RANDOM COMMUNICATION SYSTEMS BASED ON ALPHA-STABLE PROCESSES

A Thesis Submitted to
the Graduate School of Engineering and Sciences of
İzmir Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in Electronics and Communication Engineering

by

Areeb AHMED

November 2018
İZMİR

We approve the thesis of **Areeb AHMED**

Examining Committee Members:

Prof. Dr. Ferit A. SAVACI
Department of Electrical and Electronics Engineering
İzmir Institute of Technology

Prof. Dr. Muştak E. YALÇIN
Department of Electrical and Electronics Engineering
İstanbul Technical University

Prof. Dr. Cüneyt Güzeliş
Department of Electrical and Electronics Engineering,
Yaşar University

Assoc. Prof. Dr. Mustafa A. ALTINKAYA
Department of Electrical and Electronics Engineering,
İzmir Institute of Technology

Assoc. Prof. Dr. Berna ÖZBEK
Department of Electrical and Electronics Engineering
İzmir Institute of Technology

05 November 2018

Prof. Dr. Ferit A. SAVACI
Supervisor, Department of Electrical and Electronics Engineering
İzmir Institute of Technology

Prof. Dr. Enver TATLICIOĞLU
Head of the Department of Electrical
and Electronics Engineering

Prof. Dr. Aysun SOFUOĞLU
Dean of the Graduate School of
Engineering and Sciences

ACKNOWLEDGMENTS

I am extremely grateful to my advisor Prof. Dr. Ferit Acar Savaci for his outstanding supervision and assistance throughout my PhD study. I feel very lucky and proud that I had the chance to work with him. He has always given me complete freedom to independently conduct my PhD research whilst always being there to provide me with direction along with trust and encouragement. It is because of his leadership that I have managed to publish a good number of publications in such a short duration and managed to win IEEE Best Student Research Paper Award (Second Prize) this year.

I would like to show my deepest gratitude to the members of my Thesis Progress Committee Prof. Dr. Mustak Erhan Yalcin and Assoc. Prof. Dr. Mustafa Aziz Altınkaya for their valuable suggestions which clearly helped me in improving my thesis content and clarity in its presentation.

I am also thankful to Turkish Government (Turkiye Burslari) for providing me the fully funded research grant to conduct PhD studies in Turkey via grant number 13PK142514. I have learned a lot in this period of my life. Apart from professional and research skills, I feel myself socially, emotionally and financially proficient after the time spent in Turkey. I am really amazed by the amount of love provided by the Turkish People to me and to my family.

I am always thankful to my parents for their endless and loving support during my whole life. It is due to their hard work and struggle that I am able to achieve the highest level of education.

I want to dedicate my thesis to my family. I am extremely grateful to my wife Rida for her love, encouragement, support and patience especially in the last five years. She has always been a great wife and a source of motivation for me. I would like to thank my elder son Abyan for making the tough times easier for me, with his joy and fun. Additionally, I would also like to thank my newborn son Raaed as he has proven to be extremely lucky for me this year. I feel very blessed to be with them.

ABSTRACT

RANDOM COMMUNICATION SYSTEMS BASED ON ALPHA-STABLE PROCESSES

This thesis presents alpha-stable carrier based random communication systems (RCSs) as an alternate way to perform covert transmission. The first objective is to develop an optimized model of RCS which consists of a receiver that requires less computational complexity and outperforms the previously proposed receivers. Next, in order to solve the existing synchronization issue in RCSs, the general behavior of fractional lower-order covariance method in α-stable noise environments has been evaluated to establish synchronization in RCSs. An optimized range of values for the associated parameters of α-stable carrier has also been presented to optimize the proposed synchronization method.

The second objective is to establish criteria for evaluating and quantifying the security and covertness of RCSs. Therefore, the first security performance tradeoff characteristics (SPTC) have been proposed to compare the security of different RCSs. Moreover, the proposed optimized model of RCS has also been analyzed with respect to the developed security scale, i.e. SPTC. Secondly, the criterion to quantify the covertness of RCSs has also been developed to analyze the proposed RCS. Thirdly, an attack for RCS has also been proposed which highlights the potential vulnerabilities of RCSs. However, the counter-measure guidelines have been prescribed to further enhance the security of RCSs.

An inverse system approach has been adopted to propose α-stable noise driven linear time invariant system based transmitter and its corresponding inverse system based receiver as a third objective. It can be considered as the most secure model for α-stable noise carrier based RCS till now.

ÖZET

ALFA-KARARLI SÜREÜÇLER TABANLI RASSAL HABERLEŞME SİSTEMİ

Bu tez güvenli kablosuz haberleşme sistemlerine alternatif olacak alfa kararlı (α-kararlı)taşıyıcı tabanlı rassal haberleşme (RCS) sistemi sunmaktadır.Bu nedenle ilk hedef daha önce sunulmuş alıcılara göre bit hata oranını (BER) daha iyileştirecek daha az hesapsal karmaşıklık gerektiren etkin bir alıcı içeren optimal bir (RCS) geliştirmektir. Daha sonra RCS sistemlerinde daha önce ele alınmamış senkronizasyon problemini çözümlemek için alfa-kararlı ortamlar için geliştirilmiş. Kesirli düşük-mertebeli kovaryans metodu literatürdeki ilk senkonize RCS (SRCS)'i sunmak üzere kullanılmıştır.Daha sonra bu sunulan SRCS'nin BER performansını arttırmak amacıyla alfa-kararlı gürültü taşıyıcının parametrelerinin en uygun değerleri hesaplanmıştır.

İkinci hedef de RCS'nin güvenilirliğini ve gizliliğini nitelendirip değerlendirecek kriterler geliştirmek olmuştur. Bu nedenle ilk önce literatürde varolan diğer RCS modellerinin güvenlikleriyle BER performanslarını karşılaştırmak için Güvenlik Performans Tercih Karakteristikleri (STPC) sunulmuştur. Sunulan optimize edilmiş RCS bu geliştirilen güvenlik ölçüsü (STPC)ne göre analiz edilmiş ve literatürde varolan tasarımlara göre daha güvenli olduğu gösterilmiştir. Ikinci aşama olarak RCS'nin güvenilirliğini nitelendirmek için bir kriter geliştirilmiş ve sunulan optimize edilmiş RCS "istenmeyen dinleyici"açısından incelenmiştir. Üçüncü aşamada RCS'nin olası kırılganlığını sınamak için istenmeyen dinleyicinin RCS'ye saldırıları tasarlanmıştır. Bununla birlikte RCS'nin güvenirliliğini arttırmak için gizlilik aralığı ve karşı tedbir ölçüleri için bir rehber belirlenmiştir.

Karşı tedbir ölçüsü rehberi geliştirdikten sonra tezde üçüncü aşama olarak α-kararlı gürültü ile sürülmüş doğrusal zamanla değişmeyen sisteme dayali verici ile bu doğrusal vericinin tersini alıcı olarak tasarlayan "Ters Sistem" tabanlı bir yeni RCS sunulmuştur. Bu Ters Sistem tabanlı RCS de saldırılara karşı daha az kırılgan yapısı nedeniyle varolan alfa-kararlı gürültü taşıyıcı tabanlı tüm RCS'lere göre daha güvenilir olarak düşünülmektedir.Tez içinde her aşamada yapılan benzetimlerden elde edilen sonuçlar yapılan çalışmaların kullanılabilme gücünü göstermek için sunulmuştur.

To my wife Rida and my sons Abyan and Raaed…..

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Tables **Page**

LIST OF ABBREVIATIONS

α-stable	Alpha-stable
ACR	Achieved Confidence Ratio
ARMA	Autoregressive/Moving Average
BER	Bit Error Rate
CDMA	Code Division Multiple Access
CR	Confidence Ratio
CM	Chaotic Masking
CSK	Chaotic Shift Keying
DCSK	Differential Chaotic Shift Keying
DDCSK	Differentially Differential Chaotic Shift Keying
DCSK-CS	Differential Chaotic Shift Keying (Code Shifted)
DCSK-HE	Differential Chaotic Shift Keying (High Efficiency)
DCSK-I	Differential Chaotic Shift Keying (Improved)
DCSK-MC	Differential Chaotic Shift Keying (Multicarrier)
DCSK-PMA	Differential Chaotic Shift Keying (Permutation based)
DCSK-PS	Differential Chaotic Shift Keying (Phase seperated)
DCSK-RM	Differential Chaotic Shift Keying (Reference Modulated)
DCSK-WC	Differential Chaotic Shift Keying (Walsh Code based)
DCSK-UWB	Differential Chaotic Shift Keying (Ultra Wideband)
DS-SS	Direct Sequence Spread Spectrum Communication
FH-S	Frequency Hoping Spread Spectrum Communication
FLOC	Fractional Lower-Order Covariance
FLOACB	Fractional Lower-Order Auto-Covariance Block
FLOCC	Fractional Lower-Order Covariance based Correlators
H-SS	Hybrid Spread Spectrum
LTI	Linear Time Invariant
MEVM	Modified Extreme Value Method
MSNR	Mixed Signal to Noise Ratio
PAS	Pilot Assisted Synchronization
PDF	Probability Density Function
RCS	Random Communication System

RCSR	Random Carrier Signal Recognizer
RCSRI	Random Carrier Signal Recognition Indicator
SB	Synchronization Block
SCS	Stochastic Communication System
SG	Signal Generator
SKαS-NSK	Skewed Alpha-stable Noise Shift Keying
SPTC	Security Performance Tradeoff Characteristics
SRCS	Synchronized Random Communication System
TCB	Threshold Control Block
TD	Threshold Detector
TH-SS	Time Hopping Spread Spectrum Communication

CHAPTER 1

INTRODUCTION

1.1. Overview

Security of communication systems has always remained a key topic among scientists, researchers and engineers associated with the field of telecommunications; where their huge emphasis has always been given to establish secure wireless communication systems. In the last few decades, physical layer secured wireless communication systems has gained much attention all over the globe which reflects the potential of the idea to ensure covert transmission. Due to the rapid growth and demand of wireless communication systems in the last decades, increment in inter and cross disciplinary approaches between wireless, vehicular, robotics, wearable electronics and nano devices, for building future communication systems are also on the rise. Similarly, the never ending amount of wireless communication devices, to explore, apply and create digital dividends to build a fully connected world in future, are also escalating the security concerns. Therefore, growing interest in enhancing the physical layer security of wireless communications systems indicates that this field has the capability to significantly eliminate the security problems for next-generation wireless communication systems.

