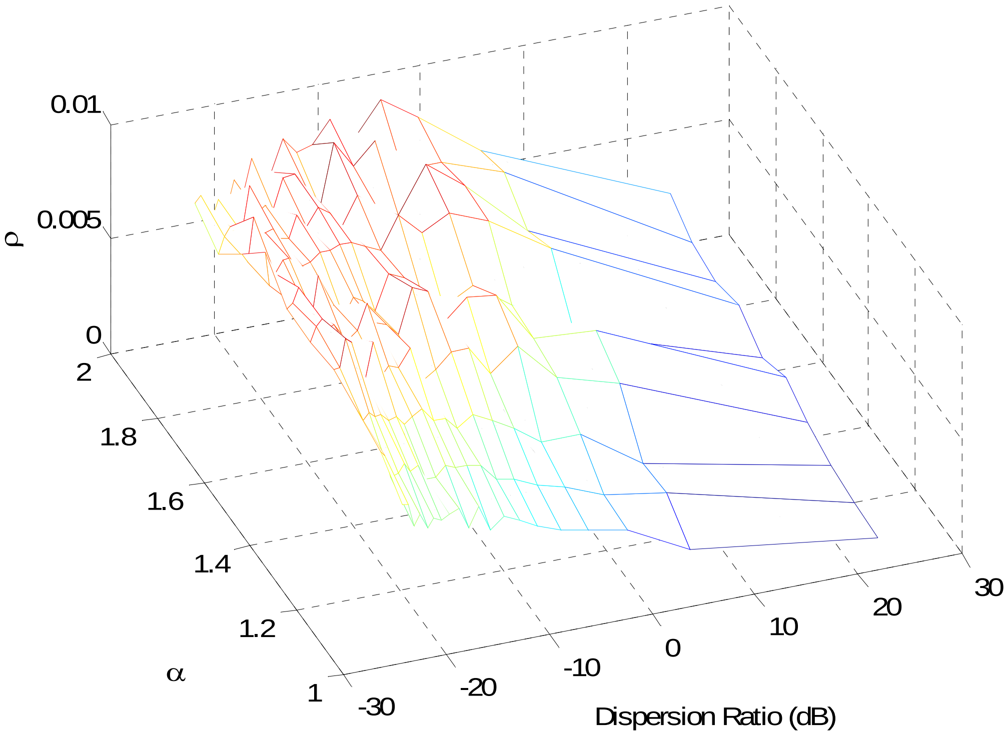

Figure 4.8 Covariation ρ of the stable distribution given in the model 4.23 with respect to α and dispertion ratio (DR) in dB.

In the following Sections, the proposed receiver models for the α-stable density parameter modulated communication system are proposed based on estimating the parameters using the least-squares, the moments and the correntropy methods.

4.2.1 Receiver Model Using Least-Squares Estimation Method

The received signal at time instant $t \in R$ through the AWGN channel is

$$X(t) = X_{S\alpha S}(t) + X_G(t) \tag{4.25}$$

where $X_{S\alpha S}(t)$ is the random carrier, and $X_G(t)$ is the Gaussian noise in the channel.

Although the pdf of the received signal does not exist in analytical form, the characteristic function of the received signal can be analytically written as

$$\varphi(\omega) = \exp\left(-\gamma_{\boldsymbol{S\alpha S}}|\omega|^{\alpha} - \gamma_{\boldsymbol{G}}|\omega|^{2}\right) \tag{4.26}$$

where $\gamma_{S\alpha S} > 0$ and $\gamma_G > 0$ are the dispersions of the SαS and Gaussian signals, respectively. This fact can be easily seen from the characteristic function of the received signal in equation (SαS + S$_G$) which is equal to the multiplication of the characteristic functions of the SαS signal and the channel noise since the density of the received signal is obtained by convolving the density of SαS signal and the density of channel noise:

$$f(x) = f_{\alpha S}(x) * f_G(x) \tag{4.27}$$

$$\varphi(\omega) = \varphi_{\alpha S}(\omega) \cdot \varphi_G(\omega) \tag{4.28}$$

where $f_{\alpha S}(x)$, $f_G(x)$ represent the pdf of αS and Gaussian distributions, respectively. The estimate of the characteristic function could be obtained by empirical characteristic function as given by (Ilow & Hatzinakos, 1998) in Eq. (4.29)

$$\varphi(\omega) = \frac{1}{N}\sum_{k=0}^{N} \exp(-jX(k)\omega) \tag{4.29}$$

Using the closed form expression of the characteristic function given in Eq. (4.26) one can obtain the following relation

$$y \overset{\Delta}{=} -\log|\varphi(\omega)|^2 = 2\gamma_{S\alpha S}|\omega|^\alpha + 2\gamma_G \omega^2 \tag{4.30}$$

The relation given above is nonlinear in α and linear in dispersions. The regression model becomes as

$$\begin{bmatrix} y(\omega_1) \\ \vdots \\ y(\omega_M) \end{bmatrix} = \begin{bmatrix} |\omega_1|^\alpha & |\omega_1|^2 \\ \vdots & \vdots \\ |\omega_M|^\alpha & |\omega_M|^2 \end{bmatrix} \begin{bmatrix} \gamma_{S\alpha S} \\ \gamma_G \end{bmatrix} + \begin{bmatrix} \varepsilon(\omega_1) \\ \vdots \\ \varepsilon(\omega_M) \end{bmatrix} \tag{4.31}$$

where $\varepsilon(\omega)$ is called as residual sum of squares (RSS), (Brcich & Zoubir, 1999) corresponding to the error term. For fixed α, the parameter vector including dispersions $\boldsymbol{\theta} = [\gamma_{S\alpha S} \quad \gamma_G]^{\boldsymbol{T}}$ may be estimated using linear least squares (Kay, 1993a) as follows

$$\hat{\boldsymbol{\theta}} = (\boldsymbol{\omega}^T \boldsymbol{\omega})^{-1} \boldsymbol{\omega}^T \mathbf{y} \tag{4.32}$$

where $\boldsymbol{\omega}$ is the coefficient matrix in Eq. 4.31.

The characteristic exponent which minimizes the estimation error $\left|\hat{\theta}-\theta\right|$ or the norm of the RSS vector $\left\|\varepsilon(\omega)\right\|$ can be chosen as the estimated characteristic exponent of the stable distribution. Figure 4.9 illustrates the variation of the estimation error and RSS norm with respect to α while the actual characteristic exponent is α=1. The magnitude of the RSS has a better performance where $\hat{\alpha}=0.97$ for $\gamma_{G}=0.5$ and $\hat{\alpha}=1.14$ for $\gamma_{G}=1$.

Since the channel noise variance is assumed to be unknown, exact values associated with the parameter vector **θ** is not known. Therefore, the estimated α which minimizes the RSS norm has been used for parameter estimation.

The bit error rate performance of the proposed receiver model has been evaluated for the unipodal α-shift keying transmitter given in Section 4.3.2.

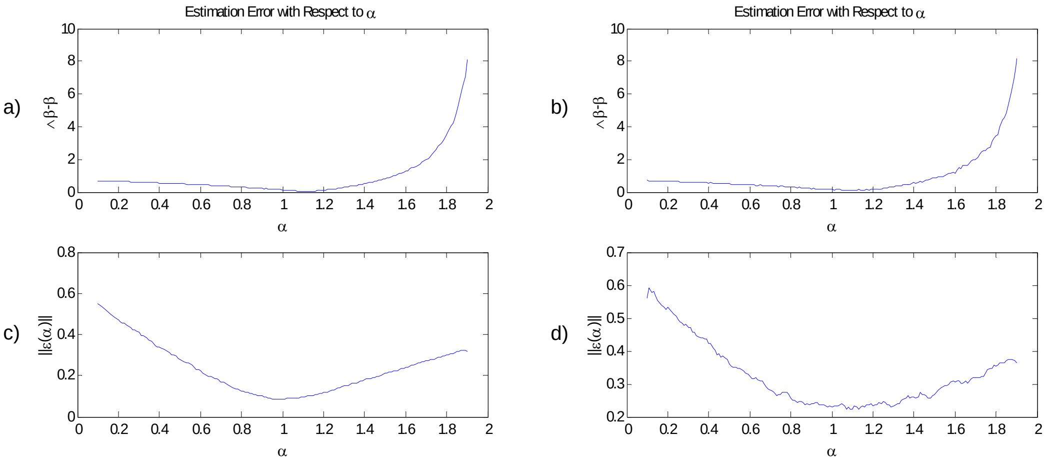

Fig 4.9 The error $\left|\hat{\beta}-\beta\right|$ with respect to the characteristic exponent α; a) $\gamma=1$, $\gamma_{G}=0.5$ b) $\gamma=1, \gamma_{G}=1$; the norm of RSS $\left\|\varepsilon(\omega)\right\|$ with respect to the characteristic exponent α; c) $\gamma=1$, $\gamma_{G}=0.5$ d) $\gamma=1, \gamma_{G}=1$.

4.2.2 Receiver Design Using Moment Type Method

Another empirical characteristic function (ECF) based density parameter estimation method is called as "moment type method". Referring to Eq. 4.26, the estimate of the empirical characteristic function of the received signal is given by (Ilow & Hatzinakos,1998) as below

$$\log|\omega_1| = -\gamma_1|\omega_1|^{\alpha_1} - \gamma_2|\omega_1|^{\alpha_2} \tag{4.33}$$

and

$$\log\left|\frac{1}{\omega_1}\right| = -\gamma_1\left|\frac{1}{\omega_1}\right|^{\alpha_1} - \gamma_2\left|\frac{1}{\omega_1}\right|^{\alpha_2} \tag{4.34}$$

where α_1 is the characteristic exponent of the transmitted signal (random carrier signal) α_2 is the characteristic exponent of the channel noise. Using the estimates of the ECF, the difference of the characteristic exponents $\Delta\alpha = \alpha_2 - \alpha_1$ can be found by solving the following nonlinear equation

$$\frac{\omega_1^{\Delta\alpha} - \omega_2^{\Delta\alpha} + \omega_1^{-\Delta\alpha} - \omega_2^{-\Delta\alpha}}{\omega_3^{\Delta\alpha} - \omega_4^{\Delta\alpha} + \omega_3^{-\Delta\alpha} - \omega_4^{-\Delta\alpha}} = \frac{\log(\hat{\varphi}(\omega_1))\log(\hat{\varphi}(1/\omega_1)) - \log(\hat{\varphi}(\omega_2))\log(\hat{\varphi}(1/\omega_2))}{\log(\hat{\varphi}(\omega_3))\log(\hat{\varphi}(1/\omega_3)) - \log(\hat{\varphi}(\omega_4))\log(\hat{\varphi}(1/\omega_4))} \tag{4.35}$$

Since we have considered the channel noise with Gaussian distribution, then the characteristic exponent of the transmitted signal can be found as $\alpha_1 = 2 - \Delta\alpha$.

Note that the rate of convergence depends on the number of data points *N* and on the values of $\omega_1, \omega_2, \omega_3, \omega_4$. Since the points ω_i and $1/\omega_i$ are both used to estimate the density parameter $\Delta\alpha$ and therefore the values $\omega_1, \cdots, \omega_4$ should be chosen close to 1. Since the standard deviation in the estimation of characteristic exponent $\Delta\alpha$ is large (Ilow & Hatzinakos, 1998) then we have not preferred this type of estimation otherwise satisfactory bit error rate performance would not be achieved.

4.2.3 Correntropy Based Receiver Design

Correntropy is a similarity measure between two random variables X and Y incorporating second and higher order moments of the random variable $X-Y$ (Liu et. al., 2007), (Jeong et.al., 2009). This similarity measure gives the correlation between these variables therefore it is also called as Generalized Correlation Function (Santamaria et. al., 2006). The correntropy function is defined as below

$$V(X,Y)=E[\kappa_\sigma(X-Y)] \tag{4.36}$$

where E is the mathematical expectation and κ_σ is the Gaussian kernel given by

$$\kappa_\sigma(X-Y)=\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{\|X-Y\|^2}{2\sigma^2}\right) \tag{4.37}$$

In practice, the correntropy is computed from the finite observations with the length *N*=5000, therefore the sample estimator of correntropy can be expressed as (Liu et. al., 2007)

$$\hat{V}_{N,\sigma}(X,Y)=\frac{1}{N}\sum_{n=1}^{N}\kappa_\sigma(X_n-Y_n) \tag{4.38}$$

Considering a discrete-time strictly stationary stochastic process, the auto-correntropy function (Santamaria et. al., 2006) can be found as

$$\hat{V}[m]=\frac{1}{N-m+1}\sum_{n=m}^{N}\kappa(x_n-x_{n-m}) \tag{4.39}$$

Using Taylor series expansion for the Gaussian Kernel, it can be defined as a type of metric expressed by a kernel function (Santamaria et. al., 2006)

$$V(t_1,t_2)=\frac{1}{\sqrt{2\pi}\sigma}\sum_{n=0}^{\infty}\frac{(-1)^n}{2^n\sigma^{2n}n!}E\left[\left\|x_{t_1}-x_{t_2}\right\|\right]^{2n}\ . \tag{4.40}$$

Since the stable distributions have infinite higher order moment greater than α, Gaussian kernel may not be a proper candidate to measure the auto-correntropy. The function including fractional lower order moments has been used for the estimation of the auto-correntropy of x_n given by

$$\hat{V}[m]=\frac{1}{N-m+1}\sum_{n=m}^{N}\left|x_n-x_{n-m}\right|^p \tag{4.41}$$

where $x_n \sim S_\alpha(\gamma,0,0)$ and $p < \alpha$.

The simulations given in Figure 4.10 and 4.11 have been performed by 50 realization of stable distributions with the length of $N = 5000$ points. It can be seen in Figure 4.10 that while α decreases (i.e., impulsiveness increases), the deviation associated with the median of the auto-correntropy also decreases and there is not any significant overlap between the median auto-correntropy values for different characteristic exponents. Thus, one can specify a threshold for the auto-correntropy of the received signal for deciding the characteristic exponent of the transmitted signal. In order to specify this threshold, the maximum and minimum values of the auto-correntropy over the realizations are illustrated in Figure 4.11. Choosing closer α values to encode the binary information in the transmitted signal may cause poor BER performance because Gaussian channel noise will increase the auto-correntropy values and the deviation of the median of the auto-correntropy of the received signal over a certain number of realizations will also increase when α of the random carrier is increased. Therefore in order to obtain a satisfactory BER performance in the receiver low α values for the transmitted noise signal should be chosen. However, if the security in communication is desired, higher α values for the carrier signals should be chosen for trading-off satisfactory BER performance.

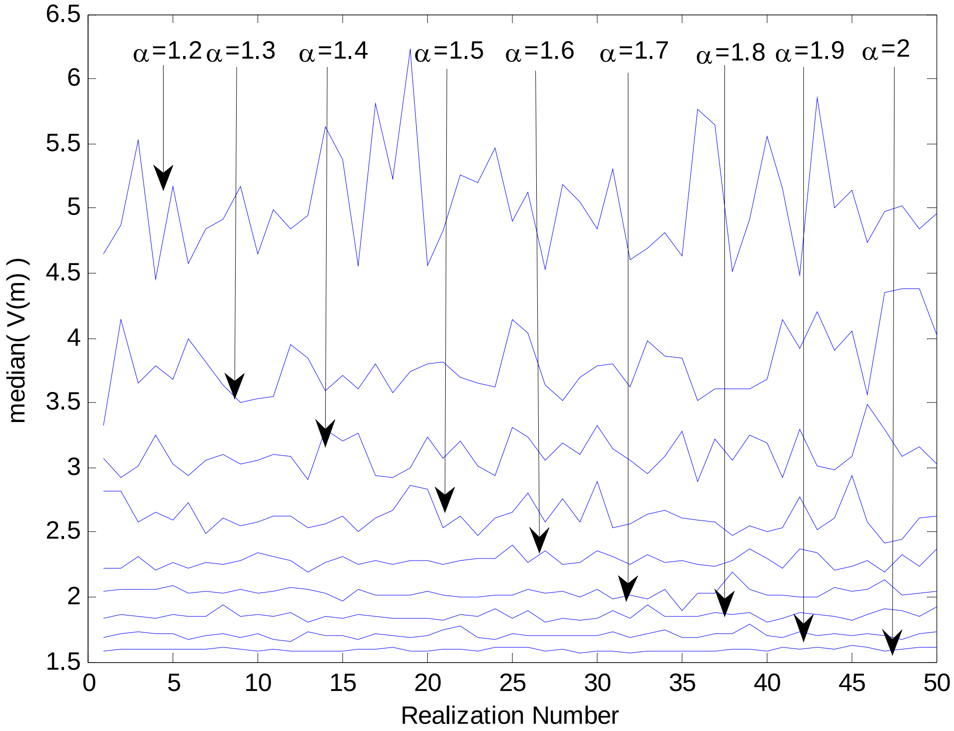

Fig 4.10 The median of auto-correntropy function expressed in Eq. 4.41.