Many conventional approaches have been used in the past to increase the security of classic sinusoidal carrier based wireless communication systems; spread spectrum (SS) communication is one of those as it works by maneuvering the parameters of conventional sinusoidal carrier Abdallah et al. (1991), Peterson et al. (1995) and Salehi, and Proakis (2007). SS communication based on Pseudo Random (PN) noise became popular due to their increased physical layer security as well as better BER performance. However, different algorithms, e.g. linear regression attack and exploiting the drawback of short linear complexity of SS signals in Tsatsanis and Giannakis (1997), Burel and Bouder (2000) and Burel, G. (2000), had been proposed later on to overcome the security provided by SS signals. This shortcoming had to be overcome by utilizing different types of noise like signals. This was the period when chaotic signals, i.e. non-periodic noise signals consisting of infinite number of states, were utilized to remove the weak holes in the security provided by SS systems. Among the unconventional approaches, chaotic communications became popular, after the discovery of the first method to synchronize chaos in 1991 by Pecora and Carroll (1990), as they used chaotic noise signals as carrier to encrypt the information content in the transmitted signals Oppenheim et al. (1992) and Dedieu et al. (1993) .However, chaotic communication systems besides having serious security vulnerabilities, proposed till now, are only able to hide the information content in the channel, but the eavesdroppers are aware of the existence of communication Sobhy and Shehata (2001). Due to the fact that the security of chaotic communication systems is derived in this way, many blind and semi-blind signal recognition techniques based on geometric forecasting approach, synchronizing circuits, auto-correlation, generalized synchronization, power analysis and signal filtering had been proposed to completely decode the information content hidden in the noise like chaotic carrier signals Short (1994), Short, K.M. (1996), Sobhy and Shehata (2001), Alvarez et al. (2004), Alvarez et al. (2004b) and Chien and Liao (2005),. The drawbacks in noise like chaotic carrier based communication systems established the need to introduce some actual noise carrier based communication systems.

Since, using noise signals as random carrier can not only hide the communication content, but it also makes the eavesdroppers unaware of its existence, hence, an eavesdropper has no idea whether a meaningful message is being sent or not Gu and Cao (2012). Therefore, efforts to use noise as a carrier to establish more secure spread spectrum communication system started in 1950's Basore (1952). However, a complete stochastic communication system based on stochastic process shift keying (SPSS) was first introduced by Salberg and Hanssen (1999). In their system, two different Autoregressive/Moving Average (ARMA) processes were used to send binary messages.

The α-stable noise, being the generalized version of the Gaussian noise, has the potential to be utilized as a random carrier as well as has the capability to be invisible in AWGN channel; where the invisibility is as severe as close the parameters of the transmitted α-stable random noise carrier to the parameters of the Gaussian noise present in the channel. However, detection and parameter estimation of α-stable random noise signals is considered to be a challenging problem in signal processing due to common characteristic properties of all heavy-tailed stable distributions which are i) the nonexistence of finite second or higher-order moments; ii) relatively high probabilities of large deviations from the median Nikias and Shao (1995). Moreover, α-stable noise signal waveform contains no repetitions or periodicities, so the pulse length is also hidden which makes it a natural candidate for secure communication. Therefore, many signal processing methods have been proposed in the past to estimate the related parameters of α-stable noise signals Ma and Nikias (1996), Tsihrintzis and Nikias (1996), Kuruoğlu (2001) and Kannan and Ravishanker (2007) or to model and estimate the number of α-stable distributions in mixture distributions Casarin (2004) and Diego et al. (2009) but utilizing them to perform covert transmission requires a priori knowledge of the utilized carrier signals. Therefore, the idea to use α-stable noise as random carrier to covertly convey the binary information provides physical layer security during transmission; which reduces the risk of eavesdropping.

This fact gave birth to symmetric and skewed α-stable random noise carrier based binary communication systems, i.e. random communication systems (RCSs) by Cek and Savaci (2009) and Cek (2015). Different receiver designs, signal detection and estimation schemes have also been utilized to increase the efficiency of RCSs; where it has also been analyzed that RCSs have the capability to perform covert transmission in fading channels as well by Cek (2015b), Xu et al. (2016) and Xu et al. (2017). However in this thesis, we have introduced an optimized model of RCS followed by the first criterion to quantify the covertness of α-stable noise based communication systems Ahmed and Savaci (2017) and Ahmed and Savaci (2017b). All studies related to RCSs have already assumed perfect synchronization; where no exact method was presented until we introduced the first method to synchronize RCSs followed by a criterion to optimize SRCSs Ahmed and Savaci (2018) and Ahmed and Savaci (2018b) which are also covered in the thesis as one of the key objectives. The security of the proposed models of RCSs is derived from the facts that i) even though α-stable mixtures can be separated by the Bayesian techniques presented by Ma and Nikias (1996) and Tsihrintzis and Nikias (1996), the pulse length cannot be estimated therefore α-stable random noise signals are undetectable or invisible to an eavesdropper; ii) the pulse length, i.e. duration of the carrier signal holding single binary information bit, needed for decoding is also hidden. These facts make it extremely difficult for an eavesdropper to blindly recognize and estimate the related parameter of α-stable carrier signals to retrieve the transmitted binary information.

In RCSs, decoding the received signal is considered extremely difficult without knowing the pulse length, i.e. duration of a single binary information bit. However, if the exact pulse length can be found then it would be possible for an eavesdropper to retrieve the binary messages hidden in the transmitted α-stable noise signals by one of the estimation methods given by Kuruoğlu (2001). Previously, there was not any attack, algorithm available to crack the hidden pulse length involved in conveying the binary information. In this thesis, the first attack, i.e. blind detection, recognition and data extraction method, for α-stable carrier signals has been proposed and analyzed from the perspective of an eavesdropper. The proposed attack first detects the possible presence of α-stable random carrier signals and then recognizes the associated impulsiveness and skewness parameters, exploited by the transmitter and the intended receiver, to extract covertly conveyed binary information. However, the covert range has also been prescribed which can be adopted to perform secure transmission by RCSs.

In order to assure true level of covertness by RCSs, an inverse system approach has also been adopted to design RCS as the main objective of the thesis which is prone to the proposed attack. Since, the newly developed RCS includes the mth-order linear time invariant (LTI) dynamical system with Sk-αSNSK signal generator (SG) at the transmitting end 'Alice' while the intended receiver 'Bob' uses the inverse LTI dynamical system of the transmitter with the modified extreme value method (MEVM) based estimator, hence, the parameters needed to decode the information carrying α-stable input has been increased from single parameter, i.e. pulse length, to the state parameters of the utilized LTI dynamical system as well. Hence, estimation of skewness parameter by an eavesdropper, without using the inverse system, will not reveal the true binary messages while the intended receiver truly decodes the binary messages. The improvement in security is shown by comparing the bit error rate performances of the intended receiver and an eavesdropper.

Therefore, in this thesis, the authors have tried to contribute a lot towards this field of RCSs which is still in its infancy. However, due to very small number of researchers working in this area, there is still a lot of work which can be done. These ideas or suggestion have been given in the end of this thesis. Before going further, the core of this thesis, i.e. α-stable noise or distribution, and its associated properties and parameter have been explained in detailed below.

1.2. Alpha-Stable Noise Distribution

Alpha-stable (α-stable) processes, especially Gaussian processes, have long being used as a useful tool to model various stochastic processes. Efforts to develop the theory of single variable stable distributions started in the 1920s and 1930s by Paul Levy and Aleksander Yakovlevich Khinchine. Classic form of stable distribution is covered in Gnedenko and Kolmogorov (1954) and Feller (1971), where it has been updated in monograph of Zolotarev (1986). A review of the state of the art on stable processes from a statistical point of view is provided by a collection of papers edited by Cambanis et al. (1991). The definitions, mathematical description and recent application of α-stable distribution are reviewed below.

Definition: As defined in Samorodnitsky and Taqqu (1994), if ≜ denotes equality in distribution and the relation

$$X_1 + X_2 + \ldots\ldots + X_n \triangleq C_n X + D_n \tag{1}$$

holds for a positive constant C_n and a real number D_n given that X_1, X_2, ……, X_n are independent and identically distributed random variables then X is said to follow and α-stable distribution.

1.2.1. Mathematical Description

The characteristic function of α-stable Levy noise $X \sim S_\alpha\ (\beta,\ \gamma,\ \mu)$ having α-stable distribution is expressed in Samorodnitsky and Taqqu (1994) as

$$\phi(\theta) = \begin{cases} \exp\{j\mu\theta - \gamma^{\alpha}\,|\theta|^{\alpha}(1 - j\beta sign(\theta) tan\left(\frac{\alpha\pi}{2}\right))\}\ if\ \alpha \neq 1 \\ \exp\{j\mu\theta - \gamma\,|\theta|(1 + j\beta\frac{2}{\pi}sign(\theta) ln\left(\frac{\alpha\pi}{2}\right))\}\ if\ \alpha = 1 \end{cases} \tag{2}$$

where

$$sign(\ x) = \begin{cases} -1 & if\ x < 1, \\ 0 & if\ x = 0, \\ 1 & if\ x > 1. \end{cases} \tag{3}$$

and the four related parameters are defined in the respective ranges as : the characteristic exponent α ($0 < \alpha \leq 2$), the skewness parameter $\beta(-1 \leq \beta \leq 1)$, the dispersion parameter γ ($\gamma \ \geq 0$) and the location parameter $\mu \in R$.

Remark 1: Gaussian, Cauchy and Levy distributions are the special cases of α-stable distributions defined as X ~ $S_{\alpha=2}$ $(\beta=0, \gamma, \mu)$, X ~ $S_{\alpha=1}$ $(\beta=0, \gamma, \mu)$ and X ~ $S_{\alpha=0.5}$ $(\beta = \mp 1, \gamma, \mu)$, respectively.

Note: The second or higher-order moments do not exist for $\alpha < 2$, moreover, the first order moment do not exist as well for $\alpha \leq 1$. The α-stable signals can be generated by utilizing the characteristic function of α-stable noise 'X', i.e. X ~ S_{α} (β, γ, μ), given in Janicki and Weron (1994).

Properties: Samorodnitsky and Taqqu (1994), Property 1.2.2 and 1.2.3,

Let X ~ S_{α} (β, γ, μ) and let h be a non-zero real constant. Then

$$h + \mathrm{X} \sim S_{\alpha}\,(\beta,\ \gamma,\ h+\mu) \tag{4}$$

and

$$h\,\mathrm{X} \sim S_{\alpha}\,(sign\ \{h\}.\beta,\ |h|\ \gamma,\ h\mu) \tag{5}$$

Types: The frequent occurrence of extreme values in the observed data of many actual physical phenomena is non-Gaussian, hence; they are considered as a random process and are modeled by α-stable distribution. However, symmetric α-stable (SαS) process indicates that positive and negative outcomes in the observed data are equally likely. However, Skewed α-stable (SkαS) process indicates that the observed data is biased towards either positive or negative outcomes. Therefore, α-stable distribution can be categorized in to two main types depending on the type of the parameter used to shape up its probability density function (PDF) as

1. Distribution dependent on α parameter is known SαS distribution which is shown in Figure 1.1.
2. Distribution dependent on β parameter is known SkαS distribution which is shown in Figure 1.2.