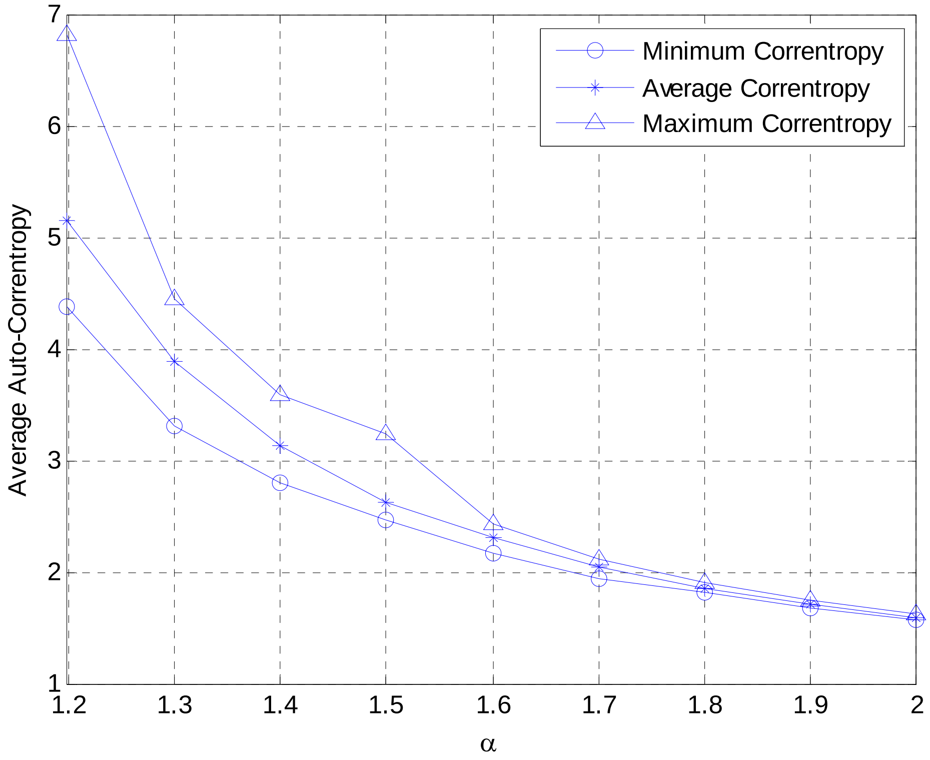

Fig 4.11 The average, maximum and minimum values associated with the median of the auto-correntropy function for 100 realizations.

4.2.4 Receiver Design Using Fractional Lower Order Moment Method

In this Section, the receiver model based on estimating the parameters of the characteristic function of the stable distribution function which uses the fractional lower order moment (FLOM) described in (Kuruoglu, 2001) has been proposed. Using the set of observations $x(k),\ k = 1,2,...,T_b$, where the length of the data is denoted as T_b, the estimate of the characteristic exponent has been evaluated by the sinc estimator (Kuruoglu, 2001) as formulated below

$$\hat{\alpha} = \arg\min_{\alpha} \left| sinc\left(\frac{p\pi}{\alpha}\right) - \left[\frac{p\pi}{2}\left(\frac{A_p \cdot A_{-p}}{\tan\frac{p\pi}{2}}\right) + S_p \cdot S_{-p} \tan\frac{p\pi}{2}\right]^{-1}\right| \tag{4.42}$$

where p is the fractional moment order $0 < p < \alpha$, T_b is the number of samples for each message bit and the absolute fractional moments A_p and signed fractional moment S_p are given by Eq. (4.43) and (4.44), respectively.

$$A_p = \frac{1}{N}\sum_{k=1}^{T_b} |x(k)|^p, \tag{4.43}$$

$$S_p = \frac{1}{N}\sum_{k=1}^{T_b} sign(x(k)) \cdot |x(k)|^p\ . \tag{4.44}$$

Once the estimate of the characteristic exponent $\hat{\alpha}$ has been computed above, the estimate of the skewness parameter β can be obtained by solving φ from the ratio estimator (Kuruoglu, 2001) as

$$S_p / A_p = \tan\left(\frac{p\varphi}{\hat{\alpha}}\right) \Big/ \tan\left(\frac{p\pi}{2}\right) \tag{4.45}$$

After computing the estimate of φ, the skewness parameter β can be obtained as below

$$\hat{\beta} = \frac{\tan(\varphi)}{\tan\left(\frac{\alpha\pi}{2}\right)} \tag{4.46}$$

A detailed analysis of the alternative methods for computing β is explained in (Kuruoglu, 2001). The consistency of the method has been compared by extreme value method (EVM) given in (Tsihrintzis & Nikias, 1996). This method divides the observed SαS distributed random signal with the length N into L non-overlapping segments as $\mathbf{X} = [x_1 \quad x_2 \quad \cdots \quad x_N] = [\mathbf{X}_1 \quad \mathbf{X}_2 \quad \cdots \quad \mathbf{X}_L]$ and then estimates the characteristic exponent α as given below

$$\hat{\alpha} = \frac{\pi}{2\sqrt{6}}\left(\frac{1}{\bar{s}} + \frac{1}{\underline{s}}\right) \tag{4.47}$$

where the terms $\bar{s}$ and $\underline{s}$ are

$$\bar{s} = \sqrt{\frac{1}{L-1}\sum_{l=1}^{L}(\bar{x}_l - \bar{x})}; \qquad \bar{x} = \frac{1}{L}\sum_{l=1}^{L}\bar{x}_l \tag{4.48}$$

$$\underline{s} = \sqrt{\frac{1}{L-1}\sum_{l=1}^{L}(\underline{x}_l - \underline{x})}; \qquad \underline{x} = \frac{1}{L}\sum_{l=1}^{L}\underline{x}_l \tag{4.49}$$

and $\bar{x}_l = \log(\max(\mathbf{X}_l))$, $\underline{x_l} = -\log(\min(-\mathbf{X}_l))$.

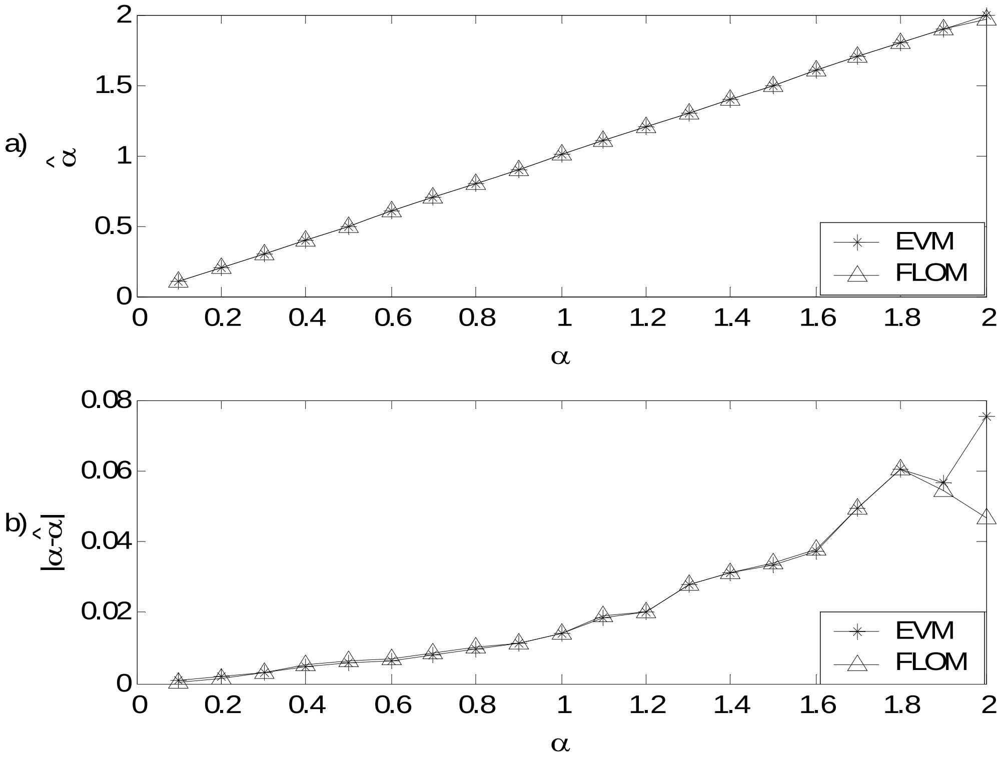

Figure 4.12 Comparison of Extreme Value Method (EVM) and FLOM Method for SαS random variables a) Mean value of the estimated α b) The standard deviation of estimation error with respect to α.

Figure 4.12 illustrates the estimation accuracy of the extreme value method (EVM) and fractional lower order moment method (FLOM). Note that while α is increasing, the standard deviation between the estimated value and the actual value of the characteristic exponent increases. One can conclude that selection of higher α values for parameter modulation may cause increased estimation error. Therefore small α values should be chosen and more distant α values provide appropriate threshold.

Since the binary message can be coded not only by the characteristic exponent but also using the skewness parameter, the density parameter estimation method by FLOM have been used for a receiver design in the proposed communication schemes explained in the following Section.

4.3 Transmitter Model Using α-Stable Distributed Noise Parameter Modulation In Digital Communication

In this Section, differing from the conventional spread-spectrum systems which use deterministic signals as a carrier signal, instead, α-stable distributions are used as a random carrier in the newly proposed random communication system: a random signal with α-stable distribution which carries the digital information is sent through the additive white Gaussian noise (AWGN) channel. Since the parameters of α-stable distributions are used to code the digital information then the random signal acts as carrier and therefore a random signal is called as a random carrier.

In the following Sections, the bit error rate performance analysis of each receiver models in AWGN channel will be given for each proposed transmitter model.

4.3.1 α-Stable ON-OFF Keying

The first approach on the random digital communication using SαS distributions is based on the α-Stable ON-OFF keying. In this communication scheme, the message bit is encoded by the characteristic exponent α where the stable noise samples x_k $k = 1,\cdots,T_b$ are drawn from the distribution $S_\alpha(1,0,0)$ during the bit length T_b if the n^{th} message bit to be sent is "0" and any random signal is not sent if the n^{th} message bit of the binary message sequence m is equal to "1".

The modulation rule can be expressed as below

$$x_k \sim \begin{cases} 0 & \text{if } m(nT_b) = 1 \\ S_\alpha(1,0,0) & \text{if } m(nT_b) = 0 \end{cases} \tag{4.50}$$

where, $k = nT_b + 1,\cdots,nT_b + T_b$ and n=0,1,….

The critical point is to determine the proper threshold at the receiver. There is not any analytical approach for the selection of threshold. According to the modulation rule defined in Eq. 4.50, the receiver observes only Gaussian noise signal existing in the channel if the message bit to be sent is "1". Since the estimation error of characteristic exponent increases when α increases, then the threshold should be chosen distant from the characteristic exponent of Gaussian noise in the channel i.e., 2. When the channel noise variance increases, then the characteristic exponent of the received signal also increases. The characteristic exponent associated with the sum of stable random variable with a Gaussian random variable gets near to 2. Therefore the threshold should be chosen as relatively near but bigger then the characteristic exponent of the SαS distribution.

The bit Error Rate (BER) performance given in Figure 4.13 has been realized over 10000 bits with a length T_b=10000 point which is sufficient to recover the characteristic exponent parameter from the observation.

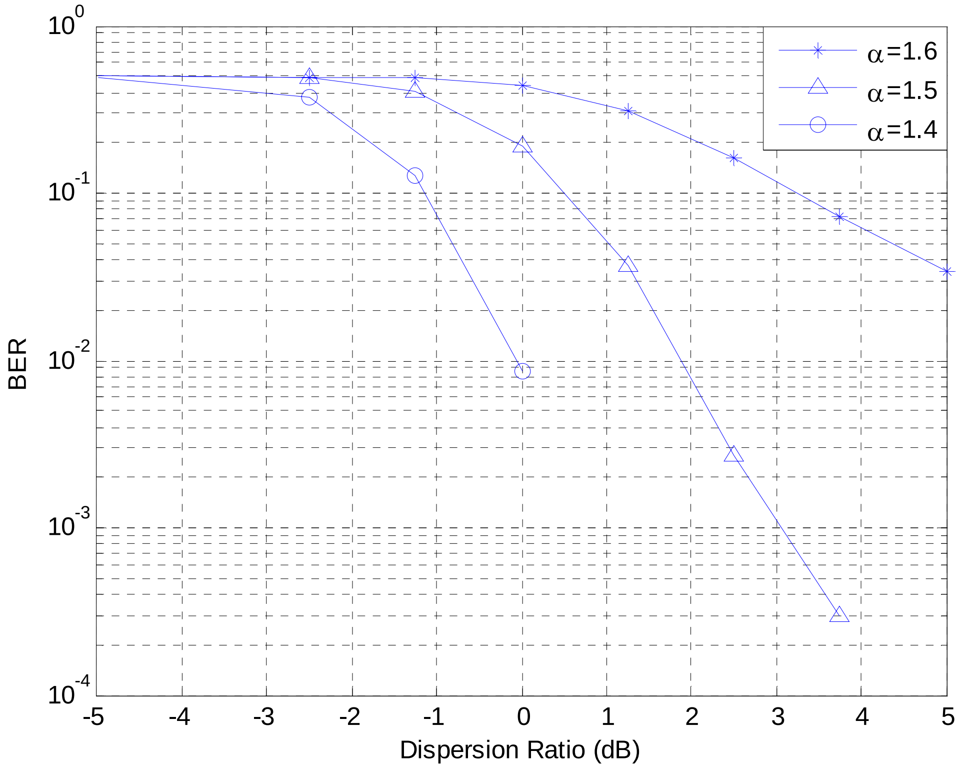

Figure 4.13 Bit error rate performance of the α-stable ON-OFF keying communication scheme with respect to the different characteristic exponents. The threshold has been chosen as 1.7.

The BER results show that when more impulsive random signal is chosen to modulate the binary information, then BER performance is improved. The advantage of this method is that the less energy is consumed since the random signal is sent from the transmitter only for the binary message “0”.

4.3.2 Unipodal α-Stable Keying

The second proposed communication scheme is called as unipodal α-stable keying whose block diagram is shown in Figure 4.14. Similarly, this communication scheme also uses SαS random signals at the transmitter. Differing from the previous method both of the binary message bits are modulated with the random signals which have different characteristic exponents α_1, α_2<2.

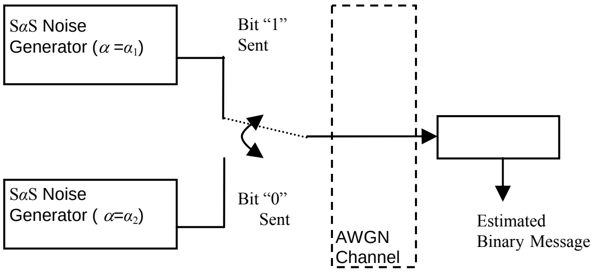

Figure 4.14 Block diagram of the proposed unipodal α-stable keying communication scheme

During the bit length T$_b$ the samples x_k, $k = 1,\cdots T_b$ are drawn from a probability density "$S_{\alpha_i}(1,0,0)$" i=1, (respectively i=2) if $m(nT_b) = 1$ (respectively $m(nT_b) = 0$) i.e.,

$$x_k \sim \begin{cases} S_{\alpha_1}(1,0,0) & \textit{if } m(nT_b) = 1 \\ S_{\alpha_2}(1,0,0) & \textit{if } m(nT_b) = 0 \end{cases} \tag{4.51}$$

where $k = nT_b + 1,\cdots,nT_b + T_b$ and n=0,1,….