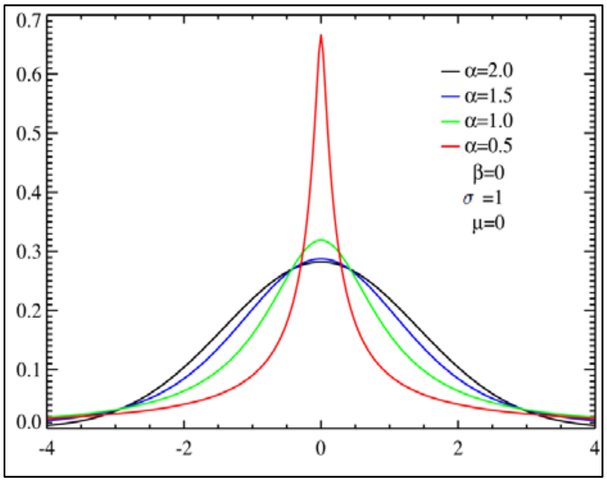


Figure 1.1. Symmetric α-stable distributions with unit scale factor

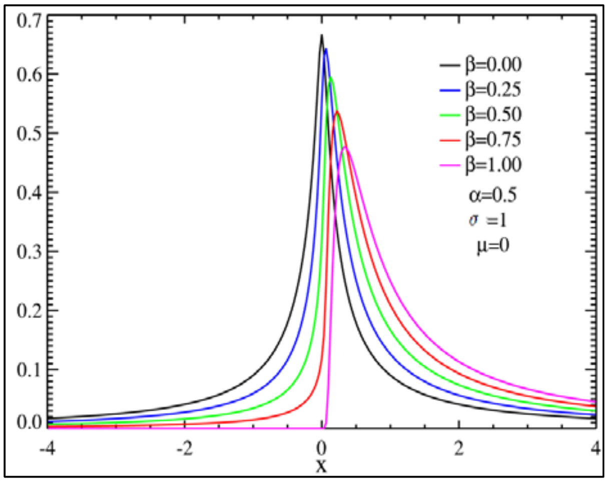


Figure 1.2. Skewed centered stable distributions with unit scale factor

1.2.2. Applications of Alpha-stable noise

As α-stable distribution is expected from superposition in natural processes, therefore it has been used in many hot areas for investigations. There are plenty of sources that follow or be modeled by α-stable distribution which includes seismic activity, ocean wave variability, lightning in the atmosphere, climatology and weather, surface texture, switching transients in power lines, telephone lines, acoustic emissions, etc.

Especially in communication, the α-stable distribution has variety of applications in many branches such as wireless, molecular, neural, deep space, underwater acoustics communications where it has been used extensively for mathematical modeling of impulsive channel noise Wang et al. (2011), Rajan and Tepedelenlioglu (2010), Kosko and Mitaim (2010) Farsad et al. (2015), He et al. (2014), Guo et al. (2008) and Banerjee and Agrawal (2013). The reason of using α-stable distribution in such versatile branches lies in the range of the associated parameter, i.e. the characteristic exponent 'α', that ranges from $0 < \alpha < 2$. Moreover, the Gaussian distribution, when $\alpha = 2$, is the most used distribution for modeling non-impulsive channel noise. For $\alpha < 2$, the distribution starts to become impulsive and non-Gaussian in nature where the tails of the distribution begin to become thicker. This impulsive nature makes α-stable distribution an attractive choice for modeling wireless signals and channel noise. The α-stable distribution is the only limiting distribution for sums of independent and identically distributed random variables according to the stability property of the generalized central limit theorem. However, the limiting distribution is Gaussian if the individual distributions have finite variance where the individual distributions have infinite variance for $\alpha < 2$ Samorodnitsky and Taqqu (1994).

1.3. Organization of This Thesis

The sections and subsections of this thesis have been briefly summarized where the synopsis of each chapter has also been given as follows:

In Chapter 2, the previous conventional and unconventional approaches, for enhancing the physical layer security of communication systems has been reviewed. Therefore, a general review of conventional sinusoidal carrier based spread spectrum communication systems has been presented where its sub types based on the PN sequence dependent manipulation of frequency and phase has also been explained. Similarly, the level of security achieved from the SS approaches has also been reviewed where its vulnerabilities in the light of previously introduced attacks has also been discussed. However, a general review of unconventional chaotic carrier based communication systems has been presented where its basic sub types, i.e. Chaotic Masking (CM) and Chaotic Shift Keying (CSK), has also been reviewed. The vulnerabilities of Chaotic Communication systems has also been discussed in the light of recently introduced geometric forecasting approach, synchronization circuits, auto-correlation, generalized synchronization, power analysis and signal filtering based attacks. Finally, the reasons to have stochastic noise based communication systems to achieve physical layer security have also been established.

In Chapter 3, the initial idea to use a basic stochastic noise based communication system, i.e. stochastic communication system (SCS), along with its merits and demerits have been explained where different receiver and detector designs for improving performance of the SCSs has also been highlighted. On the other side, the concept to use α-stable noise as random carrier by utilizing RCSs has been explained where the previously proposed different estimators based receivers has been reviewed and compared on the basis of BER. Finally, the future research pathways in this field have also been summarized.

In Chapter 4, the proposed optimized model of Random Communication System has been given which is based on the Modified Extreme value Method based Estimator. The BER performance of the proposed model has also been compared with previously proposed receivers. Moreover, the section 'Synchronized Random Communication System' introduces the first method to synchronize RCSs which is based on Fractional Lower Order Covariance (FLOC) technique. Therefore, the evaluated general behavior of FLOC in α-stable noise environments has also been added as a subsection which is the key facilitator in establishing SRCSs. Finally, a criterion to optimize SRCS has also been proposed in this section which enhances the BER performance by maneuvering the associated parameters of α-stable noise carrier.

In chapter 5, the security and covertness analysis of the proposed optimized model of RCS has been carried out where initially the first Security Performance Tradeoff Characteristics (SPTC) and the first Covertness criterion to quantify the covertness of RCSs have been introduced. However, the first attack to highlight the vulnerabilities of RCSs has also been included as a separate section which indicates the weak links in RCSs. Moreover, some important points to further strengthen the security of RCSs have also been added as a subsection. Finally, following the guidelines, the possible configuration of the most optimized and secure RCS has also been introduced as a last section of this chapter.

Finally in Chapter 6, the conclusive remarks on the current and future research directions on open problems related to RCSs are presented as potential pathways.

CHAPTER 2

PHYSICAL LAYER SECURITY FROM CONVENTIONALAND UNCONVENTIONAL COMMUNICATION SYSTEMS

Investigations to increase the covertness by strengthening the security of physical layer began in 1950s Basore (1952). Spread spectrum (SS) communication was the first step towards achieving covertness in physical layer secured communication systems. Later on, chaotic communication laid the basics of chaotic carrier based communication systems. The inspiration of chaotic communication arose from the major advantages provided by chaotic signals which have inherent resistance to eavesdropping at the time of its discovery. However, afterwards, different techniques were also presented to infiltrate chaotic communication systems as well. In this chapter, we have provided brief insight into these communication systems and have reviewed them on the basis of their vulnerabilities computed by different proposed attacks. Moreover, common problems and future challenges related to the physical layer secured communication systems have also been highlighted.

In this chapter, entire information related to SS communications and chaotic communications has been briefly provided in a tutorial style. However, the topics, not in harmony with the objectives of the thesis, have been left out in support of detailed explanation of relevant ones. However, we have at least pointed out every topic in conjunction with references mentioning the relevant material

2.1. Overview

Physical layer secured communication systems play a vital role in civil and military applications. It has always being investigated to ensure the confidentiality of the communication between the legal transmitter and the intended receivers rather than intruders. Previously, jamming was considered as the most effective method to avoid eavesdropping at the physical layer in wireless communication systems. However, in this chapter, several prevailing types of communication systems, to enhance the security at the physical layer for wireless communication, have been reviewed. We classify these methods as conventional and unconventional based on their utilized form of carrier waveforms. First, we have briefly explained their working principle and the type of carrier used to achieve security and then we have discussed their sub types. Finally, we illustrate their effectiveness and security mechanisms. Several physical layer secured SS communication systems which utilize pseudorandom noise and chaotic noise have been discussed in terms of their abilities to improve the security of wireless communication systems where their vulnerabilities have also been highlighted. Due to the pointed security deficiencies of SS and Chaotic Communications systems, the need of an alternate way of performing covert communications at the physical layer have also been emphasized. Therefore, in the last section, the chapter has been concluded with remarks to improve the physical layer security by adopting stochastic noise based communication systems.

2.2. Conventional Spread Spectrum Communication Systems

Spread Spectrum (SS) communication, as defined in Pickholtz et al. (1982) and Salehi and Proakis (2007), provides a mean of covert transmission by spreading the transmitted signal bandwidth. Additionally, pseudo randomness is utilized to produce the transmitted signal consisting of spectrum approximately identical to the stochastic noise and seems resistant to eavesdropping. However, the SS communication systems fall in the category of conventional communication systems because they maneuver the parameters of conventional sinusoidal carrier to covertly convey the underlying hidden binary information.

2.2.1. Methodology

As shown in Figure 2.1, a separate signal obtained as Pseudo random Noise (PN) is exploited to broaden the spectrum of the transmitted signal, i.e. binary information signal added with the PN. The PN signal is not dependent on the incoming binary signal. The receiver separates the binary information from the PN signal by generating the same PN signal. The bandwidth of the transmitted signal, binary information signal added with the PN signal, is extremely greater than the conventional binary information signal.

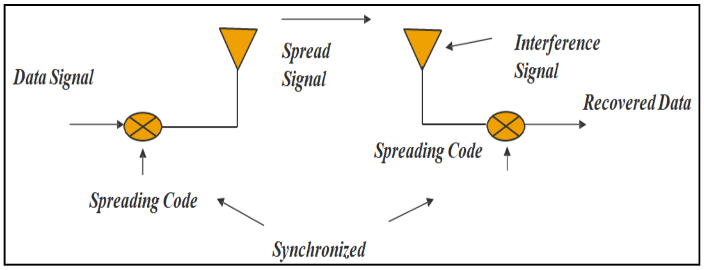


Figure 2.1. SS based Communication System (Source: Salehi and Proakis 2007)

2.2.2. Types of SS Communication Systems

SS communication has been divided into four main types which has been given in Pickholtz et al. (1982) and recently stated in Salehi and Proakis (2007) as

- Direct Sequence Spread Spectrum Communication (DS-SS) – In which the binary information signal phase is manipulated by the PN signal.
- Frequency Hopping Spread Spectrum (FH-SS) - In which the binary information signal frequency is manipulated by the PN signal.
- Time Hopping Spread Spectrum (TH-SS) - In which the binary information

signal initiation time is manipulated by the PN signal.

- Hybrid Spread Spectrum (H–SS) - Grouping of DS- SS, FH-SS, TH-SS.

2.2.3. Security and Vulnerabilities of SS Communications

The SS communication assumes to provide covertness as well as it allows overcoming the channel impairments like multipath distortion, fading, noise, interference and attenuation. Therefore, in the beginning, it was a unique way of signal encryption by utilizing the concepts of physical layer. Moreover, it also optimizes the bandwidth utilization with decreased interference.

According to the mechanism of DS-SS communications, the bandwidth of the transmitted signal is broadened by utilizing pseudorandom sequence. Therefore, multiple accesses are orthogonal to each other which guarantee its usefulness, hence, SS communication is considered as the backbone of CDMA communication systems. However, it is difficult to assure the synchronization of the entire system as the quantity of users utilizing the communication link is also large.

Nonetheless, SS communication based on PN noise became popular due to their increased physical layer security as well as efficient BER performance. Later on, different algorithms, e.g. linear regression attack, exploiting the drawback of short linear complexity of SS signals had been proposed Peterson et al. (1995), Tsatsanis and Giannakis (1997), Burel and Bouder (2000) and Burel, G. (2000). This shortcoming can be overcome by utilizing different types of noise signals. Therefore, chaotic signals, i.e. non-periodic noise signals consisting of infinite number of states, can be utilized to remove the weak holes in the security provided by PN based conventional SS communication systems.

2.3. Unconventional Chaotic Communication Systems

After Shannon's discovery in Shannon (1949) that the maximal entropy of noise can increase the channel capacity of communication systems, the area of chaotic communication systems has attained significant interest of the groups involved in establishing covert transmission by unconventional communication system. It was Chuas who first studied the concept and developed the practical chaotic electrical circuit in 1980 Chua, L. O (1980). Later on in Pecora and Carroll (1990), the authors proposed the first method to synchronize chaos, which then started a series of investigations related to the chaotic communication systems.

Since, chaotic maps are highly sensitive to initial conditions; hence, they enable them to produce an infinite amount of uncorrelated noise signals. Therefore, they are also highly effective to become likely nominees for multi-user SS communication systems Lau and Tse (2003), Kurian (2005), Vali et al. (2012), Vali et al. (2012b), Berber and Feng (2013) and Kaddoum et al. (2013). It has been discussed in detailed in Hasler and Schimming (2002) that no elementary principle of conventional communication contradicts the phenomenon of using chaos in digital communications. Moreover, it has been observed in Xia et al. (2004), Yu and Yao (2005) and Lynnyk, V. and Celikovsky, S. (2010) that chaos based modulation schemes perform extremely well in comparison to the SS communication schemes, which involve alleviation of fading in multipath environment, jamming resistibility, interception resistibility, hence, provides covert communications.

Chaotic communications is now considered as a separate field in covert communications research focusing on enhancing physical layer security. From the learning of chaotic dynamical systems, chaotic behavior has been evolved to chaotic communications with applications ranging from signal processing, cryptography, neural networks etc. The reason of rapid increase in this area is straightforward: complex behavior of chaotic dynamical systems, however, it can be observed in fairly simple manner in legal master and slave systems. Due to the broadband, uncorrelated and a-periodic behavior of chaotic systems, its prediction is highly unlikely for longer duration. These characteristics are in accordance with the considered necessities for carrier signals exploited in communication systems, especially to achieve or enhance the physical layer security.

2.3.1. Methodology

Chaotic systems were assumed to be as non-synchronized systems before late 1990's as it is stated that the trajectories of two identical chaotic systems quickly become uncorrelated even if started at nearly the same initial conditions. However, Pecora and Carroll comes up with the possibility of designing chaotic systems in a way showed who proved both theoretically and experimentally that the second system, i.e. slave system, called the response system can receive some of the state variables transmitted by first chaotic system, i.e. master system, called the driving system. Hence, the two systems can be synchronized by forcing the state variables of the slave system to synchronize with the other state variables not passed to the slave system. The concept was proven both theoretically and experimentally in Pecora and Carroll (1990), Pecora and Carroll (1991), Carroll and Pecora (1991) and Pecora and Carroll (1991b).

Establishing synchronization in chaotic systems by Pecora and Carroll was considered as a breakthrough in communication systems especially in signal processing communities. Chaotic Masking (CM) and Chaotic Shift Keying (CSK) were the first application of chaos in communication systems which were reported in Oppenheim et al. (1992) and Parlitz et al. (1992). They performed covert transmission by adding a chaotic signal to a speech signal and then the concept of synchronization effect can be utilized to recover the noise-like transmitted chaotic signal, hence, resulting in transmitted speech signal is simply applying subtraction. After that, another idea to perform covert communications by adopting CM was proposed in Kocarev et al. (1992) where the Chua's circuit was utilized to produce chaotic signals. They further proved the synchronization effect in chaotic systems by practical experiments by hiding the information signal in the transmitted chaotic signal. However, the idea of performing covert communications relies on the condition that the power of the chaotic signal should be higher than that of the information signal.

2.3.2. Types of Chaotic Communication Systems

There are two major branches of analog chaotic communication systems as defined in Kaddoum (2016) as

Coherent detection schemes: It involves a synchronized version of the chaotic carrier produced by the receiver. The detection procedure is performed by utilizing the replica of the transmitted signal in different methods Dedieu et al. (1993), Parlitz et al. (1992) and Kolumbán (1997). The basic type of coherent chaotic communication scheme is CM which has been shown in Figure 2.2.

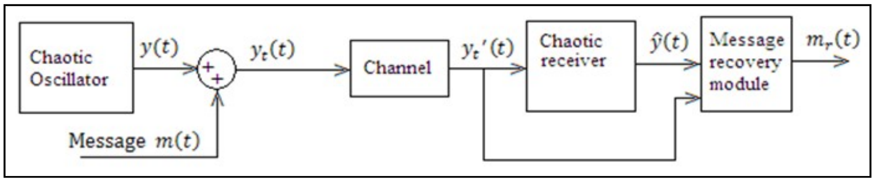


Figure 2.2. Chaotic Masking Scheme based Communication System (Source: Dedieu et al. 1993)

Non-coherent detection schemes: It involves data recovery by performing the detection of the received signal without the need of any synchronized version of the chaotic carrier for the receiver Kennedy (2000) and Kennedy (2000b). The basic type of non-coherent chaotic communication scheme is CSK which has been shown in Figure 2.3.

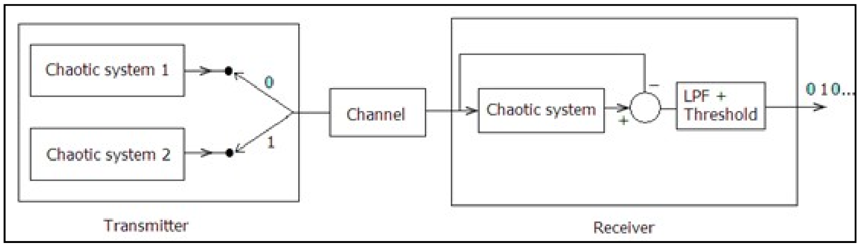
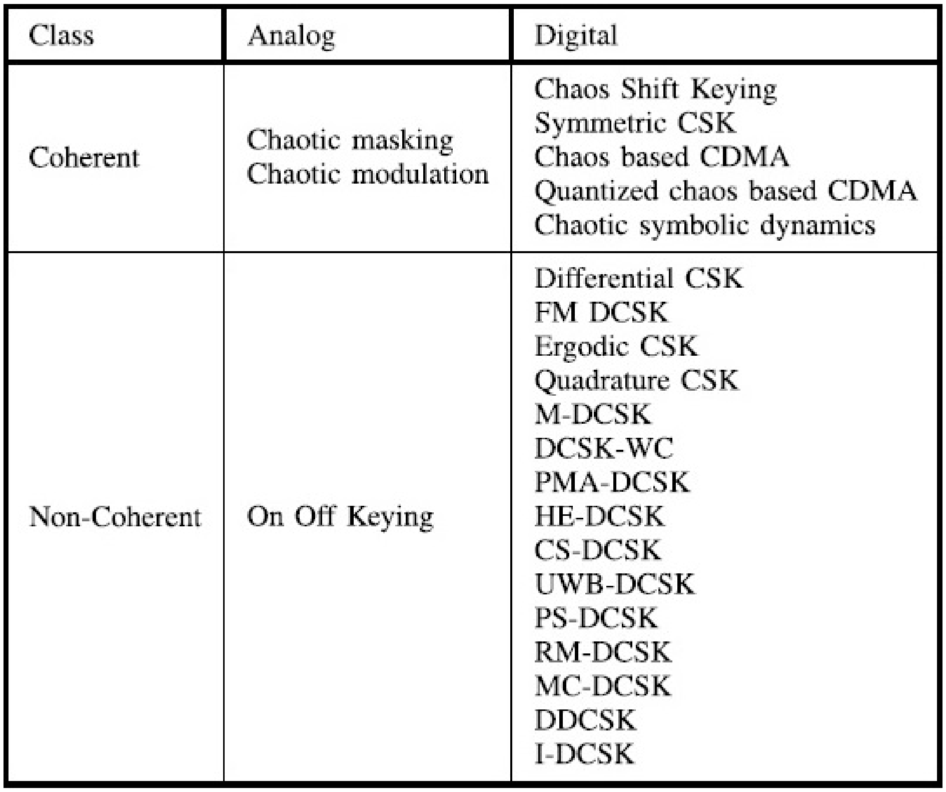


Figure 2.3. Chaotic Shift Keying based Communication System (Source: Parlitz et al. 1992)

Chaotic communications has been further classified in Table 2.1 which summarizes different analog modulation classes and their corresponding proposed chaos-based modulation schemes Kaddoum (2016).

Table 2.1. Classification of Chaotic Communication systems (Source: Kaddoum 2016)



Class	Analog	Digital
Coherent	Chaotic masking Chaotic modulation	Chaos Shift Keying Symmetric CSK Chaos based CDMA Quantized chaos based CDMA Chaotic symbolic dynamics
Non-Coherent	On Off Keying	Differential CSK FM DCSK Ergodic CSK Quadrature CSK M-DCSK DCSK-WC PMA-DCSK HE-DCSK CS-DCSK UWB-DCSK PS-DCSK RM-DCSK MC-DCSK DDCSK I-DCSK

2.3.3. Physical Implementation

Regarding the Physical Implementation of chaotic communication systems, it has already been carried out which increases the practicality of utilizing noise like signals for establishing secure communication systems at the physical layer. Some of the chaotic systems which have been developed and assessed under ideal and non-ideal channel conditions have been given below as

1) Chaotic encryption technique based on the inverse-system has been

experimentally demonstrated with indoor radio transmission Kelber et al. (1996);

2) Chaotic encryption technique based on the inverse-system has been implemented in digital-signal processor and wire link Dmitriev et al. (1998);

3) Chaotic pulse position modulation technique has been experimentally demonstrated in indoor radio transmission Sushchik et al. (2000);

4) Chaotic encrypted codes in multiuser CDMA system in wire link Agnelli et al. (2001);

5) Chaotic Shift keying technique in indoor radio transmission Dmitriev et al. (2001);

6) Differential Chaotic Shift keying frequency-modulation technique in radio link by channel simulator Król et al. (2001).