As an illustrative example, the message sequence and the corresponding stable distributed signal are shown in Figure 4.15a and Figure 4.15b, respectively. The bit duration is T$_b$=10^4 and the characteristic exponents have been chosen as α_1=1, α_2=0.5. Due to the high impulsive behavior of the signal with α_2=0.5, the signal having characteristic exponent α$_1$=1 can not be observed clearly. This indicates that the characteristic exponents should be chosen near to each other to provide security.

The BER performances of unipodal α-shift keying have been performed by density parameter estimation method described by (Kuruoglu, 2001) given in Section 4.2.4 and the least squares estimation method described by (Brcich & Zoubir, 1999) given in Section 4.2.1.

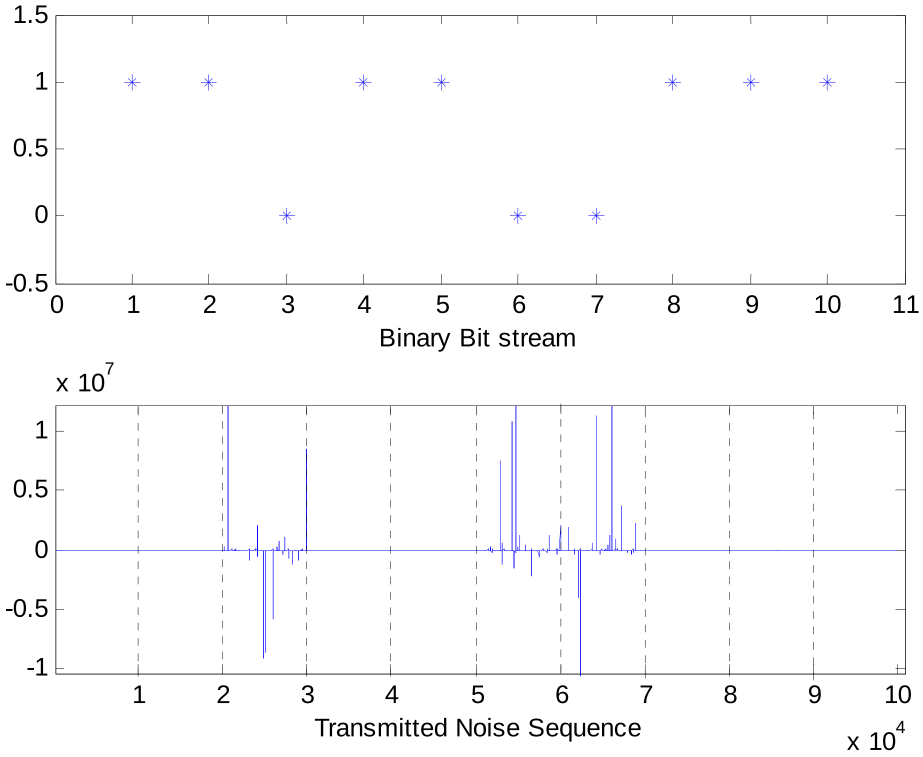

Figure 4.15 a) The message bit stream. b)Transmitted noise sequence.

Figure 4.16 gives the BER performance of the unipodal α-shift keying using the method given by (Kuruoglu, 2001). The simulation has been performed through 10000 bit where each bit has length 10000 points. It is shown that when the characteristic exponents of the random carriers α_1 and α_2 are chosen far from each other then the error probability decreases, as expected.

In order to maintain the security without reducing the BER performance, one should choose both α_1, α_2 near to each other but far from the characteristic exponent of the Gaussian, i.e., 2.

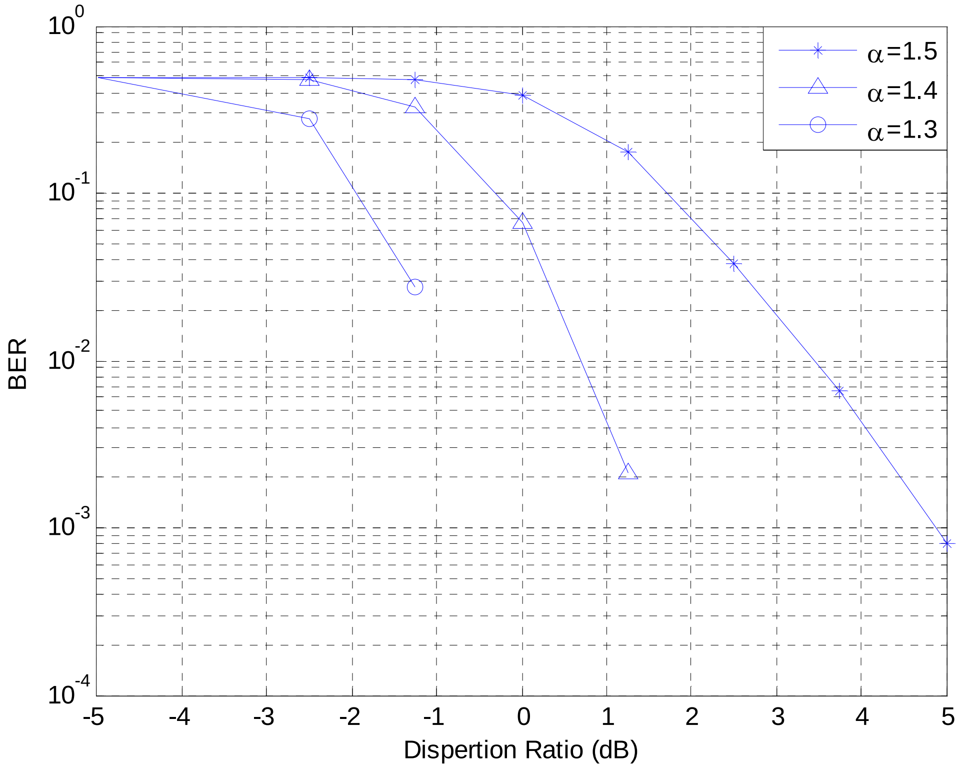

Figure 4.16 BER performance for unipodal α-stable shift keying, α_1=1.85. with the threshold = 1.65

The second method representing BER performance using the parameter estimation described in Section 4.2.1 is shown in Figure 4.17. Due to computational complexities and consuming very long simulation time, the random signal length could be chosen maximum T_b=5000 points and the BER simulation could be performed by 1000 bits. Compared to the density parameter estimation method, the reduced data length causes the estimation accuracy to become poorer even when the dispertion ratio is relatively high. It is observed that this method gives an unsatisfactory BER performance. However, the BER performance of the method is satisfactory for low values of α, while sacrificing for security.

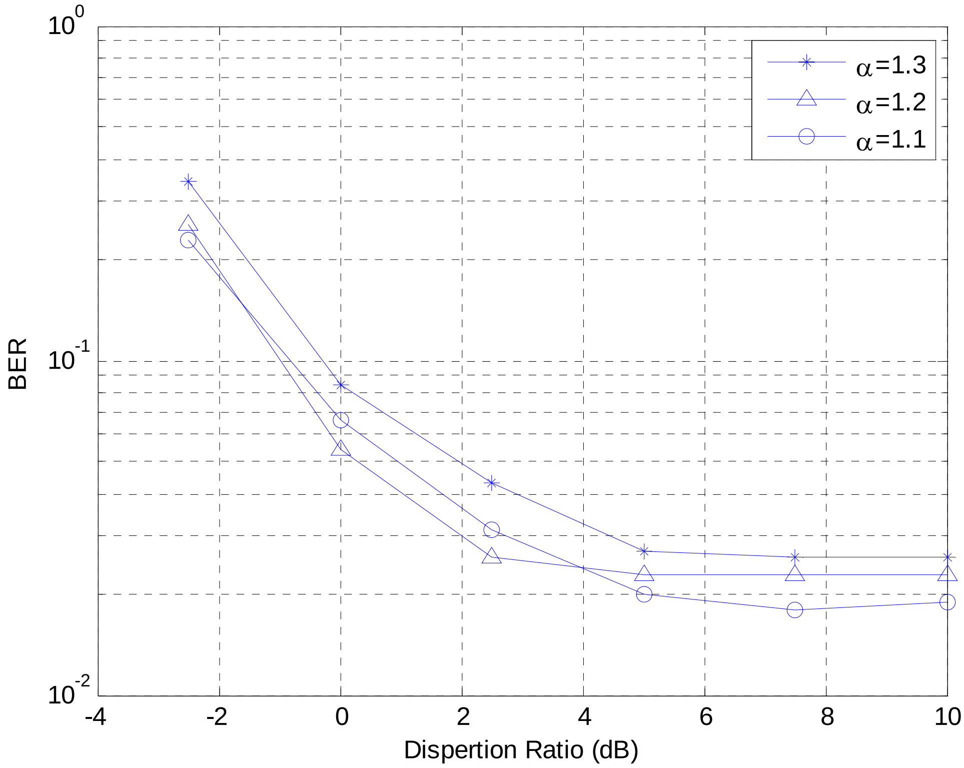

Figure 4.17 BER performance of the least-square based parameter estimation based receiver. α_1=1.6 and the threshold has been taken as 1.45.

The BER performance of the unipodal α-shift keying with correntropy-based receiver is given in Figure. 4.18. It can be seen that the performance of the correntropy based receiver becomes saturated near 5 dB and gives a restricted error performance. The signal length could be chosen as maximum 5000 points due to the computational restrictions. This caused to observe more deviative results. Therefore, one can say that correntropy based receiver needs to be improved about threshold selections about the correntropy values and binary clustering.

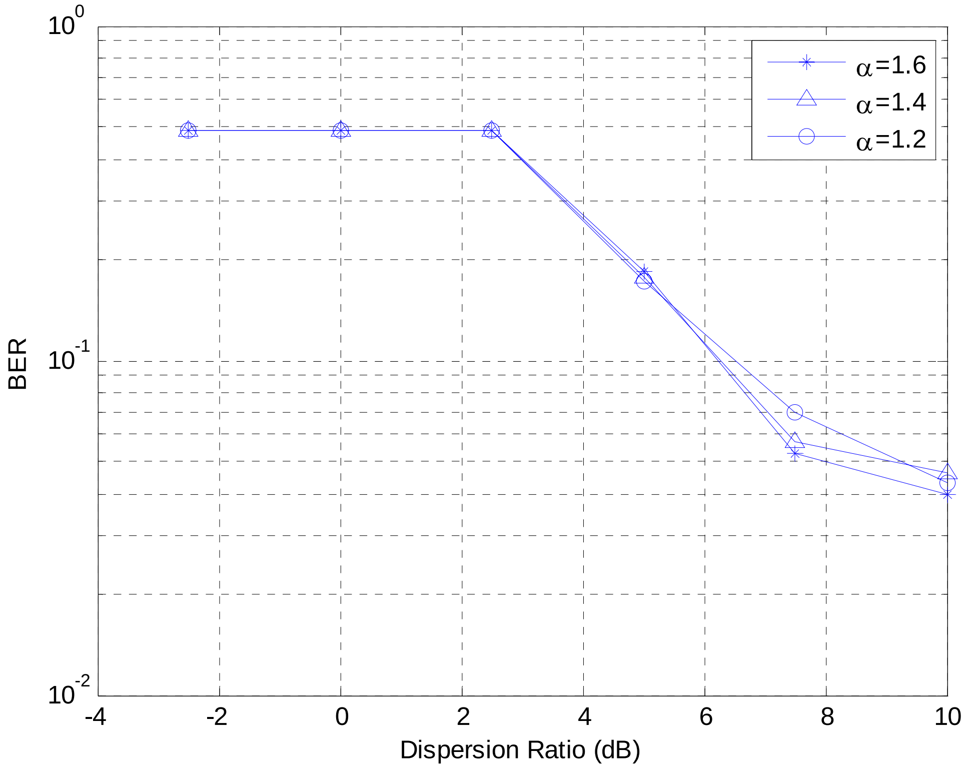

Figure 4.18 BER performance of the correntropy based parameter estimation based receiver. α_1=1.8 and the threshold has been taken as 1.65.

4.3.3 Antipodal α-Stable Keying

In this proposed communication scheme, while the characteristic exponent α is kept constant the skewness parameter β is used to modulate the binary information. The block diagram of the proposed communication scheme is given in Figure 4.19.

During the bit length T$_b$ the samples x_k produced by the transmitter, $k = 1,\cdots T_b$ are expressed as

$$x_k \sim \begin{cases} S_\alpha(1,\beta,0) & if\ m(nT_b)=1 \\ S_\alpha(1,-\beta,0) & if\ m(nT_b)=0 \end{cases} \tag{4.52}$$

where $k = nT_b + 1,\cdots,nT_b + T_b$ and n=0,1,….

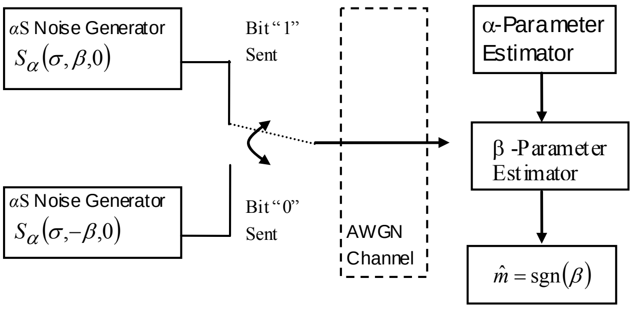

Figure 4.19 Block diagram of digital communication scheme based on skewed α-stable distributions.

The Gaussian noise in the channel will cause the deviation in the true value of the characteristic exponent and since the skewness parameter will also be estimated by using the estimated characteristic exponent by the method given in (Kuruoglu, 2001) then the deviation in the true value of the skewness parameter will also occur. But, since in the receiver, the message bit is estimated according to the sign of the estimated skewness parameter therefore by proper thresholding, a satisfactory BER performance is obtained and this proposed scheme is more robust to the errors in the estimations. In Figure 4.20, the BER performance is shown with respect to the different characteristic exponent values. It can be clearly seen that the BER performance increases by decreasing the characteristic exponent of the random carrier while keeping the skewness parameter constant.

The Figure 4.21 illustrates that the selection of more skewed distribution will improve the BER performance while the characteristic exponents are kept constant. This is because the convolution of the transmitted random signal with the skewed stable distribution and the Gaussian noise in the channel results in the more symmetrized and the less skewed distribution at the receiver.

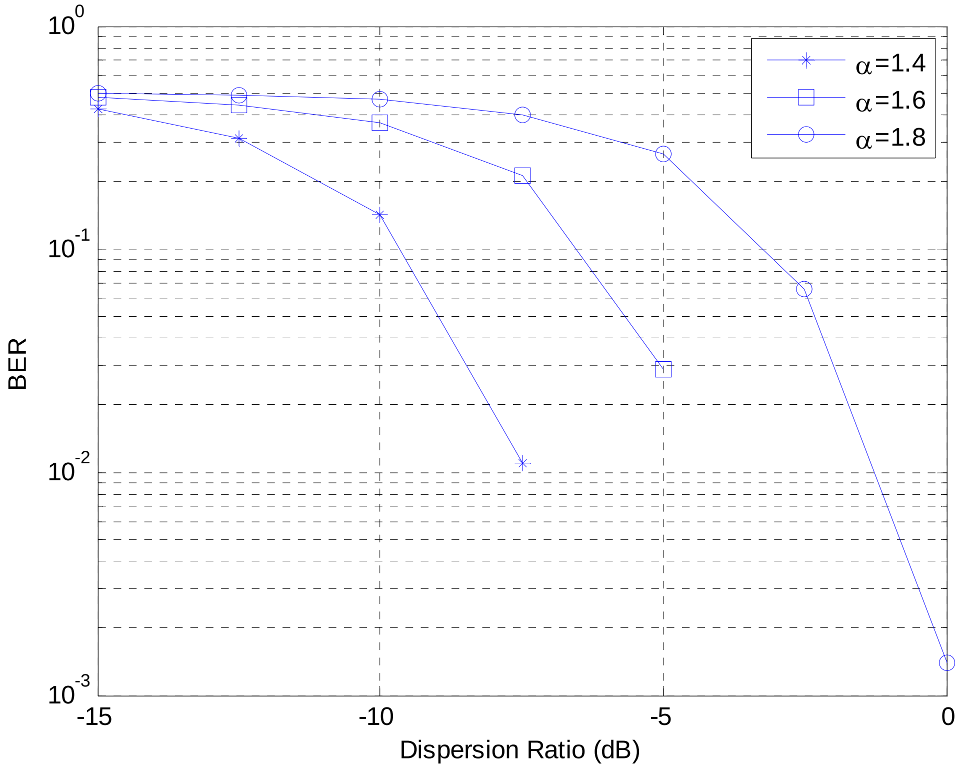

Figure 4.20 BER performance for Antipodal α-stable shift keying, β=0.7.

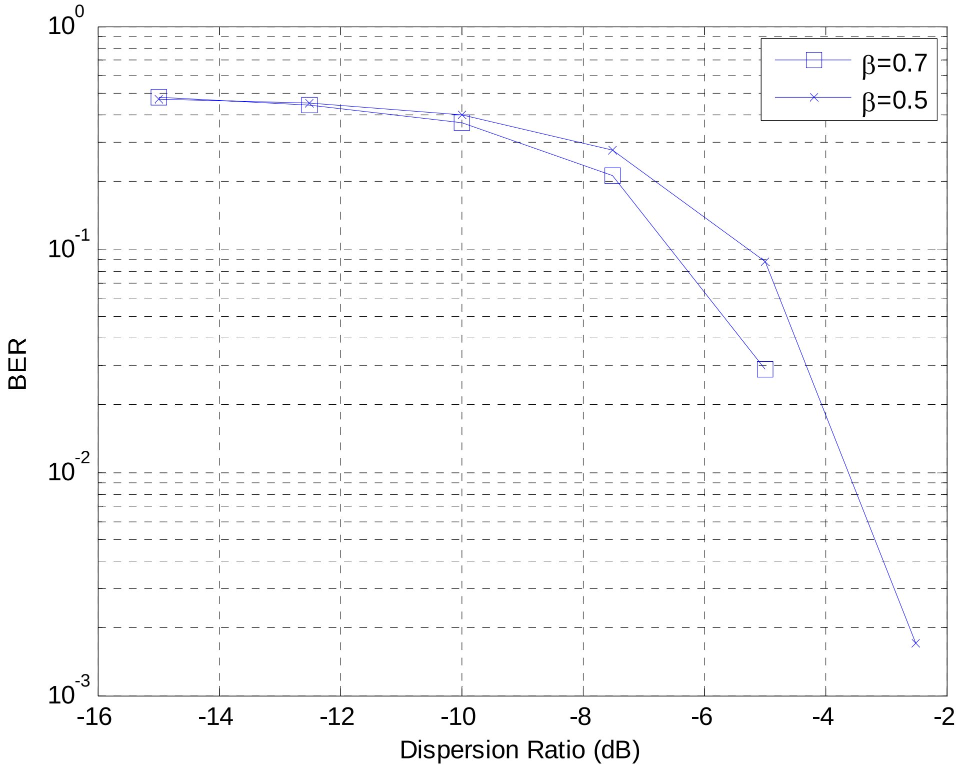

Figure 4.21 BER performance for Antipodal α-stable shift keying, α=1.6.

4.3.4 Quadrature *α-Stable Keying*

In Sections 4.3.1 - 4.3.3 either the characteristic exponents or the skewness parameter have been used for the coding in the proposed random communication systems. In this Section, both the characteristic exponent and the skewness parameter have been used to modulate the binary information. By the two parameters of a stable random carrier, two message bits are encoded, thus, the twice data transmission rate is obtained. In the receiver, the density parameter estimation method given by (Kuruoglu, 2001) has been applied since β parameter is estimated by using the estimated α parameter therefore the two stage estimation procedure is applied for each bit pair. The block diagram of the proposed communication scheme is shown in Figure 4.22.

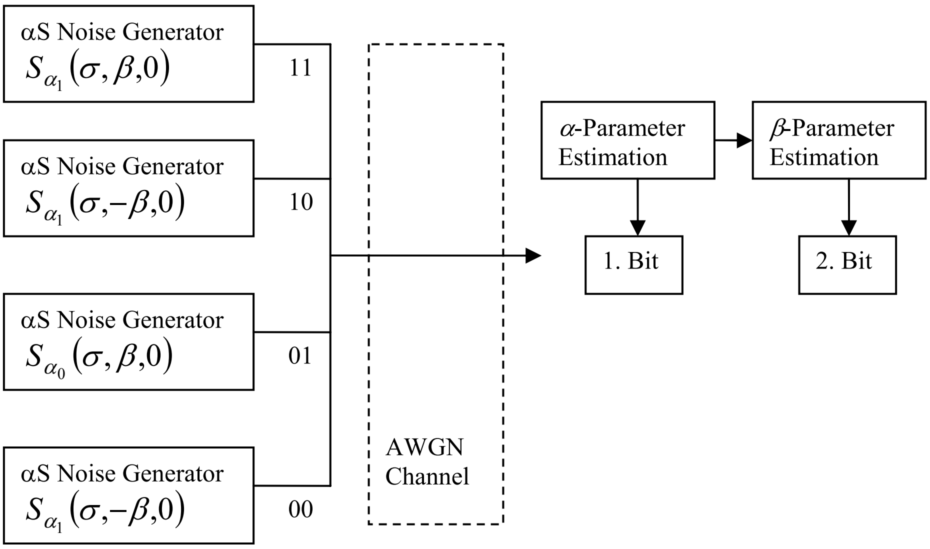

Figure 4.22 The block diagram of the quadrature α-stable keying communication scheme.

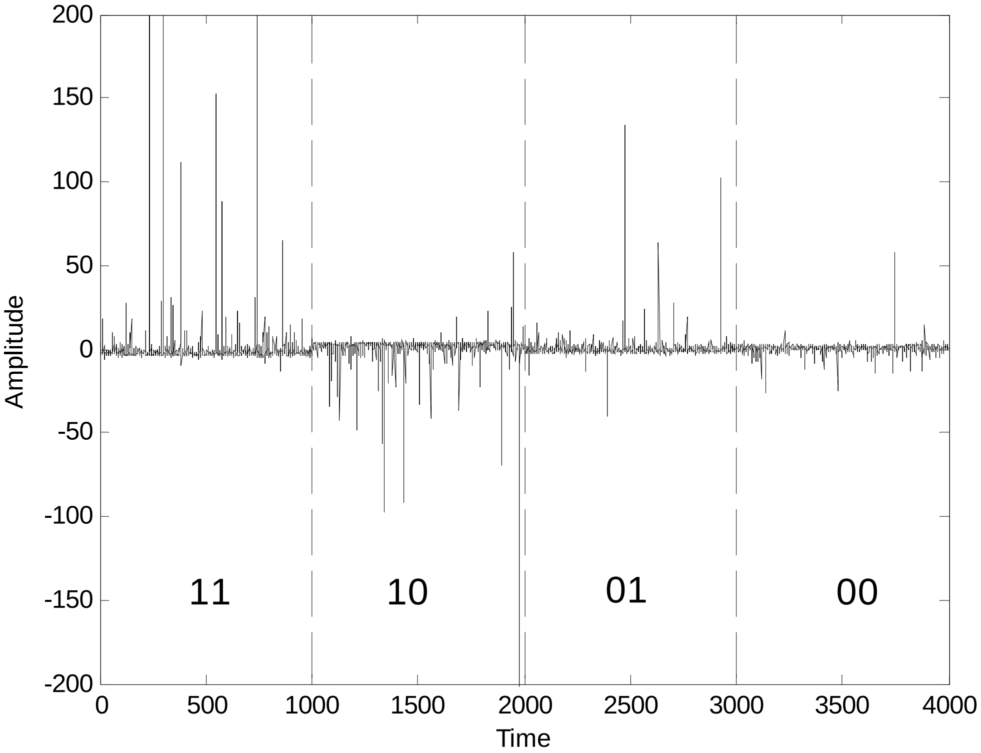

Figure 4.23 A realization of random signal for each message bit pair. $\alpha_1 = 1.2, \alpha_0 = 1.5$ and $\beta = 0.9$.

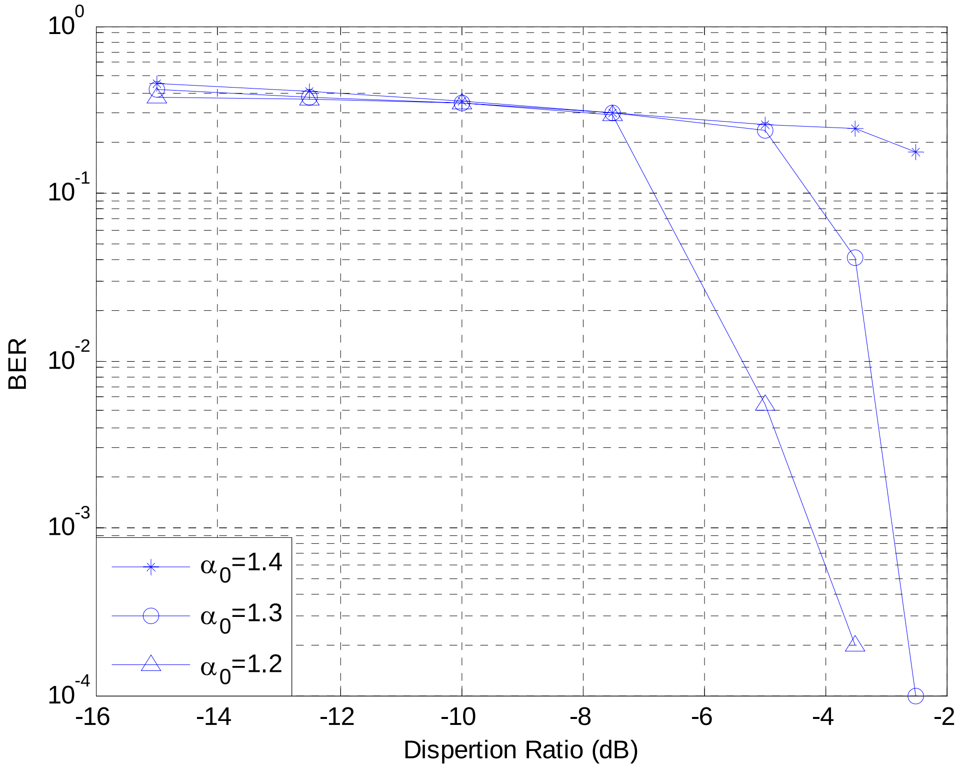

Figure 4.24 The BER performance of the quadrature α-stable keying communication scheme with α_1=1.7, β=0.9 and the threshold 1.65.

As an illustration, a realization of the time domain signal for each bit pair is represented in Figure 4.23. The BER performance of the communication scheme is shown in terms of the variations of α_0 , α_1 and β parameters of the random carriers in Figure 4.24 and Figure 4.25, respectively.

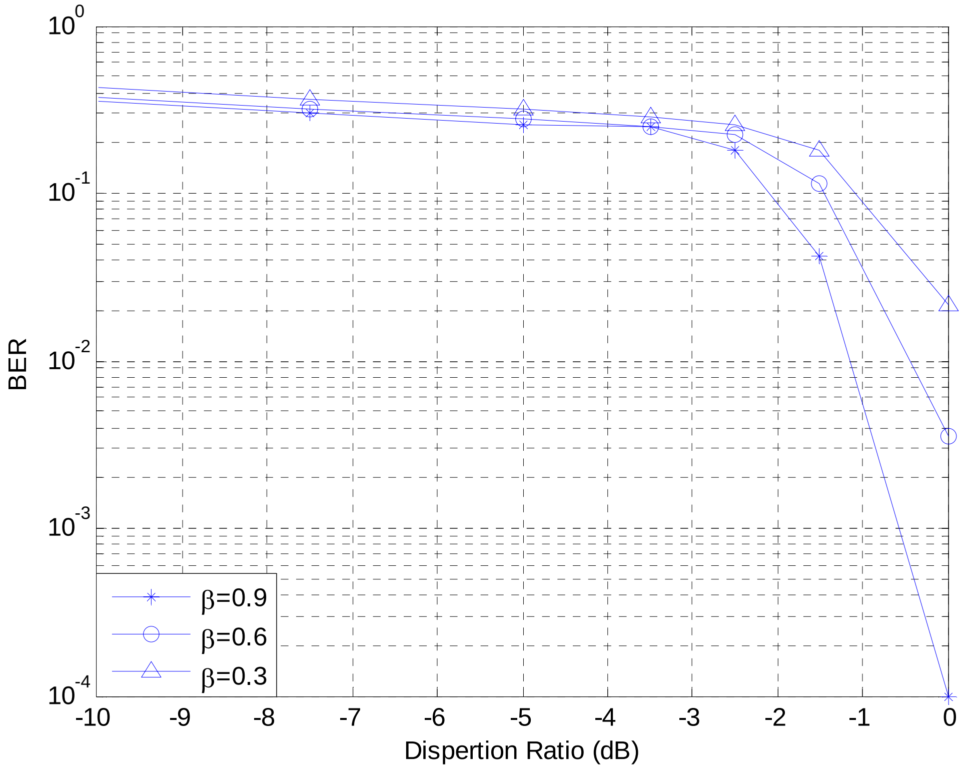

Figure 4.25 The block diagram of the quadrature α-stable keying communication scheme α_1=1.7, α_0=1.5 and threshold = 1.65.

When compared with the BER performances of the communication schemes proposed in the previous Sections, it can be seen that in order to obtain the same BER performance, modulation with low characteristic exponent values (i.e., more impulsive random carrier) is done at the expense of more energy consumption in the transmitter and losing security. Since for the skewed distributions, the estimate of the characteristic exponent is more erroneous in limited number of samples. Therefore in order to estimate the first message bit depending on the characteristic exponent correctly the number of samples should be increased.

BER performance is more sensitive to the threshold values of the characteristic exponent compared to threshold values of the skewness parameter of the random carrier since the sign of the skewness parameter decides the true message bit, not the true value of the skewness parameter.

In spite of its poor performance by the quadrature α-stable keying twice the data transmission rate is achieved.

4.3.5 Antipodal α-Stable Keying With Random Parameter

In the previous Sections, different types of α-stable noise parameter modulation based digital communication schemes have been given. In this Section, in the transmitter side, instead of choosing the parameter of the α-stable distribution deterministically, the noise parameters have been chosen from uniform distribution to encode the binary information. The application of random parameter modulation has been applied for antipodal α-stable shift keying transmitter type.