The above examples reflect that significant efforts has already been done to physically implement chaotic communication systems which paves the way for future research in physical layer security enhancement via unconventional communication systems.

2.3.4. Security and Vulnerabilities of Chaotic Communication Systems

So far, two methods, i.e. SS and chaotic communications, to enhance the security of communication systems at the physical layer have been discussed. Both of them work by shifting narrowband signals to a wideband configuration. Chaotic communication is the first unconventional communication system at the physical layer which has been physically tested but they lack in BER performance in comparison to classical communication systems Abel and Schwarz (2002). Nonetheless, the achieved security of chaotic communication systems is higher than SS communication as shown in Kong (2015) which was the main objective at the time of its arrival, hence; they were considered secure at the beginning. Nowadays, there are many investigations available which highlights the weak links in chaotic communications and provides possible method to break the security of these systems. However, some significant investigations, e.g. Short (1994), Short, K.M. (1996), Yang et al. (1998), Sobhy and Shehata (2001), Alvarez et al. (2004), Alvarez et al. (2004b) and Chien and Liao (2005), has better highlighted the low level of security in chaotic communications systems which reflects that it is no longer a robust method to achieve security at the physical layer. The key vulnerabilities of chaotic communication systems revealed in the selected investigation have been briefly reviewed below.

In the first study Short (1994) conducted by the Nonlinear Dynamics (NLD) Research group at the Naval Research Lab in USA, three different information signals, i.e. chaotic signal other than the carrier signal, period doubled signal and triangular wave, masked through the chaotic carrier were tested and every time the power spectrum of the hidden signal was found out by subtracting the geometrically forecasted carrier NLD from the received signal where the utilized density of the information signal to the chaotic carrier signal was up to -30 dB. Moreover, further methods were utilized to completely unmask and recreate the three utilized information signals hidden in the transmitted chaotic carrier with almost complete accuracy.

Similarly in Short, K.M. (1996), the transmitted signals, generated from the Lorenz system based chaotic transmitter, are processed from the perspective of an eavesdropper where the x-coordinate of the utilized generator was utilized for information masking. Therefore, it has been shown that the message sinusoidal signal can possibly be extracted if the eavesdropper decodes the x-coordinate. Moreover, detailed extraction of phase-modulated and frequency modulated chaotic signals have also been shown where the spectrum of the underlying information signal has been unmasked by the utilized prediction process. Therefore, the results in Short (1994) and Short (1996) declares the basic chaotic masking or chaotic switching techniques as unsecure due to the comparatively simple geometric structure of a low-dimensional chaotic attractor where the possibility of extraction the various utilized measures always exists, hence an eavesdropper may well be able to reveal the underlying information message.

The security of a general chaotic switching scheme, in which the information signal is switched by two different chaotic generators, has been thoroughly analyzed in the study Yang et al. (1998). Simple examples have been utilized to establish the robustness of proposed generalized synchronization method in breaking different chaotic switching systems where an eavesdropper with no knowledge of the parameters and structure of the chaotic transmitter in chaotic switching schemes can extract the hidden information signal. Moreover, it has also been shown that the utilized method is not dependent on the order of the transmitter as the simulations for both high and low order transmitters has also been included, hence, the level of security of chaotic switching systems will be still less even if the transmitter based on two hyper-chaotic systems has been utilized.

With the progress and acceptability of the above signal processing methods to unmask chaotic switching and chaotic masking techniques, researchers also started to propose potential attacks for breaking chaotic communication systems. The first attack in Sobhy (2001) proposes to reveal the hidden information message by plotting the received against the time delayed version of it or by plotting the autocorrelation function of the time series. Both cases would result in unique observations after comparing them with complied list of results which can be used to find out the utilized chaotic generator in the transmitter. Later on, the system and its inverse can be built to apply the decoding process.

Similarly another potential blind attack to break chaotic parameter modulation has been proposed in Alvarez et al. (2004). It has been shown that the claimed security of the utilized chaotic system can be compromised to an eavesdropper who has negligible knowledge of the system, i.e. the detection has been made with no knowledge of encryption method of non-linear time-varying system, nor its keys or parameters values. The eavesdropper without any chaotic receiver can reveal the information message by short time power analysis of the received signal. Firstly, the received signal is squared and then passed through four pole Butterworth low pass filter and then quantized with an inverting Smith-trigger. The binary information can then be revealed from the resultant signal.

Another study, i.e. Alvarez et al. (2004b), has analyzed the low level security of both chaotic communication and synchronization where the authors has pointed out the vulnerabilities of chaotic masking and chaotic modulation scheme done through Lorenz generators. The proposed attack is also blind where the eavesdropper has no knowledge of the transmitter's structure and the underlying chaotic system parameters.

2.4. Conclusive Remarks

The attacks and the related analysis discussed above have raised some serious questions on the security achieved by employing chaotic communications. Although, some counter measures guidelines and intelligent design techniques have been given in Chien and Liao (2005) to improve the security of chaotic communication systems, but the point to ponder is that all the chaotic communication systems, proposed till now and discussed above, even with no vulnerabilities are only able to hide the information content in the channel, but the eavesdroppers are aware of the existence of communication Sobhy and Shehata (2001). Therefore, no matter how much robust chaotic communication is proposed, still, it would be visible to the intruders and unwanted listeners. Due to this fact that the security of chaotic communication systems is derived in this way, many much more efficient blind and semi-blind signal recognition techniques will also be proposed in the future as well. Therefore, chaotic communication can no longer be considered as the most secure way of communication at the physical layer. The drawbacks in noise like chaotic carrier based communication systems have established the need to introduce some actual noise based communication systems.

CHAPTER 3

STOCHASTIC NOISE BASED COMMUNICATION SYSTEMS

Communication systems which either uses noise like signals or actual noise signals as carriers to transmit information falls under the category of unconventional communication systems due to non-utilization of conventional sinusoidal carrier signals and no alteration of any aspect of deterministic carrier signal for transmitting base band digital information. Among unconventional communication systems, random or stochastic noise carrier based communication systems have been utilized in the past to ensure covert transmission which have been reviewed in this chapter. However, the main objective of this chapter is to discuss the previously introduced α-stable noise carrier based communication systems where different receiver designs, proposed in the past, to enhance the performance of these α-stable noise carrier based communication systems, has also been discussed in detail. Moreover, their performances and drawbacks has also been highlighted which can help to design more better receivers for α-stable noise carrier based communication systems. Additionally, potential research pathways have also been given in the last section and many of them have extensively been touched in the later chapters of this thesis.

3.1. Stochastic Communication Systems

If stochastic processes are utilized as carrier in place of deterministic waveforms for a digital communication keying concept then the corresponding system is termed as Stochastic Communication Systems (SCS) [Salberg and Hanssen (1999)]. Higher degree of security and reduced risk of eavesdropping unlike conventional digital communication systems are considered as the main benefits of SCSs where the non-coherent receivers, simpler than spread spectrum and chaotic counterparts, are an added advantage.

Conventional digital communication keying concept implies amplitude shift keying, phase shift keying and frequency shift keying for transmission of baseband information where the intended receiver uses some estimation criterion to identify the modulated parameter of deterministic carrier signal followed by a decision rule to categorize the received signals. The communication keying methods based on the above concept do not provide any security against intruders. Additionally, utilizing spread spectrum (SS) communication systems discussed in the previous chapter, for spreading the signal bandwidth by utilizing PN codes for encoding and decoding at the transmitter and receiver, respectively, require exact synchronization and absolute understanding of the PN sequence Gibson (1993) which is a drawback of SS communication systems. Similarly, chaotic communication systems like SS communication systems also exploit self-synchronization property of certain chaotic oscillators to achieve strict synchronization before initiating the decoding process which is also a tiring procedure for practical communication Hayes et al. (1993).

3.1.1. Stochastic Process Shift Keying Encoding

Salberg and Hanssen (1999) first introduced the concept of SCSs which was solely based on the use of ARMA stochastic processes. The method was further generalized in Salberg and Hanssen (2000). In Salberg and Hanssen (1999), the technique which utilizes noise like stochastic process $X_0(t),\ 0 < t < T$ to transmit binary information bit '0' and $X_1(t),\ 0 < t < T$ to transmit binary information bit '1' for encoding digital information is named Stochastic Process Shift Keying (SPSK) which results in two subsequent equal and different source bits have entirely different and similar transmitted waveforms, respectively as the realizations of two different stochastic processes are close in a statistical sense. Thus an extra layer of security is added in the transmitted waveform due to the hidden pulse length and absence of discontinuities, repetitions and periodicities. The author utilized ARMA processes, however there are many alternative to ARMA processes that could be utilized for SPSK concept, e.g. flicker-noise ($\frac{1}{f^{\gamma}}$-noise) processes with-different spectral exponents γ_1 and γ_2 and bilinear and nonlinear processes.

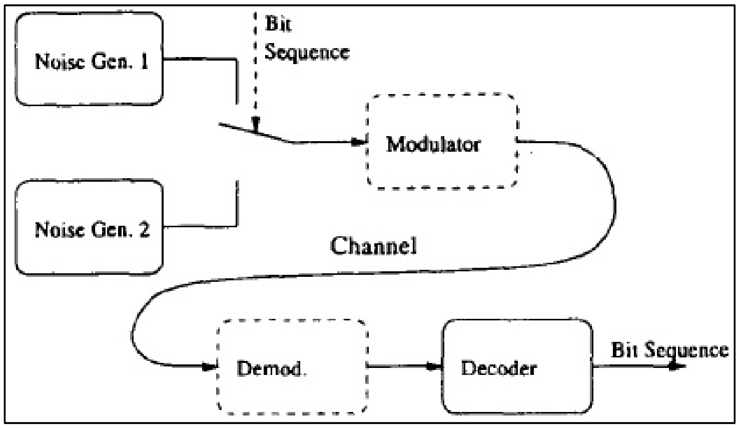


Figure 3.1. Block diagram of SPSK communication system (Source: Salberg and Hanssen 1999)

In Figure 3.l, the block diagram of a real-time SPSK communication system has been shown. The transmitter has known characteristics and can be considered as a source of two different noise generators where the source bit stream guides the transmitted waveform to generate the noise waveforms for the corresponding binary information bits ‘0’ and ‘1’ by alternating between the generators by a fast low-noise switch. The switch controls both the noise generators for sending source bits where T is the period or the pulse length of the switch known only to the transmitter and the intended receiver. The stochastic processes can also be generated digitally before transmission to an alternative to analog noise generators as shown in Figure 3.l.