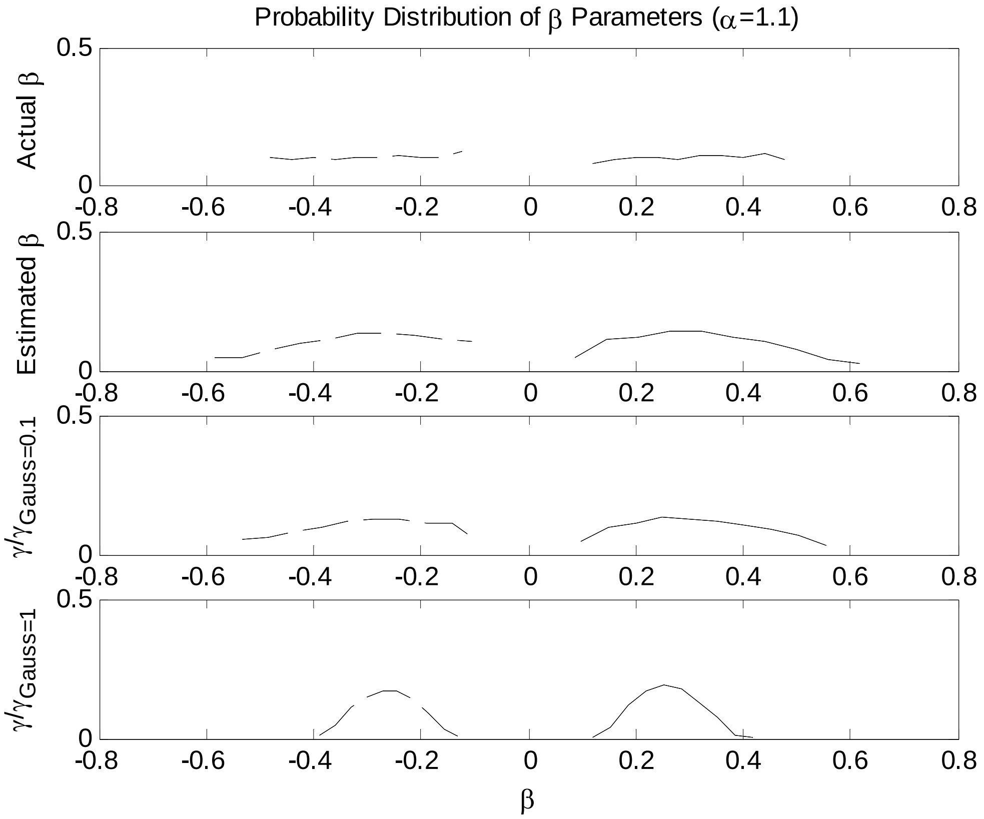

Figure 4.26 The distribution of the skewness parameter *β* for different dispersion ratios (α=1.1).

In order to illustrate experimentally, 100 realizations of skewed α-stable noise signal having α=1.1, $\beta \in \boldsymbol{U}[0.1 \quad 0.5]$ and $\beta \in \boldsymbol{U}[-0.1 \quad -0.5]$ has been transmitted through the channel with no-noise case and with dispersion ratios 0.1 and 1, respectively. The distributions corresponding to actual and estimated values of β are shown Figure 4.26. The same experiment has been repeated with α=1.5 and the results are given in Figure 4.27.

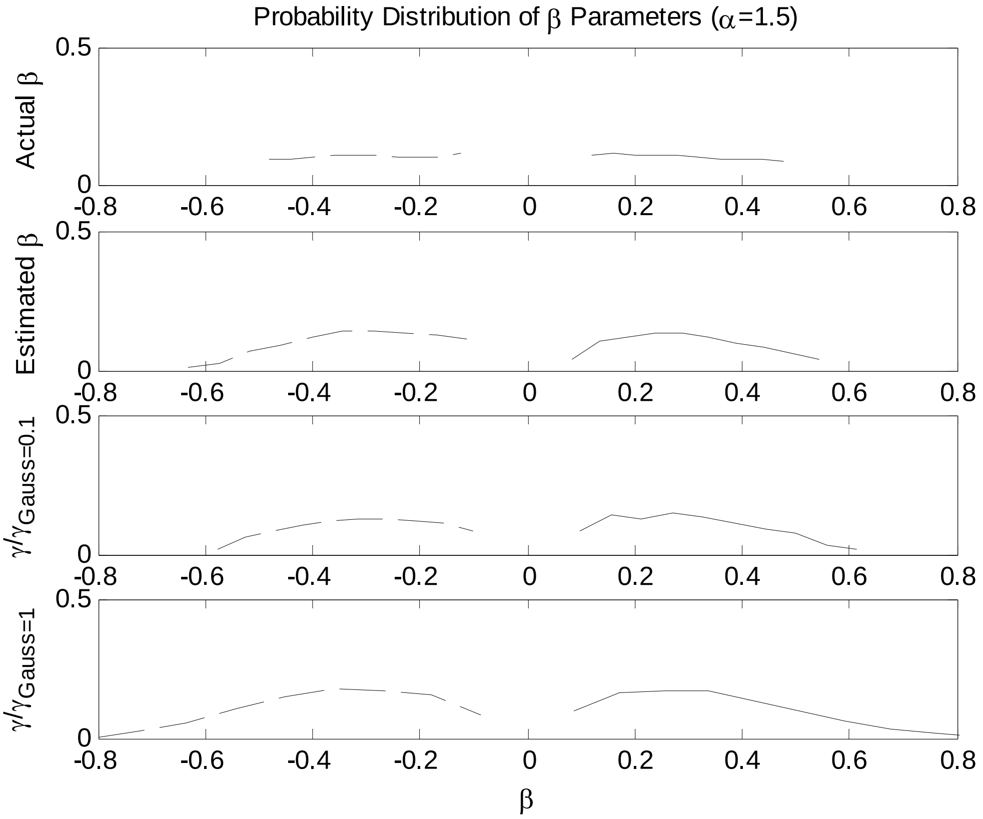

Figure 4.27 The distribution of the skewness parameter β for different dispersion ratios (α=1.5).

One can conclude that even though the estimation of β becomes erroneous under Gaussian noise contamination and while α increases, the estimated β does not change its sign so that receiver can estimate the message bit without an error. Hence, antipodal α-shift keying communication scheme can also be proposed by selection of β from a specified distribution.

During the bit length T$_b$ the samples x_k produced by the transmitter, $k = 1,\cdots T_b$ are expressed as

$$x_k \sim \begin{cases} S_\alpha(1,\beta,0) & \text{if } m(nT_b) = 1 \\ S_\alpha(1,-\beta,0) & \text{if } m(nT_b) = 0 \end{cases} \tag{4.53}$$

where $k = nT_b + 1,\cdots,nT_b + T_b$, $\beta \in U[0.5 \quad 0.9]$, $-\beta \in U[-0.5 \quad -0.9]$, U denotes the uniform distribution and n=0,1,….

The BER performance of this communication scheme is given in Figure 4.28 and Figure 4.29.

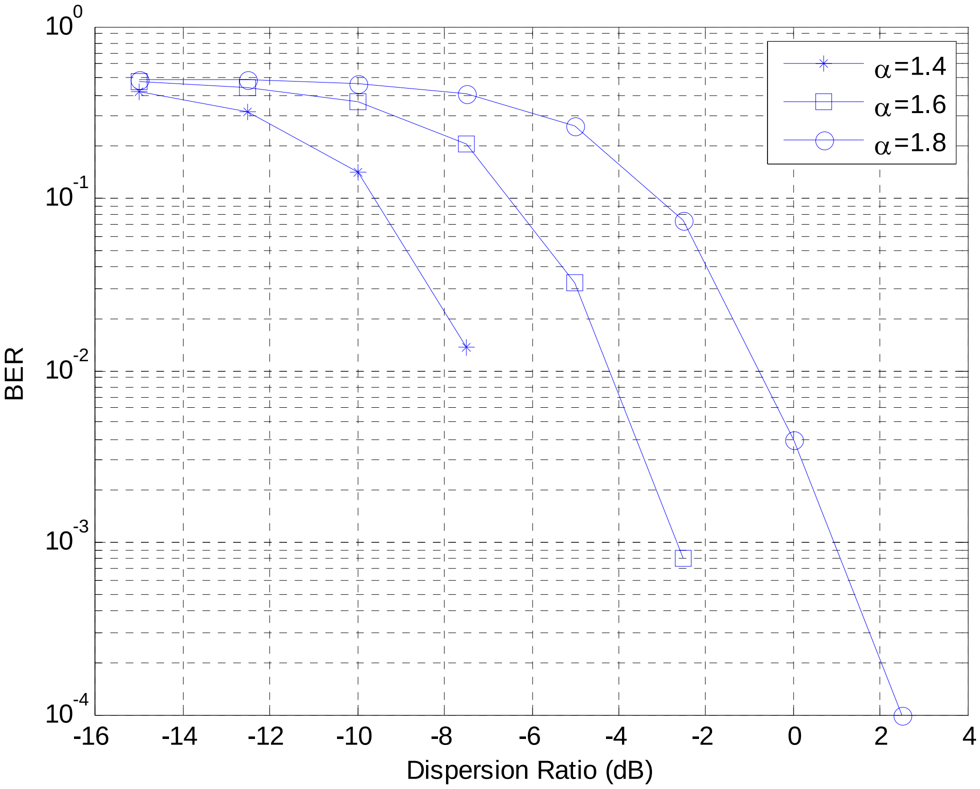

Figure 4.28 The BER performance for antipodal α-keying with random parameters $\beta \in \boldsymbol{U}[0.5 \quad 0.9]$.

It can be observed that almost the same estimation performance compared with the antipodal α-shift keying with constant parameter modulation could be achieved by this proposed communication scheme.

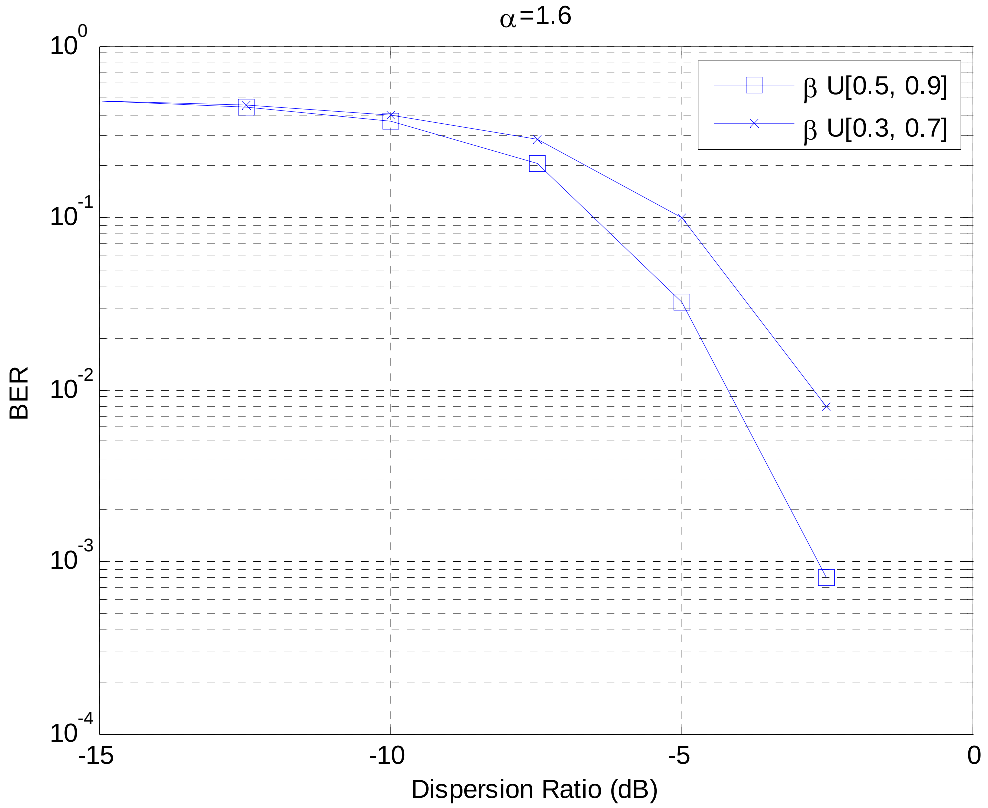

Figure 4.29 The BER performance for antipodal α-keying with random parameters (α=1.6).

4.4 Detection of α-Stable Distributed Signals in White Gaussian Noise

In this Section, the detection probabilities of symmetric α-Stable (SαS) and skewed α-stable distributions in additive white Gaussian noise (AWGN) environment have been derived. It has been observed that satisfactory BER performance is obtained when the detection probability becomes higher, as expected.

4.4.1 Detection Of Symmetric α-Stable Distributed Signals In White Gaussian Noise

In this Subsection, the detection performances of the communication scheme which use unipodal (Cek & Savacı, 2009) α-shift keying in its transmitter part and the FLOM method in its receiver part have been given. Receiver Operating

Characteristics (ROCs) (i.e., the probability of detection P_D versus the probability of false alarm P_{FA}) have been evaluated by applying Neyman-Pearson test to obtain detection performance. The main contribution of this Section is to find the detection probabilities of SαS distributions embedded in Gaussian noise environment.

Binary Hypothesis Testing (BHT) for detecting SαS distribution in Gaussian noise environment:

The detector structure is designed under the hypotheses formulated below

$\mathcal{H}_1: y = x_1 + n\,, \qquad x_1 \sim S_{\alpha_1}(\sigma,0,0)$ (4.54.a)

$\mathcal{H}_0: y = x_0 + n\,, \qquad x_0 \sim S_{\alpha_0}(\sigma,0,0)$ (4.54.b)

where the Gaussian white noise model is also a member of SαS distribution with α=2 and represented as $n \sim S_2(\sigma_G,0,0)$.

For each hypothesis, the probability density function (pdf) $f(y;H_k)$ of a single observation y shown in Figure 4.30 has been obtained by convolving pdfs of the SαS and the Gaussian distributions as in Eq. 4.54a and Eq. 4.54b.

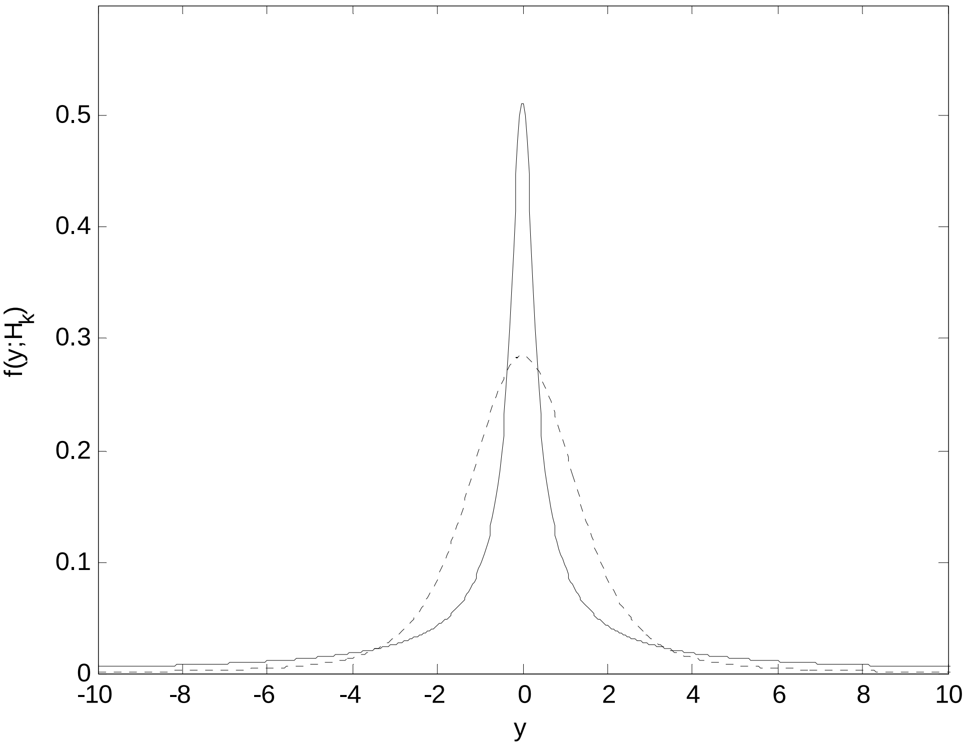

Figure 4.30 Resultant normalized pdfs $f(y;H_k)$ for the hypothesis $\mathcal{H}_1$ $\alpha_1 = 0.5$ (Solid), the hypothesis $\mathcal{H}_0$ $\alpha_0 = 1.5$ (Dotted), $\sigma = 1$ for both hypotheses and $\sigma_G = 0.1$.

Neyman Pearson Detector for SαS Distribution Embedded in Gaussian Noise: The decision statistics are obtained by applying the Neyman-Pearson test (Kay, 1993b):

$$L(y) \overset{\Delta}{=} \frac{f(y;H_1)}{f(y;H_0)} > \gamma \tag{4.55}$$

where γ is the threshold.