Another possibility to design more robust SPSK communication system is utilize stochastic processes $X_0(t)$, and $X_1(t)$ with different bi-spectral densities (e.g., Nikias and Petropulu (1993) and same power spectral densities, hence, the digital information can be encoded by bi-spectral densities of the processes. This attribute of encoding information with different bi-spectral densities would result in SPSK communication system not sensitive to symmetrical amplitude probability density function based additive colored noise, hence, resulting in enhanced natural security against additive Gaussian noise.

The SPSK, shown in Figure 3.1, can also be referred as ‘carrier free’ communication system if no modulation is carried out on the transmitted waveform where the choice of modulating the transmitted waveform before transmission is always possible. The transmitted waveform can be modulated by modulating phase, frequency and amplitude depending on the purpose of SCS. Moreover, the effect of a possible jammer can also be minimized if broadband stochastic processes are utilized which results in transmitting a physical signal of a wide frequency band.

3.1.2. Decoding of Stochastic Processes

The decoding process for the SPSK when utilizing linear Gaussian processes as a carrier, were first given in Salberg and Hanssen (1999) which has been reviewed in this section.

Let say we have a received data vector X = $[x_1, x_2, \cdots, x_n]^{\mathrm{T}}$ containing samples of the Gaussian stochastic process which has been obtained according to the relation given below as

$$X = S + N \tag{6}$$

where S is a transmitted vector containing information samples generated from a stochastic process and N is a white noise vector independent of the stochastic process. S and N have means equal to zero. Furthermore, S has a covariance matrix $\mathbf{R}_{\mathrm{s,i}} = E\{SS^{\mathrm{T}}|\Omega_{\mathrm{i}}\}$where Ω_{i} is class i={0, 1} and N has a covariance matrix equals to $\sigma_{\mathrm{n}}^2\mathbf{I}$. Therefore, the mean of X is also equal to zero and covariance matrix $\mathbf{R}_{\mathrm{i}} = \mathbf{R}_{\mathrm{s,i}} + \sigma_{\mathrm{n}}^2\mathbf{I}$.

The intended receiver has to select $\Omega_0$when

$$\mathrm{P}\ (\Omega_0|\mathrm{X}) > \mathrm{P}\ (\Omega_1|\mathrm{X}) \tag{7}$$

and vice versa if he has to communicate with minimum error probability 'P_e'. The likelihood function can be written as

$$\mathrm{P}\ (\mathrm{X}|\Omega_0) \underset{\Omega_1}{\overset{\Omega_0}{\gtrless}} \mathrm{P}\ (\mathrm{X}|\Omega_1) \tag{8}$$

and log-likelihood function can be written as

$$L(\mathrm{X}) = \log\frac{\mathrm{P}\,(\mathrm{X}|\Omega_0)}{\mathrm{P}\,(\mathrm{X}|\Omega_1)} = \mathrm{X}^{\mathrm{T}}\,(R_0^{-1} - R_1^{-1})\mathrm{X} + \tau \underset{\Omega_1}{\overset{\Omega_0}{\gtrless}} 0 \tag{9}$$

where $\tau \ = \ \log\frac{|R_0|}{|R_1|}$ and P (Ω_0), P (Ω_1) are a-priori probabilities while using Bayes rule.

The log-likelihood ratio has been reduced to S_n according to Fukunaga and Krile, (1969) and evaluated at time ‘n’ as

$$S_n = \sum_{k=1}^{n} \frac{1}{2}\log\frac{\sigma_0^2}{\sigma_1^2} + \frac{\left(\epsilon_k^0\right)^2}{2\sigma_0^2} - \frac{\left(\epsilon_k^1\right)^2}{2\sigma_1^2} \tag{10}$$

where ϵ_k^{i} for i = 0, 1 are the innovation sequences defined as

$$\epsilon_k^{\mathrm{i}} = x_k - \hat{x}_{k|k-1,\theta_i} \tag{11}$$

and $\hat{x}_{k|k-1,\theta_i}$ is the MMSE estimate of x_k can be calculated by the Kalman filter in Scharf, (1991) as they are based on parameters of $X_i(t)$.

Therefore, the transmitted sequence can be decoded asynchronously by an intended receiver after studying the sign of the derivative of the log-likelihood ratio as the log-likelihood ratio S_n increases and decreases when binary information bit ‘1’ and ‘0’ are sent.

3.1.3. Receiver designs for SPSK

It has been shown in the last section that covertness can be ensured in digital communications in a straightforward fashion by employing SPSK. By transmitting noise like waveforms, generated from realizations of a stochastic process, the transmitted waveform has been further explained by a more prominent mathematical interpretation. Moreover in order to design better receiver for noise based communication systems, a subspace detector, proposed in Salberg and Hanssen (2001), for the SPSK has also been reviewed in this section.

3.1.3.1. Subspace Detector for SPSK

For a SPSK technique proposed by Salberg and Hanssen (1999) and Salberg and Hanssen (2000), the transmitted waveform $X(t)$ can be better represented by a mathematical relation given in Salberg and Hanssen (2001) as

$$\mathrm{r}X(t) = \sum_{n=-\infty}^{\infty} \sum_{k=1}^{K} x_n(k)\emptyset_k(t - nT_s) \tag{12}$$

where $x_n = [x_n(1), x_n(2),\cdots, x_n(K)]^{\mathrm{T}}$ is a random vector and $x_n(k)$ is its *k*th element. Similarly, the $\emptyset_k(t)$ is a *k*th basis function. The *n*th symbol from a received continuous time pulse $\mathbf{r} \in \mathbb{L}^{\mathbf{2}}$ can be represented by

$$\mathbf{r} = \sum_{k=1}^{K} x_n(k)\emptyset_k(t) + \mathbf{n} \tag{13}$$

where $\mathbf{n}$ is a WGN process and $\emptyset_k(t) \in \mathbb{L}^{\mathbf{2}}$ corresponds to $\emptyset_k(t)$. The received vector is

$$\mathbf{y_n} = \mathbf{x_n} + \mathbf{n} \tag{14}$$

where $\mathbf{y_n} = G(\mathbf{r}), \boldsymbol{G} : \mathbb{L}^{\mathbf{2}} \rightarrow \mathbb{R}^{\boldsymbol{K}}$ is a established vector obtained by correlation of r and elements of a basis $\mathbf{B} = [\mathbf{b_1}, \mathbf{b_2},\cdots, \mathbf{b_K}]^{\mathrm{T}} : \mathbf{b_i} \in \mathbb{L}^{\mathbf{2}}$. Therefore,

$$\mathbf{y_n} = G(\mathbf{r}) = (\mathbf{r}, \mathbf{B}) \tag{15}$$

can be termed as a coordinate vector of **r** with regard to the basis **B** during the transmission of *n*th symbol. The decoding can be carried out easily if selected **B** is orthonormal to the signaling waveforms **Φ**

$$(\mathbf{\Phi}, \mathbf{B}) = \mathbf{I}_{\boldsymbol{K}} \tag{16}$$

where $\mathbf{I_K}$ denotes $K \times K$ matrix.

The received vector $\mathbf{y_n}$ facilitates to recognize the received bit as ‘0’ or ‘1’. The matched subspace detectors introduced in Scharf (1991) are the most appropriate detectors as the transmitted vectors are the subspace signals. The decision criterion is not dependent on the additive noise variance which is the main advantage of subspace detectors. The orthogonal projection vector as introduced in Scharf (1991) has been used in Salberg and Hanssen (2001) to develop a projection vector such that $\mathbf{P}_{F_i}\mathbf{r}$ is a projection of $\mathbf{r}$ onto the subspace $(\mathbf{F}_i)$ where

$$\mathbf{P}_{F_i} = \mathbf{F}_i(\mathbf{F}_i^T\mathbf{F}_i)^{-1}\mathbf{F}_i^T : i = 0,1 \tag{17}$$

The decision is made by selecting class Ω_0 if

$$\mathbf{y}_\mathbf{n}^{\boldsymbol{T}}\mathbf{P}_{F_0}\mathbf{y}_\mathbf{n} > \mathbf{y}_\mathbf{n}^{\boldsymbol{T}}\mathbf{P}_{F_1}\mathbf{y}_\mathbf{n} \tag{18}$$

and vice versa. The received energy of the subspace $\mathbf{F}_i$ is measured by the detector and selects the subspace based on the level of energy, hence, resulting in the selection of the corresponding class.

3.2. Alpha-stable noise based SPSK

The SPSK, discussed in the previous section, is a novel technique to enhance physical layer security of communication systems. Since stochastic signals are noise like, it is really hard to determine the existence of information bearing content in the received noise signal Anfinsen (2001). Therefore, the idea to use noise like sequences started to gain further attention. Afterwards, it was observed in Hughes (2000), Yang and Petropulu (2003) and Win et al. (2009) that multiple access interference in a multi-user network such as wireless packet networks and networks with ultra wideband and narrow band systems and cognitive radio network results in SαS distribution. Since it was observed that the statistical characteristics of modulated signal and background interference are similar, this prompted Cek and Savaci (2009) to investigate the usage of SαS distributed sequence as noise carrier for covert communications.

3.2.1. Receiver Designs for Alpha-Stable noise based SPSK

The first SαS noise based SPSK technique proposed in Cek and Savaci (2009) was named ‘stable non-Gaussian noise parameter modulation’ due to the transmission of SαS noise as a carrier which had been transmitted with respect to the incoming message signal. Later on, SkαS distributed noise carrier was also utilized to encode binary messages in Cek (2015). Specifically, the Sα_iS and Skα_iS noise waveforms are transmitted in SαS and SkαS noise based SPSK techniques, respectively, for covert transmission of the binary information bit ‘i’ where $i \in \{0,\ 1\}$. Then, the corresponding noise sequences were transmitted through AWGN channel. The basic principle to propose SαS and SkαS noise based SPSK techniques lies in the exploitation of either the characteristic exponent ‘α’ of the SαS noise sequence or the skewness parameter ‘β’ of the SkαS noise sequence to encode binary messages which has been adopted in all the investigations conducted afterwards Xu et al. (2014), Xu et al. (2016) and Cek (2015b). At the intended receiver side, the estimation of the characteristic exponent ‘α’ or the skewness parameter ‘β’ is performed by different estimators followed by a hard decision to determine hidden binary messages. Different receivers had been proposed in the past to increase the efficiency of SαS and SkαS noise based SPSK techniques which have been comprehensively reviewed in the subsections given below.