Since there does not exist an analytical expression for the probability density (pdf) of the αS random variable, then the pdf of sum of SαS distribution with Gaussian distribution has been numerically determined by using the characteristic functions of the resultant densities in each hypothesis as

$$f(y;H_k) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \exp\left(-i\theta y - \sigma^{\alpha_k}|\theta|^{\alpha_k} - \sigma_G^2\theta^2\right)d\theta,\ k = 0,1. \tag{4.56}$$

Note that only asymptotic expansions for the pdf of SαS and for the pdf of the sum of SαS random variables are available in (Tsihrintiz & Nikias, 1993), (Tsihrintiz & Nikias, 1995). The probability of detection P_D and the probability of false alarm P_{FA} are defined as:

$$P_D = \int_{y:L(y)>\gamma} \frac{1}{2\pi} \int_{-\infty}^{\infty} \exp\left(-i\theta y - \sigma^{\alpha_1}|\theta|^{\alpha_1} - \sigma_G^2\theta^2\right) d\theta dy \tag{4.57}$$

$$P_{FA} = \int_{y:L(y)>\gamma} \frac{1}{2\pi} \int_{-\infty}^{\infty} \exp\left(-i\theta y - \sigma^{\alpha_0}|\theta|^{\alpha_0} - \sigma_G^2\theta^2\right) d\theta dy \tag{4.58}$$

where the characteristic exponents α₁, α₀ and the scale parameters σ, σ$_G$ are assumed to be known because they are used for encoding the message signal in the transmitter part of the random communication system proposed in (Cek & Savacı, 2009). The performance of the receiver has been analyzed obtaining ROCs (i.e., P$_D$ versus P$_{FA}$) shown in Figure 4.31 for the different choices of characteristic exponents.

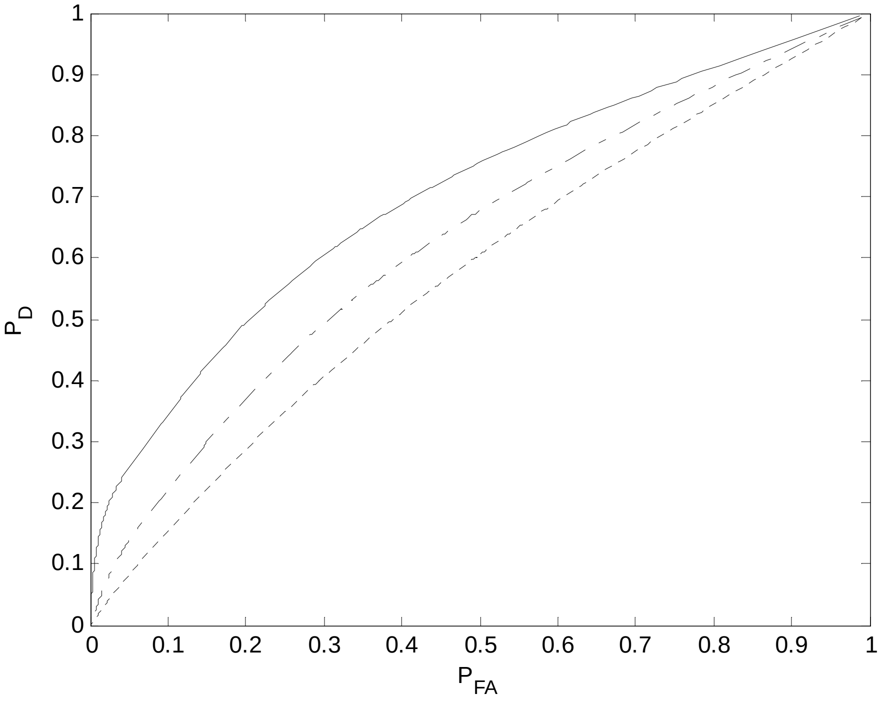

Figure 4.31 The variation of the ROCs with respect to the different characteristic exponents where the fixed $\alpha_1 = 0.5$ and $\alpha_0 = 1.5$ (Solid), $\alpha_0 = 1.0$ (Dashed-Dotted), $\alpha_0 = 0.75$ (Dotted). The scale parameters have been chosen as $\sigma_G = 0.1$, $\sigma = 1$.

Figure 4.32 illustrates the effect of the Gaussian noise in the channel to the receiver performance. It can be seen that when the Guassian interference increases then the detection probability decreases.

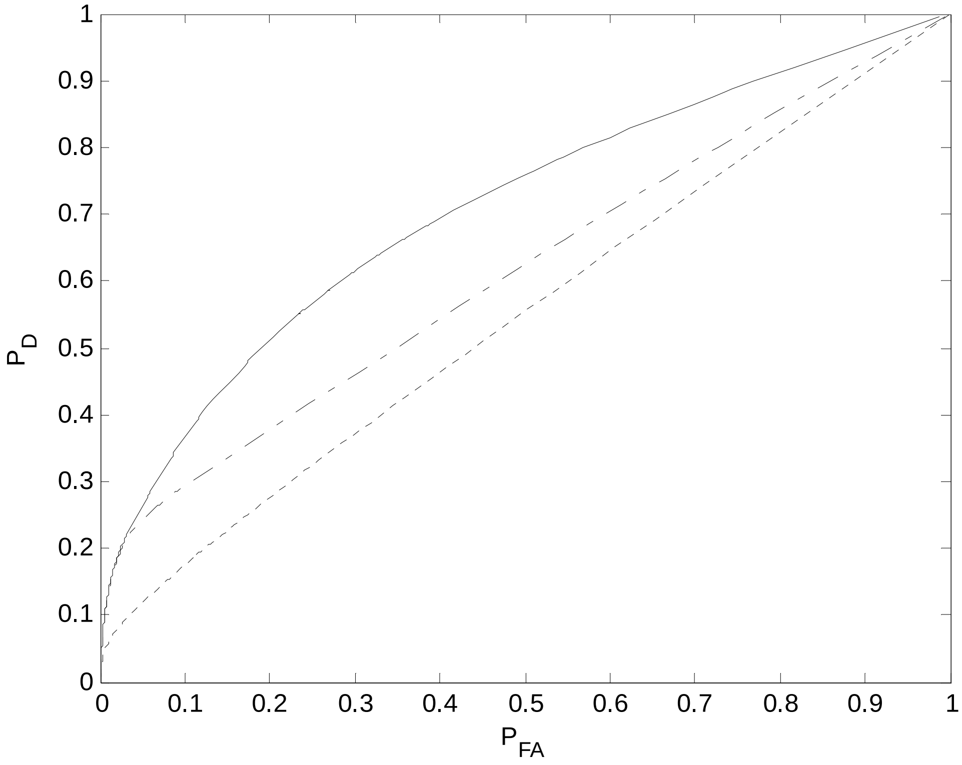

Figure 4.32 The variation of the receiver operating characteristics with respect to the different scale parameters of Gaussian noise where $\alpha_1 = 0.5$, $\alpha_0 = 1.5$, $\sigma = 1$ and $\sigma_G = 0.001$ (Solid), $\sigma_G = 0.1$ (Dashed-Dotted) and $\sigma_G = 10$ (Dotted).

In fact, the distance between the densities can be a clue about the detection performance of the detector. Therefore, under the binary hypothesis defined in (4.54.a) and (4.54.b), we have computed the Hellinger distance (Scott, 1992) between the pdfs as

$$d(f(y;H_1), f(y;H_0)) \overset{\Delta}{=} \left(\int_{-\infty}^{\infty} \left(\sqrt{f(y;H_1)} - \sqrt{f(y;H_0)} \right)^2 dy \right)^{1/2} . \tag{4.59}$$

It can easily be seen in Figure 4.33 that the probability of detection increases if the impulsiveness of the distribution "α_0" is increased in the Gaussian environment.

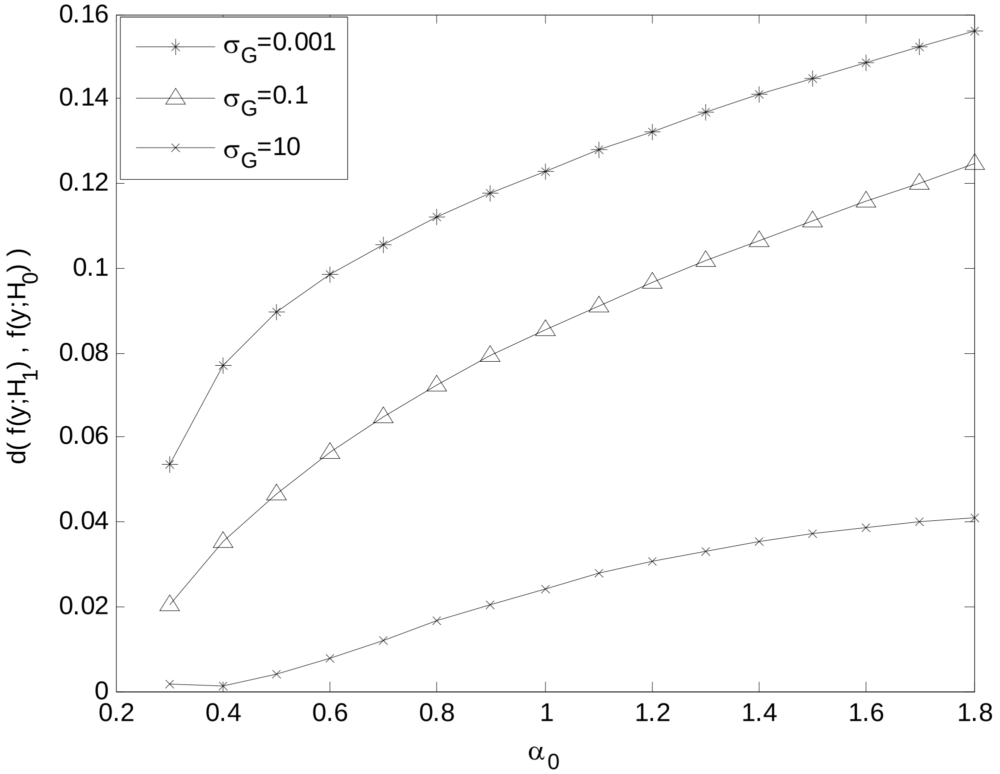

Figure 4.33 For fixed α_1 ($\alpha_1 = 0.2$), the Hellinger distance with respect to α_0 for various Gaussian scale parameters σ_G.

As conclusion, this Section addresses the problem of detection of the symmetric α-stable distributed random signals which are mixed with white Gaussian noise by observing single sample as:

i. The ROCs indicate that the detectability of the single observation decreases when the variance of the Gaussian noise increases. Because, if the variance of the Gaussian density in the channel increases, then Hellinger distance between the resulting densities $f_y(\cdot)$ in each hypothesis decreases and hence due to the similar f_y s in each hypothesis the detection performance of the detector reduces,

ii. If we do not choose the characteristic exponents (CE) of the SαS distributions in each hypothesis close to each other, then the Hellinger distance between the densities is increased and the detection probabilities can thus be increased. The above discussions imply that the security can be increased if the closely chosen characteristic exponents of SαS distributions approach to the characteristic exponent of the Gaussian noise in the channel.

4.4.2 Detection of Skewed α-Stable Distributed Signals in White Gaussian Noise

In this subSection, the detection performances of the communication scheme which use antipodal α-shift keying in its transmitter part and the FLOM method in its receiver part has been given. Receiver Operating Characteristics (ROCs) (i.e., the probability of detection P_D versus the probability of false alarm P_{FA}) have been evaluated by applying the Neyman-Pearson test to obtain detection performance as given in the previous Subsection. The contribution of this subSection is to find the detection probabilities of skewed α-stable distributions embedded in Gaussian noise environment.

Binary Hypothesis Testing (BHT) for detecting skewed αS distribution in Gaussian noise environment:
The detector structure is designed under the hypotheses formulated below

$$\mathcal{H}_1 : y = x_1 + n, \qquad x_1 \sim S_{\alpha_1}(\sigma, \beta, 0) \tag{4.60.a}$$

$$\mathcal{H}_0 : y = x_0 + n, \qquad x_0 \sim S_{\alpha_0}(\sigma, -\beta, 0) \tag{4.60.b}$$

where the Gaussian white noise model is also a member of SαS distribution with α=2 and represented as $n \sim S_2(\sigma_G, 0, 0)$.

The probability of detection P_D and the probability of false alarm P_{FA} associated with the skewed case are defined as:

$$P_D = \int_{y:L(y)>\gamma} \frac{1}{2\pi} \int_{-\infty}^{\infty} \exp\left(-i\omega y - \sigma^{\alpha_1} |\omega|^{\alpha_1} + i\theta(\omega, \alpha, \beta) - \sigma_G^2 \omega^2\right) d\omega dy \tag{4.61}$$

$$P_{FA} = \int_{y:L(y)>\gamma} \frac{1}{2\pi} \int_{-\infty}^{\infty} \exp\left(-i\omega y - \sigma^{\alpha_0} |\omega|^{\alpha_0} - i\theta(\omega, \alpha, \beta) - \sigma_G^2 \omega^2\right) d\omega dy \tag{4.62}$$

where

$$\theta(\omega,\alpha,\beta)=\begin{cases}\beta|\omega|^{\alpha-1}\tan\left(\dfrac{\pi\alpha}{2}\right) & \text{if } \alpha\neq 1\\ -\beta\dfrac{2}{\pi}\ln|\omega| & \text{if } \alpha=1\end{cases} \tag{4.63}$$

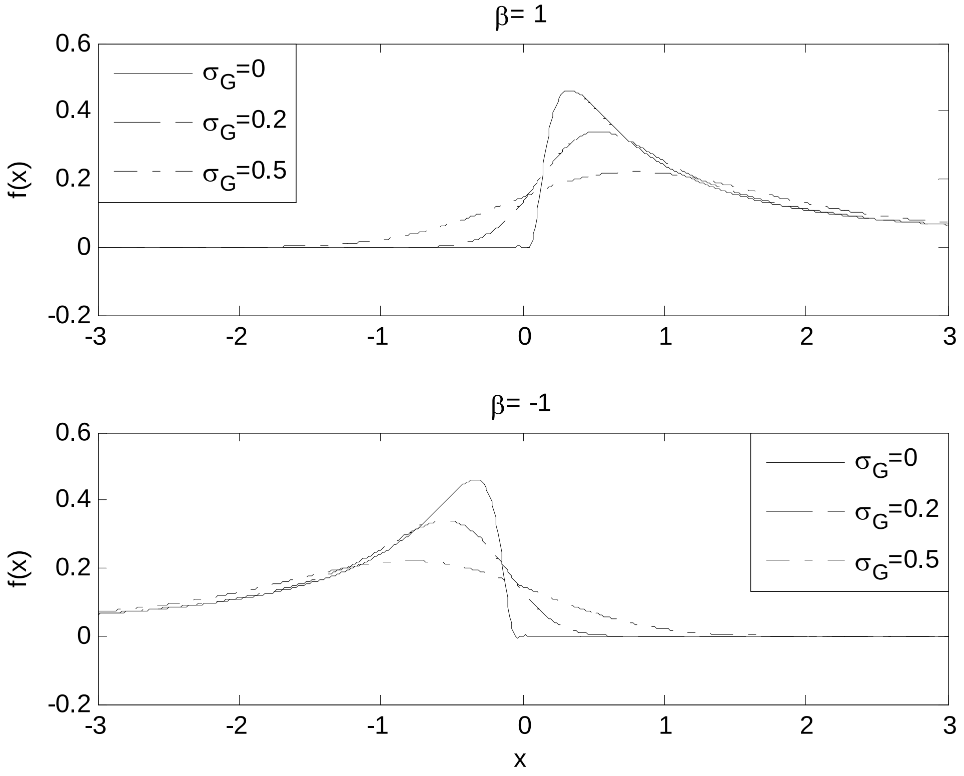

Figure 4.34 Probability density function of summation of skewed α-stable and Gaussian random variables is illustrated under various Gaussian noise variances and opposite skewness (α=0.5).