3.2.1.1. Receiver based on SINC Estimator

Since, the receiver in SαS and SkαS noise based SPSK techniques has to estimate the modulated parameter of the transmitted noise carrier, the first receiver based on SINC estimator was proposed in Cek and Savaci (2009). The receiver decodes the received SαS noise carrier signal $x(k)$ by utilizing the SINC estimator, introduced in Kuruoğlu (2001), to estimate the characteristic exponent ‘α’ according to the relation given below

$$SINC\left(\frac{p\pi}{\alpha}\right) = \left[\frac{p\pi}{2}\left(\frac{A_pA_{-p}}{\tan p\pi/2}\right) + S_pS_{-p}\tan p\pi/2\right]^{-1} \qquad (19)$$

where $k = 1, 2, \cdots, T_b$ and T_b is the number of noise sample per binary information bit. Similarly, p is the order of the fractional moments where the fractional moments A_p and S_p can be computed by the relations given below

$$A_p = \frac{1}{N}\sum_{k=1}^{T_b} |x(k)|^p \tag{20}$$

And

$$S_p = \frac{1}{N}\sum_{k=1}^{T_b} sign(x(k))|x(k)|^p \tag{21}$$

3.2.1.2. Receiver based on Correlators

Another receiver based on the non-coherent demodulator had been proposed in Xu et al. (2014). The sent binary information bit is decoded by calculating the correlation function of the received noise waveform during bit duration T_b which is followed by a hard decision as shown in Figure 3.2. The output of the demodulator $Z_m(t)$ is given by

$$Z_m(t) = \int_{\frac{T}{2}}^{T} r(t) r\left(t - \frac{T}{2}\right) dt \tag{22}$$

where $r(t)$ equals the transmitted signal $x(t)$. Perfect synchronization has been assumed throughout. However, no channel noise has been assumed here. A very simple decision rule has been used, i.e. the estimated binary information bit is declared as ‘0’ or ‘1’ ‘if $Z_m(t)$ is greater or less than zero, respectively. The main benefit of the receiver shown in Figure 3.2 is that it avoids carrier recovery and synchronization issues. Moreover, the utilized decision rule is very simple which ensures fast data rate.

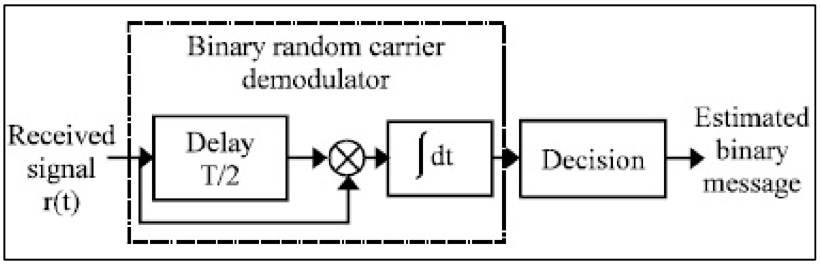


Figure 3.2. Receiver based on Correlators (Source: Xu et al. 2014)

3.2.1.3. Receiver based on Logarithmic Estimator

The main drawback of the receiver based on SINC estimator is that it requires inversion of the SINC function and selection of moment exponents. Moreover, SINC estimator requires large number of samples for accurate estimation of the modulated parameters ‘α’ or ‘β’ which comes brings upon a baggage of complex computations, hence, effects the speed of transmission. Therefore in Xu et al. (2016), the authors proposed a receiver based on logarithmic estimator in which they utilized logarithmic moments to estimate α. The intended receiver has to obtain the following moments

$$L_1 = \mathbf{E}[\log|\boldsymbol{X}|] = \Psi_0\left(1-\frac{1}{\alpha}\right)+\frac{1}{\alpha}(\log\frac{\gamma}{\mathbf{cos}\,\boldsymbol{\theta}}) \tag{23}$$

$$L_2 = \mathbf{E}[(\log|\boldsymbol{X}| - \mathbf{E}[\log|\boldsymbol{X}|)^2] = \Psi_1\left(\frac{1}{2}+\frac{1}{\alpha^2}\right)-\frac{\theta^2}{\alpha^2} \tag{24}$$

$$L_3 = \mathbf{E}[(\log|\boldsymbol{X}| - \mathbf{E}[\log|\boldsymbol{X}|)^3] = \Psi_2\left(1-\frac{1}{\alpha^3}\right) \tag{25}$$

where the polygama function values Ψ_{k} can be obtained by the relation given in Kuruoğlu (2001) as

$$\Psi_{k-1} = \left(\frac{d}{dx}\right)^k \log\Gamma(x)\,|_{x=1} \tag{26}$$

For precise estimation of ‘α’ in SαS noise based SPSK, centro-symmetrization given in

Kuruoğlu (2001) as

$$\boldsymbol{X}_K^S = \boldsymbol{X}_{2K} - \boldsymbol{X}_{2K-1} \sim S_\alpha\,(\beta{=}0,\, 2\gamma,\, \mu{=}0) \qquad (27)$$

has to be applied on the received data to obtain the transformed data. Then 'α' can be estimated by equating the sample moments and actual moments. However, the higher order moments are not very noisy. Therefore, the authors in Xu et al. (2016) have solved the moment's equation by setting $\theta = 0$. Similarly, the more clear representation for the estimates of α can be seen below

$$\alpha = \left(\frac{L_2}{\Psi_1} - \frac{1}{2}\right)^{-\frac{1}{2}} \qquad (28)$$

3.2.2. Performance Analysis of Different Receivers

The BER performances of receivers based on SINC, Correlators and logarithmic estimators have been reviewed in this section while few drawbacks of each approach have also been pointed out. The standard measure of signal strength in signal processing has always been associated with the power of a second-order process, i.e. $E[X^2]$. This term $E[X^2]$ is usually linked with the physical concept of energy and power to analyze the performance of conventional communication systems. However, it is inapplicable α-stable distribution, i.e. when the processes have heavy tails. Therefore, the strength of the process cannot be associated with its second-order power as it is always infinite in the special case of heavy algebraic tails.

Since, the AWGN channel power is also represented by its variance; therefore, measuring BER of intended receivers, against channel signal to noise ratio (SNR), is an effective criterion to measure the performances of conventional communication systems. However as discussed in Ma and Nikias (1995), second and higher order moments of α-stable distributions (excluding Gaussian distribution) do not exist, therefore, SNR can no longer be used to measure the quality of the channel in α-stable noise based communication systems. Therefore, there is a need for a special separate criterion which can serve the required purpose.

3.2.2.1. Performance Criterion

To solve the problem of non applicability of SNR for α-stable noise based communication systems, mixed signal-to-noise ratio (MSNR) have been introduced in Ma (1996b) which is defined below as

$$\mathrm{MSNR}_{dB} = 10\log\frac{\gamma}{\gamma_G} \tag{29}$$

where γ and γ_G are the dispersion parameters of the information bearing α-stable random carrier signal and the channel noise, respectively, while BER is the percentage of bits with errors divided by the total number of transmitted bits.

Similarly, geometric signal-to-noise ratio (GSNR) is another important criterion to analyze α-stable noise based communication systems which has been recently defined and used in Xu et al. (2016) as

$$\mathrm{GSNR}_{dB} = 10\log_{10}\frac{S_{0,\alpha}^2(X)}{S_{0,g}^2} \tag{30}$$

where $S_{0,\alpha}^2$ is the geometric power defined in Xu et al. (2016) as

$$S_{0,\alpha} = \gamma C_g{}^{\frac{1}{\alpha}-1} = e^{E[\log|X|]} \tag{31}$$

where $C_g \cong 1.78$ is the exponential of Euler constant. For example, let say the PDF of a Gaussian distribution is $f(x) = \frac{1}{\sqrt{2\pi}\gamma_g}e^{\frac{-x^2}{2\gamma_g^2}}$ and its geometric power is represented as

$$S_{0,g} = \frac{\gamma_g}{\sqrt{2C_g}} \tag{32}$$

3.2.2.2. Performance Evaluation

In order to practically implement SPSK techniques, better receiver designs are needed to first optimize SαS and SkαS noise based communication systems. Therefore, it is necessary to review the performances of previously proposed receivers in order to discuss their limitations. Therefore, BER of previous receivers based on SINC, Correlation and logarithmic estimators introduced in Cek and Savaci (2009), Xu et al. (2014) and Xu et al. (2014) has been compared in this sub-section where the BER have been computed against either MSNR_{dB} or GSNR_{dB}. In order to perform the comparative analysis of the three receivers, the receiver based on SINC estimator introduced in Cek and Savaci (2009) has first been compared with the Correlation receiver which has been proposed in Xu et al. (2014) and then with the receiver based on the logarithmic estimator which has been proposed in Xu et al. (2014).

The receiver proposed in Cek and Savaci (2009) which is based on SαS noise based SPSK technique estimates the characteristic exponent ‘α’ of the received sequence and a hard limiter declares the transmitted binary information bit as ‘0’ or ‘1’. The BER performance of the receiver based on SINC estimator has not been computed in Cek and Savaci (2009) but certain limitations have been pointed out in Xu et al. (2014). Firstly, due to the utilization of two SαS noise sequence generators in the transmitter side, the complexity of the adopted approach in Cek and Savaci (2009) to propose the first SαS noise based communication system has been increased. Secondly, increasing the difference between α_0 and α_1 increases the risk of being detected by an eavesdropper, hence results in worse security while achieving efficient BER rate. In contrast, decreasing the difference between α_0 and α_1 increases the risk of being undetected by an intended receiver, hence results in worst BER rate while improving the security. Thirdly, the transmission rate is low as large numbers of samples, i.e. greater bit duration, are required to accurately estimate the modulated characteristic exponent ‘α’. The shortcoming of receiver based on SINC estimator SαS noise based communication systems prompted the authors in Xu et al. (2014) to propose correlation based receiver which has shown efficient BER performance in Xu et al. (2014) as

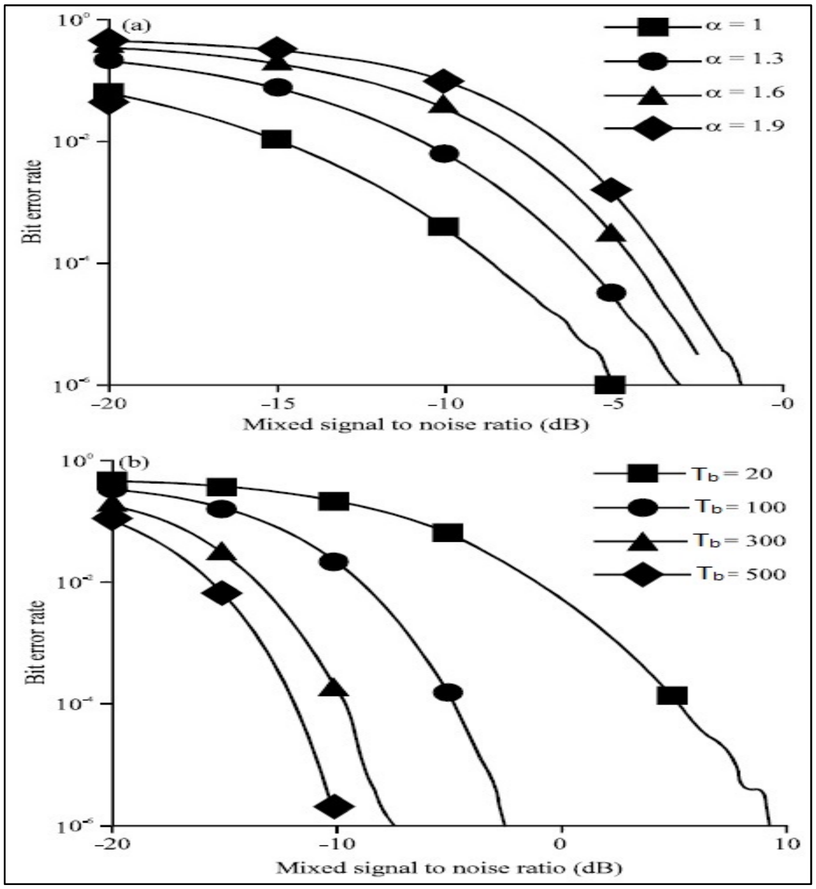


Figure 3.3. BER vs. MSNR$_{db}$ for different a) characteristic exponents 'α' and b) bit duration 'T$_b$' (Source: Xu et al. 2014)

The performance of the correlation based receiver has been shown in Figure 3.3 where different values of 'α' and 'T$_b$' are utilized to broaden the universality of the result. In Figure 3.3a, The BERs of the correlation based receiver in Xu et al. (2014) has been evaluated for various values of 'α' which shows that fixed $T_b = 100$ BER gradually decreases with the increase in the values of α and vice versa. Similarly in Figure 3.3b, with fixed α, the BER reduced with the increment in number of noise samples representing single binary information bit.