It can be seen in Figure 4.34 that the Gaussian interference decreases the skewness of the α-stable distribution and results in wider pdf. Therefore, more skewed distribution will provide an increase in the detection probability. The detection probabilities of the skewed α-stable distributed signals are shown in Figure 4.35.

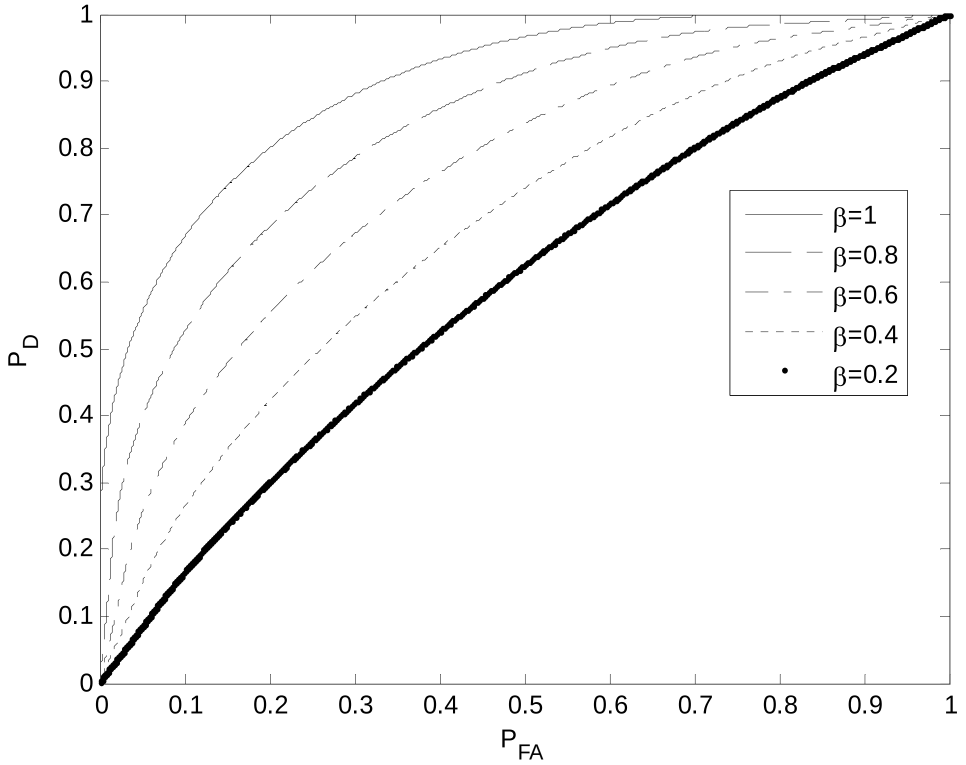

Figure 4.35 Illustration of probability of detection P_D versus probability of false alarm, P_{FA} (α=0.6, σ=0.5, σ_G=1).

The problem of detection of the skewed α-stable distributed random signals which are mixed with white Gaussian noise by observing single sample has been addressed in this subSection and the ROCs indicate that delectability of the single observation decreases when the variance of the Gaussian noise increases. The above discussions imply that the selection of more skewed stable signal will result increased detection probability.

CHAPTER FIVE
CONCLUSIONS

In this thesis, novel signal processing techniques for designing secure communication systems have been introduced. Instead of using any deterministic signal as in the conventional spread spectrum techniques the newly introduced secure digital communication scheme uses random signals which have α-stable distributions as a random carrier.

Before discussing the proposed random communication schemes, fundamentals of the chaotic communication schemes have been explained in the beginning of the thesis since historically chaotic signals due to their noise-like spectrum have been first studied extensively in the past twenty five years as an alternative spread spectrum communication technique.

Besides the existing chaotic modulation techniques such as chaotic frequency and pulse position modulation in the literature the new chaotic communication scheme involving double sideband amplitude modulation has also been introduced as a novel contribution. Since the modulation techniques using chaotic signals to spread the spectrum can not be used in the high frequency range, the proposed study aims to shift the frequency content of the message signal which is masked by the chaotic signal by the carrier frequency in order to provide the chaotic communication for possible wireless applications at high frequencies. The drawback of the proposed method is weak robustness of the receiver when the signal to noise ratio decreases. Therefore improvement in the performance of the receiver is needed as further work.

Although chaotic signals have been accepted as proper candidates because of their broad-band nature, like noise signals but since the chaotic signals have low fundamental frequencies and their power is concentrated at low frequencies, the chaotic communication especially based on the masking techniques can be easily broken by the methods explained in Chapter 2.

In Chapter 3, as a contribution to the chaotic communication systems the security performance have been improved by masking the chaotic signal with an impulsive noise having alpha-stable distribution with specified distribution parameters before transmitting the signal through the Gaussian noise channel. Since the noise model is non-Gaussian, the tracking problem of the chaotic trajectory could not be solved by suboptimal filters such as extended Kalman filtering. Therefore, the particle filtering techniques which are based on Bayesian estimation have been considered for filtering the noisy observations of the receiver. The proposed methods use SαS random signal as a *jammer* through the channel and a broad-band signal can thus be obtained. Since the characteristic exponent of the impulsive noise is assumed to be known by the receiver, the noisy observation can be filtered by using particle filtering techniques. It has been shown that SαS noise is a candidate tool for increasing the security but the receiver performance for tracking the chaotic trajectory may be poor. The disadvantage of the particle filtering based receiver is to determine the prior density for the initiation of the filtering algorithm. To overcome this problem initial densities have been estimated by observing the histogram of the noise-free chaotic trajectory. The chaotic dynamics of Henon map has been estimated in the non-Gaussian environment by using the particle filtering method. It has been shown that the proposed method has a certain spectrum-spreading effect but it can offer limited filtering performance if the distribution of the particles and prior densities can not be chosen properly which is already an open problem.

In Chapter 4, novel random communication systems have been introduced based on α-stable distributions. The binary message has been modulated by α-stable distributed signals with specified parameters such as characteristic exponent α and skewness parameterβ. These parameters have been used to encode the binary message signal. It was shown that the impulsiveness parameter "*alpha*" can be properly estimated at the receiver if the length of the generated noise sequence is properly chosen and from these estimated *alpha* values the binary message can be decoded. Although, the effect of additive white Gaussian noise (AWGN) channel has been observed as small deviations in the actual *alpha* values, by properly choosing threshold in the detector the same amount of deviations occur in the *alpha* values and hence the actual message bits can be estimated. The receiver derives discriminating information associated with the observed random signal which carries the binary message.

Several methods have been given to design the receiver for estimating SαS distributed random carrier signals in Section 4.2. The first method given in Section 4.2.1 is based on the least-square estimation and uses empirical characteristic function. Although the stable distributions can not be formulated analytically, the characteristic function of the stable distributions can be expressed analytically. The estimate of the empirical characteristic function (ECF) can be directly obtained from the observations. Using regression analysis, parameter estimation of the stable distribution has been tried to be obtained by the least squares estimation. The bit error rate (BER) performances have been realized for the least-squares estimation method and it has been observed that the error probability in detection saturates even though the energy of the random carrier comparatively higher with respect to the Gaussian noise in the channel (i.e. dispersion ratio increases). This is because the standard deviation of the parameter estimation is dramatically high so that erroneous estimation has been obtained even while there is a weak interfering Gaussian noise in the channel. On the other hand, since the method is computationally expensive, the length of the SαS random signal is insufficient to perform a proper estimate. In Section 4.2.2 by investigating the moment type estimator which is also based on the use of ECF it has been concluded that the empirical characteristic function based parameter estimation methods are not preferable for random communication systems.

In Section 4.2.3, the correntropy based receiver has been considered as an alternative receiver model. Varying impulsiveness of the stable random signals by changing the characteristic exponent has been modeled by using similarity measure (auto-correntropy) between the samples of the observed signal in the receiver and the random carriers. Since the Gaussian kernel can not successfully discriminate the stable random signals with different characteristic exponents which represents the binary codes of the message signal, fractional lower order moment has been considered for defining the similarity. Due to computational complexity, the signal length for one bit duration has to be decreased compared to the other receiver methods defined above that caused poorer bit error rate performance. Moreover, it was observed that the standard deviation of the estimated auto-correntropy value for the specified characteristic exponent increased while the characteristic exponent is decreased. Therefore it is critical that the proper selection of relatively low characteristic exponents near to each other to reduce the error performance of the correntropy method.

The last receiver model given in Section 4.2.4 is based on density parameter estimation method which uses the fractional lower order moments (FLOM) to detect the distribution parameters of the observed random signal. More generally, since the moments greater then the characteristic exponent of the stable distribution is infinite, fractional lower order statistics is significant to extract the discriminative information from the observations at the receiver. The performance of communication scheme associated with density parameter estimation has been analyzed by computing bit error rate (BER) performances. It is observed that, there are some critical points in deciding the BER performance. First, when the *alpha* values of distributions are decreased then the impulsiveness of the noise increases which causes poor bit error rate performances. Second, when the characteristic exponents of the stable noise signals are selected far from each other, the bit error rate increases. In order to reduce the estimation error, the length of the noise sequence should be chosen sufficiently large.

In Section 4.3.3, the skewness parameter β of the alpha-stable distribution has been used to modulate the binary message while the characteristic exponents of the random carriers are chosen equal to each other. The BER results illustrate that when the value of skewness parameter is increased, the positive-skewed and negative-skewed distributions can be more easily estimated. This causes decrease in the BER performance of the system.

In Section 4.3.4, both characteristic exponents and skewness parameters of the random carrier have been used for random communication in order to double the transmission speed. It has been observed that while the transmission speed is increased, the BER performance becomes poorer since the estimation of the skewness parameter depends on the estimated characteristic exponent. A possible deviation on estimating the characteristic exponents brings a misleading estimation on skewness parameter.

In Section 4.3.5, as another random communication scheme, instead of coding the binary message bit with constant noise parameters, it has been considered to use skewed α-stable distributed noise signal where the parameters of the parameters of the noise is also taken from a known distribution. Since the stable noise parameters are also changed for each message bit the possibility of the determining the parameters by an intruder is also avoided and a higher security can thus be achieved. The BER performance of the method can be increased by appropriate selection of the threshold.

Since the purpose of using random signals for communication is to provide security, in Section 4.4, the receiver operating characteristics (ROC) which identify the detectability of the random signals under Gaussian contamination having different stable distribution have been evaluated.

In Section 4.4.1, the problem of detection of the symmetric α-stable distributed random signals which are mixed with white Gaussian noise by observing single sample has been analyzed.The ROCs indicate that the detectability of the single observation decreases when the variance of the Gaussian noise increases. Because, if the variance of the Gaussian density in the channel increases, then the Hellinger distance between the densities associated with each hypothesis decreases and hence due to the smaller distance between the densities, the detection performance of the detector reduces. If we do not choose the characteristic exponents of the SαS distributions in each hypothesis close to each other, then the Hellinger distance between the densities is increased and the detection probabilities can thus be increased.

The above discussions imply that the security can be increased if the closely chosen characteristic exponents of SαS distributions approach to the characteristic exponent of the Gaussian noise in the channel. In Section 4.4.2, the construction and performance of a skewed α-stable noise detector has been presented. As it is expected, when the impulsiveness of the stable noise is increased, i.e. α parameter is decreased, detection performance increases. The detectability of the proposed system increases when the stable distribution is more skewed.

After the analysis given in Chapter 4, one can conclude that the random signals with α-stable distributions can be proper carriers for secure random communication. Bit error rate performance can be improved by choosing the more impulsive and/or more skewed stable distributions. Since the detectability increases while the impulsiveness and/or skewness are being increased, there is an inverse relation with security and error performance. This *trade-off* should be taken into account before designing the proposed random communication systems.

The proposed random communication schemes have been analyzed in memoryless channels. In order to interpret the applicability of the method in wireless communication systems, it is essential to analyze the proposed method under interference of both random and deterministic signals, in different fading channels such as Rayleigh and Rician fading which have memory. Analyzing the proposed random communication scheme in such channel models will be the further projections by deriving analytical or approximate models using covariation of the stable distributions with time-delay models and source separation techniques like independent component analysis (ICA). Although the proposed methods in the thesis introduce several communications models for only single user, adaptation of time-division multiple accesses (TDMA) for stable distributions and the analysis of the multivariate stable-distributions will provide to develop multi-user secure-communication systems as a further work.

REFERENCES

Abel, A. & Schwarz, W. (2002). The chaos communications-principles, schemes, and system Analysis. *Proc. of IEEE, 90* (5), 691-710.

Altınkaya M. A., Deliç H., Sankur B., Anarım E., (2002). Subspace-based frequency estimation of sinusoidal signals in alpha-stable noise. *Signal Processing*, 82, 1807-1827

Alvarez E., Fernandez P., Garcia J.J., Marcano (1999). A., New approach to chaotic encryiption. *Physics Letters A*, 263, 373-375.

Alvarez G., Montoya F., Pastor G. (2004). Breaking parameter modulated chaotic secure communication system, *Chaos Solitons and Fractals*, 21, 783-787.

Alvarez G., Montoya F., Pastor G., Romera M. (2005a). Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value. *Chaos Solitons & Fractals*, 23, 1749-1756.

Alvarez G., Li S., Montoya F., Pastor G., Romera M. (2005b). Breaking projective chaos synchronization secure communication using filtering and generalized synchronization, *Chaos Solitons and Fractals*, 24, 775-783.

Alvarez G., Hernandez L., Munoz J., Montoya F., Li S. (2005c), Security analysis of communication system based on the synchronization of different order chaotic systems. *Physics Letters A*. 345, 245-250.

Arulampalam M.S., Maskell S., Gordon N., Clapp T. (2002). A tutorial on particle filters for online nonlinear/non-Gaussian Bayesian tracking. *IEEE Transaction on Signal Processing*, 50, 174-188.

Basore, B. L., (1952). *Noise-like signals and their detection by correlation*. Ph. D. Thesis, Cambridge: MIT, MA.

Bergstrom H.(1952). On some expansions of stable distribution functions. *Arkiv for Matematik*, *2*, 375-378.

Berozzi T. Ruyet D.L., Panazio C., Thien H. V: (2004). Channel tracking using particle filtering in unresolvable multipath environments. *EURASIP Journal on Applied Signal Processing*, 15, 2328-2338.

Brcich R., Zoubir A., (1999). Estimation and detection in a mixture of symmetric alpha stable and Gaussian interference, *Higher Order Statistic, IEEE Signal Proc. Workshop*, 219-223.

Bu S., Wang Bing-Hong. (2004). Improving the security of chaotic encryption by using a simple modulating method. *Chaos Solitons and Fractals*, 19, 919-924.

Callegari S., Rovatti R., Setti G. (2003a). Spectral properties of chaos-based FM signals: Theory and simulation results. *IEEE Transactions on Circuits & Systems –I: Fundamental Theory and Applications*, 50, (1), 3-15.

Callegari S., Rovatti R., Setti G. (2003b). Chaos based FM signals: Applications and implementation issues. *IEEE Transactions on Circuits & Systems–I: Fundamental Theory and Applications*, 50, (8), 1141-1147.

Cek M. E., Savacı F. A. (2009). Stable non-Gaussian noise parameter modulation in digital communication. *Electronics Letters, 45*, (24),1256–1257.

Chen M., Min W. (2008). Unknown input observer based chaotic secure communication. *Physics Letters A*, 372, 1595-1600.

Chua L. O., Kocarev L., Eckert K., Itoh M. (1992). Experimental chaos synchronization in Chua’s circuit, *Int. J. Bif. Chaos*, 2, (3), 705-708.

Chua L. O. (1994). Chua’s circuit 10 years later. *International Journal of Circuit Theory and Applications*, 22, 279-305.

Cuomo, K.M., Oppenheim, A.V., Strogatz, H. (1993). Synchronization of Lorenz based chaotic circuits with applications to communications. *IEEE Trans. Circuits & Systems, 40* (10), 626–633.

Dmitriev S. A., Kislov Y. V., Panas I. A. et. al. (1985). *USSR Inventor’s certificate* No. 279024, No.9.

Dmitriev S. A., Kletsov M. A., Laktyushkin M. A., (2006). Ultra wideband wireless communications based on dynamic chaos, *J. Comm. Tech. & Elec.*, 51, (10).

Dmitriev A. S., Kuzmin L. V., Laktushkin A. M. (2004). Amplitude modulation and demodulation of chaotic carriers, *Nonlinear Dynamics of Electronic Systems* (NDES), 138-141.

Erdogmus D., Agrawal R., Principe J. C. (2005). A mutual information extension to the matched filter. *Signal Processing, 85*, 927-935.

Fernandez J.G., Larrando H.A., Slavin H.A., Levin D.G., Hidalgo R.M., Rivera R.R. (2003). Masking properties of APD communication systems. *Physica A*, 328, 351-359.

Forester J.R., (2004). Channel modelling sub-comittee report final, from http://grouper.ieee.org/groups/802/15/pub/04/15-04-0662-02-004a-channel-model-final-report-rl.pdf

Fortuna L., Frasca M., Rizzo A. (2003). Chaotic pulse position modulation to improve the efficiency of the sonar sensors. *IEEE Transactions on Instrumentation & Measurement*, 52, (6), 1809-1814.

Garel B. & Kodia B. (2009). Signed symmetric covariation coefficient for alpha-stable dependence modeling. *Statistics*, 347, 315-320.

Gençağa D., Kuruoğlu E.E., Ertüzün A. (2008). Modelling of non-stationary autoregressive alpha stable processes by particle filters. *Digital Signal Processing*, 18, 465-478.

Geranoitis E. (1985). Coherent hybrid DS-SFH spread-spectrum multiple access communication. *IEEE Journal on Selected Areas in Communication*. 3, (5), 695-705.

Geranoitis E. (1986). Noncoherent hybrid DS-SFH spread-spectrum multiple access communication. *IEEE Transactions on Communication*. 34, (9), 862-872.

Gonzales J.A., Reyes L. I, Suarez J.J., Guerrero L.E., Gutiérrez. (2002). A mechanism for randomness. *Physics Letters A*, 295, 25-34.

Gustafsson F., Gunnarsson F., Bergman N., Forssell U., Jansson J., Karlsson R., Norlund Per-Johan. (2002). Particle filters for positioning, navigation and tracking. *IEEE Transacitons on Signal Processing*, 50, 425-437.

Haykın S. (1994). *Communication systems*. Third Edition, John & Wiley Sons Inc.

Huang N.E., Shen Z., Long S. R., Wu M.C., Shih H.H., Zheng Q., Yen Nai-Chyuan, Tung C.C., Liu H.H. (1998). The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis. *Proceedings of Royal Society*, 454, 903-995.

Hugues-Salas O., Shore K. A. (2010). An extended Kalman filtering approach to time-delay systems: Application to chaotic secure communication. *IEEE Transactions an Cirucuits and Systems* – I: *Regular Papers*. 57,(11), 1-11.

Ilow J., Hatzinakos D., (1998). Applications of the empirical characteristic function to estimation and detection problems. *Signal Processing*, 65, 199-219.

Janicki A., Weron A., (1994). *Simulation and chaotic behavior of α-stable stochastic processes*. First Edition, NY, Marcel Dekker.

Jeong K.H., Liu W., Han S., Hasanbelliu E., Principe J.C. (2009). The correntropy MACE filter. *Pattern Recognition*, 42, 871-885.

Kassam S. A. (1988). *Signal detection in non-Gaussian noise*, Berlin: Springer-Verlag.

Kay S.M. (1993a). *Fundamentals of statistical signal processing – estimation theory*, NY: Prentice Hall.

Kay S.M. (1993b). *Fundamentals of statistical signal processing – detection theory*, NY: Prentice Hall.

Kennedy M. P., Rovatti R., Setti G. (2000). *Chaotic electronics in telecommunications*. First Edition, CRC Press.

Kis G., Jako Z., Kenedy M.P., Kolumban G. (1998). Chaotic communications without synchronization. *IEE Telecommunications Conference*, 49-53.

Kolumban G., Kennedy M.P., Chua L. O. (1998). The role of synchronization in digital communications using chaos II. Chaotic Modulation and Chaotic Synchronization, *IEEE Trans. Cct & Syst.*, 45, 1129-1140.

Kolumban G. Kennedy M. P., Jako Z., Kis G. (2002). Chaotic communications with correlator receivers: Theory and performance limits. *Proceedings of IEEE*, 90, 711- 732.

Kolumban, G., Lau, F. C. M., Tse, C. K. (2005). Generalization of waveform communications: the Fourier analyzer approach. *Circuits Systems & Signal Processing*, 24 (5), 451–474.

Kowatsch M., Lafferl J. (1983). A spread-spectrum concept combining chirp modulation and pseudonoise coding. *IEEE Transactions on Communications*, 31,(10), 1133-1142.

Kuruoglu E.E., Fitzgerald W.J., Rayner P. J.W (1998). Near optimal detection of signals in impulsive noise modeled with a symmetric α-stable distribution, *IEEE Communication Letters, 2,* (10), 282-284.

Kuruoglu, E. E. (2001). Density parameter estimation of skewed alpha-stable distributions. *IEEE Trans. Signal Processing*, 49 (10), 2192–2201.

Larger L., Goedgebuer J. P., Udaltsov V.S., Rhodes W.T. (2001). Radio transmission system using FM high dimensional chaotic oscillator. *Electronics Letters*, 37, 594-595.

Lau F.C.M., Tse C.K.. (2003). *Chaos-based digital communication systems*. First Edition, Berlin: Springer.

Leon D., Balkır S., Hoffman M.W., Perez L. C. (2004). Pseudo-chaotic PN-sequence generator circuits for spread-spectrum communications. *IEE Proceedings of Cicuits Devices Systems*, 151, 543-550.

Li C., Yan J. (2006). Generalized projective synchronization of chaos: The cascade synchronization approach. *Chaos Solitons and Fractals*, 30, 140-146.

Li Demin, Wang Z., Zhou J., Fang J., Ni J. (2007). *Chaos Solitons and Fractals*. 38,1217-1224

Li Damei, Lu Jun-an, Wu X. (2005). Linearly coupled synchronization of the unified chaotic systems and Lorenz systems. *Chaos Solitons and Fractals*, 23, 79-85.

Li Guo-Hui. (2005). Synchronization of chaotic systems with parameter driven by a chaotic signal. *Chaos Solitons and Fractals*, 26, 1485-1489.

Li Guo-Hui, Meng G., (2006). Detection of harmonic signals from chaotic interference by empirical mode decompoisition. *Chaos Solitons and Fractals*, 30, 930-935.

Li Shujun, Mou X., Cai Y. (2001) Improving security of a chaotic encryption approach. 290, 127-133.

Li Xutao, Chen Z., Wang S. (2008). An approximate representation of heavy tailed noise: Bi parameter Cauchy Gaussian mixture model. *Int. Conf. Signal Processing*, 76-79.

Liu W., Pokharel P.P., Principe J.C. (2007). Correntropy: Properties and applications in non-Gaussian signal processing. *IEEE Transactions on Signal Processing*. 55, *11*, 5286-5298.

Liu B., Ma Xiao-chuan, Hou Chao-huan. (2008). A particle filter using SVD based sampling Kalman filter to obtain the proposal distribution. *IEEE Conference on Cybernetics and Intelligent Systems*, 581-584.

Luca M. B., Azou S., Burel G., Serbanescu A. (2005). A complete receiver solution for direct sequence spread-spectrum communication system. *IEEE International Symposium on Circuits & Systems* (ISCAS) 2005, 3813-3816.

Lü J., Zhou T., Zhang S. (2002). Chaos synchronization between linearly coupled chaotic systems. *Chaos Solitons and Fractals*, 14, 529-541.

Mihaylova L., Brasnett P., Achim A., Bull D., Canagarajah N. (2005). Particle filtering with alpha-stable distributions. *IEEE Workshop on Statistical Signal Processing* (SSP'05), 381-386.

Miller G. (1978). Properties of certain symmetric stable distribution. *Journal of Multivariate Analysis*, 8, 346-360.

Min L., Zhang X. (2005). A generalized synchronization theorem for an array of differential equations with application to secure communication. *International Journal of Bifurcation and Chaos*, 15, 119-135.

Minai A.A., Pandian T.D. (1998). Communicating with noise: How chaos and noise combine to generate secure encryption keys. *Chaos*, 8, 621-629.

Morgül Ö. (2000). Synchronization and chaotic masking scheme based on occasional coupling, *Physical Review E*, 62, (3), 3543-3551.

Morgül Ö., Solak E., Akgül M. (2003). Observer based chaotic message transmission. *International Journal of Bifurcation and Chaos*, 13, 1003-1017.

Murali K., Leung H., Yu H. (2003). Design of non-coherent receiver for analog spread spectrum Communication Based on chaotic masking, *IEEE Trans. Cct. & Syst. – I*, 50, 432-441.

Nikias C. L., Shao M. (1995). *Signal processing with α-stable distributions and applications*. First Edition, NY: Wiley.

Okamoto E., Iwanami Y. (2006). A trellis-coded chaotic modulation scheme. *IEEE International Conference on Communications* (ICC’06), 5010-5015.

Pareek N.K., Patidar V., Sud K.K. (2005). Cryptography using multiple one-dimensional chaotic maps. *Communications in Non-linear Science and Numerical Simulation*. 10, 715-723.

Patidar V., Sud K.K., (2009). A novel pseudo random bit generator based on chaotic standard map and its testing. *Electronic Journal of Theoretical Physics*, 20, 327-344.

Pecora L. M., Caroll T. L. (1990). Synchronization in chaotic systems, *Physical Review Letters*, 64, 821-824.

Pecora M. L., Caroll T. L. (1991). Driving systems with chaotic signals. *Physical Review A, 44* (4), 2374-2383.

Peng Z.K., Tse P. W. Chu F. L. (2005). An improved Hilbert-Huang transform and its application in vibration signal analysis. *Journal of Sound and Vibration*, 286, 187-205.

Pokharel P. P., Liu W., Principe J.C. (2009). A low complexity robust detector in impulsive noise. *Signal Processing*, 89, 1902-1909.

Proakis J. G., (2000). *Digital communications*, Fourth Edition, Mc Graw Hill.

Punskaya E., Andrieu C., Doucet A., Fitzgerald W.J. (2001). Particle filtering demodulation in fading channels with non-Gaussian additive noise. *IEEE Transactions on Communications*. 49, 579-582.

Rasband S.N., (1990). *Chaotic dynamics of nonlinear systems*, New York, Wiley.

Ruan H., Zhai T., Yaz E.E. (2003). A chaotic secure communication scheme with extended Kalman filter. *IEEE Conference on Control Applications*, 404-408.

Rulkov N. F., Suschik M. M., Tsimring L. V., Volkovskii A. R. (2001). Digital communication using chaotic pulse position modulation. *IEEE Transactions on Circuits and Systems-I*, 48, (12), 1436-1444.

Samorodnitsky, G., Taqqu, M. S. (1994). *Stable non-Gaussian random processes,* NY, First Edition, Chapman & Hall / CRC.

Sandhu G., Berber S.M. (2005). Investigations on operation of a secure communication system based on chaotic phase shift keying scheme. *Int. Conf. on Information Technology and Applications,* 584-587.

Santamaria I., Pokharel P.P., Principe J.C. (2006) Generalized correlation function: Definition, properties and application to blind equalization. *IEEE Transactions on Signal Processing*, 54, *6*, 2187-2197.

Savacı, F.A., Yalçın, M.E., Güzeliş, C., (2003). Steady-state analysis of nonlinearly coupled Chua's circuit with periodic input. *Int. J. Bifurcation & Chaos 13,* (11), 3395–3407.

Schimming, T., Hasler, M., (2000). Optimal detection of differential chaos shift keying. *Int. J. Bifurcation & Chaos, 47,* (11), 1712–1719.

Scott D.W. (1992). *Multivariate density estimation*. First Edition, Wiley & Sons Inc.

Setti G., Mazzini G., Rovatti R., CallegariS. (2002). Statistical modelling of discrete-time chaotic process. Basic finite dimenaional tools and applications. *Proceedings of IEEE*, 90, 662-690.

Siwiak K., McKeown D.,(2004). *Ultra wide band radio technology*, Chichester UK: Wiley.

Sobiski D.J., Thorp J.S. (1998). PDMA-1. Chaotic communication via the extended Kalman filter. *IEEE Transactions on Circuits & Systems-I, Fundamental Theory and Applications*, 45, 194-198.

Stavroulakis, P.(2006). *Chaos Applications in Telecommunication*. First Edition, Boca Raton, CRC Press.

Strogatz S. H. (2001). *Nonlinear dynamics and chaos : with applications to physics, biology chemistry and engineering*, First Edition, West view Press.

Sushchik M., Rulkov N., Larson L., Tsimring L., Abarbanel H., Kung Y., Volkovskii A. (2000). Chaotic pulse position modulation: A robust method of communication with chaos. *IEEE Communication Letters*, 4, (4), 128-130.

Swami A., Sadler B. M. (2002). On some detection and estimation problems in heavy tailed noise. *Signal Processing, 82,* 1829–1846.

Tao C., Du G. (2003). A new approach to breaking down chaotic secure communication, *International Journal of Bifurecation and Chaos*, 13, 2689-2698.

Tsihrintz G. A., Nikias C.L. (1993). Detection and classification of signals in impulsive noise modeled as an alpha-stable process. *Asilomar Conf. on Signals Systs. & Comp., 1,* 707-710.

Tsihrintzis G.A., Nikias. C. L., (1995). Performance of optimum and suboptimum receivers in the presence of impulsive noise modeled as an alpha stable process’, *IEEE Transactions on Communications, 43,* 904-914

Tsihrintzis G.A., Nikias. C. L., (1996). Fast estimation of the parameters of alpha-stable impulsive interference. *IEEE Transactions on Signal Processing*, 44, 1492-1503.

Volkovskii A. R, Tsimring L. Sh. (1999). Synchronization and communication using chaotic frequency modulation. *Int. J. Circuit Theory & App.*, 27, 569-576.

Volkovskii A. R., Tsimring L. Sh., Rulkov N. F., Langmore I. (2005). Spread spectrum communication system with chaotic frequency modulation, *Chaos*, 15, 033101, 1-6.

Wang K., Zhou G., Xiang Z. (2008). Detection of binary signal with both impulsive and Gaussian interference. *Int. Conf. Communications and Networking in China*, 790-793.

Win M. Z., Scholtz R. A. (2000). Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications. *IEEE Transactions on Communications*. 48, 679-689.

Xia Y., Tse C. K., Lau F.C.M. (2004). Performance of differential chaos shift keying digital communication systems over a multipath fading channel with delay spread. *IEEE Transactions on Cirucuits and Systems-II: Express Briefs*, 1-5.

Xie W., Wen C., Li Z. (2000). Impulsive control for stabilization and synchronization of Lorenz systems. *Physics Letters A*. 275, 67-72.

Yalçın M.E. (2007). Increasing the entropy of a random number generator using n-scroll chaotic attractors. *International Journal of Bifurcation and Chaos*, 17, 4471-4479.

Yang T., Chua L. O. (1997). Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication. *IEEE*

Transactions on Circuits and Systems-I: Fundamental Theory and Applications, 44, 976-988.

Yang T., Yang L. B., Yang C. M. (1998). Breaking chaotic secure communication using a spectrogram", *Physics Letters A*, 247, 105-111.

Yang T. (2001). *Chaotic communication systems*. First Edition, Nova Science Publishers, New York.

Yang T. (2004). A survey of chaotic secure communication systems. *International Journal of Computational Cognition.* 2, 81-130.

Zhang. B., Chen, M., Zhou, D., Li, Z.(2007). Particle-filter based estimation and prediction of chaotic states. *Chaos, Solitons and Fractals*, 32, 1491-1498.

Zhang J., Qiu T., Tang H. (2007). The robustness analysis of DLMP algorithm under the fractional lower order α-stable distribution environments. *Signal Processing*, 87, 1709-1720.