Another receiver proposed in Xu et al. (2016) for enhancing the performance of SαS noise based communication system has also been compared with the receiver based on SINC estimator. The corresponding BERs have also been evaluated against GSNR_{dB} in Xu et al. (2016) as given in Figure 3.4.

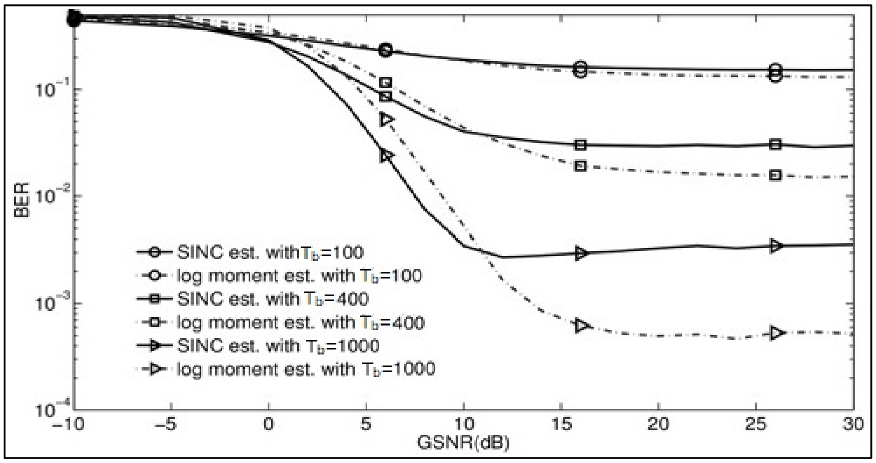


Figure 3.4. BER performance in AWGN channels with α_0= 1.0, α_1 = 1.5 and N = 100, 400, 1000, respectively BER vs. GSNR$_{db}$ for different bit duration 'T_b' (Source: Xu et al. 2016)

In Figure 3.4, the BER performance of the receiver based on logarithmic estimator has been compared with receiver based on SINC estimator in AWGN channel has been examined which has been characterized by GSNR$_{db}$ and bit duration T_b of the transmitted SαS noise realizations. The receiver based on logarithmic estimator has outperformed the receiver based on SINC estimator at every point. It can be seen that BERs decrease rapidly with the increment in T_b which is similar to previous comparison. At low GSNR$_{db}$, both receivers have increased BERs while at GSNR$_{db}$ < 0 the BER reaches to a level, i.e. BER = 0.5, in which communication is not possible. Furthermore, the BER starts to degrade at high GSNR$_{db}$, i.e. GSNR$_{db}$ > 5 dB.

3.3. M-Ary alpha-stable noise modulation

Due to the progress of SαS and SkαS noise based communication systems to implement binary SPSK and successful BER analysis of the proposed designs, the α-stable noise modulation capable to transmit M-ary binary information was also proposed in Cek (2015b) which was named as 'M-ary symmetric α-stable differential shift keying (M-ary SαS-DSK)'. The proposed M-ary SαS-DSK has also reflected efficient BER performance in comparison to its previous counterparts, i.e. 2-ary SαS and SkαS noise carrier based communication systems.

The M-ary SαS-DSK transmits SαS distributed noise signal generated within interval $\left[0, \frac{T_b}{2^K}\right]$. The imposed sequential delay operation modifies the transmitted impulsive noise signal in accordance to the depending on the transmitted bit block which is then multiplied with ‘-1’ or ‘1’ in accordance with the corresponding binary information bit holding the hidden information content for an intended receiver.

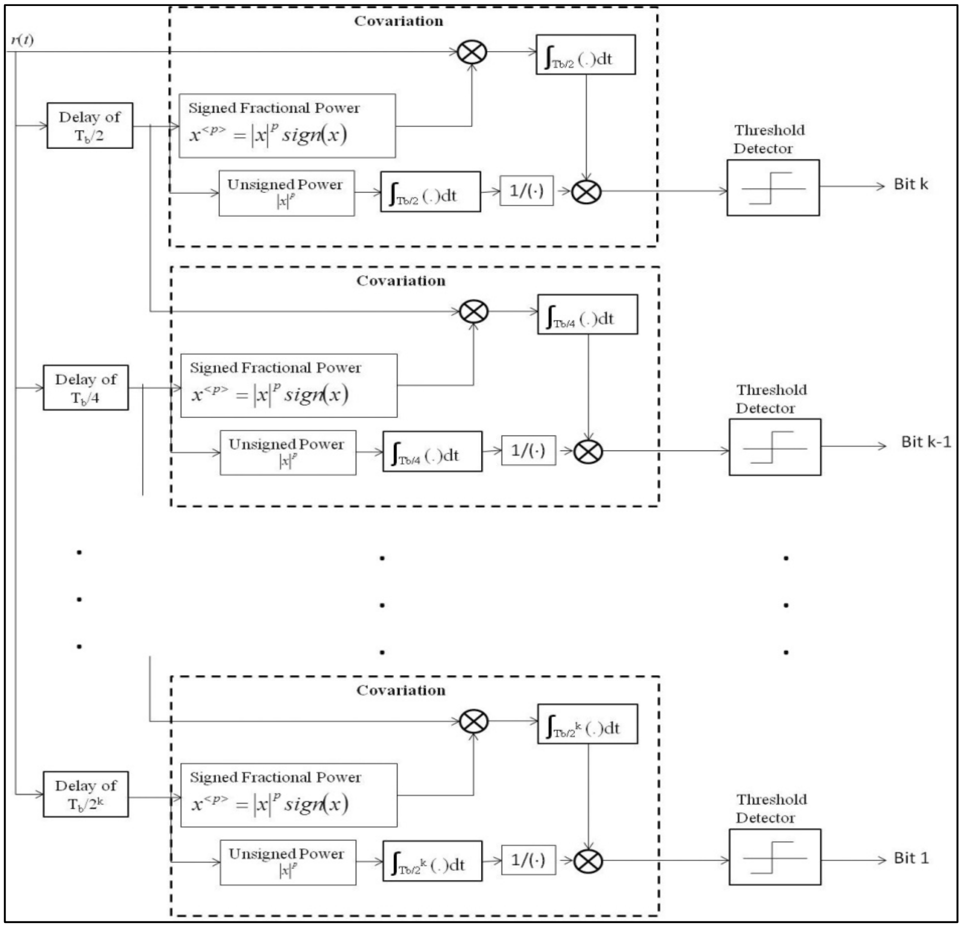


Figure 3.5. Proposed receiver of M-ary SαS-DSK (Source: Cek 2015b)

The receiver shown in Figure 3.5 has an identical structure of the transmitter but in the reverse order, hence, the first recovered message at the intended receiver side is the last coded message bit at the transmitter side. The receiver performs by sequentially separating the received signal in to two parts where the co-variation is computed among the first and second half of the signal. The binary information bit is estimated by monitoring the sign of co-variation. The transmitted *k*-bit block of data can be obtained by repeating the above procedure *k* times.

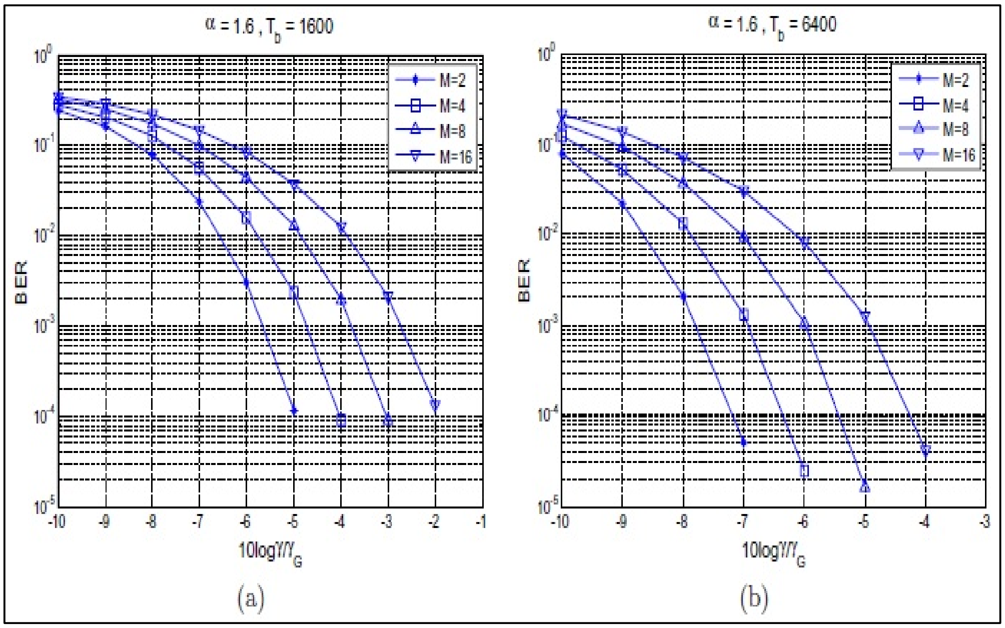


Figure 3.6. BER performances of the M-ary SαS-DSK w.r.t. different T_b,
(a) T_b = 1600, (b) T_b = 6400 (Source: Cek 2015b)

The BER performance of M-ary SαS-DSK as shown in Figure 3.6 demonstrates that the proposed M-ary SαS noise based SPSK techniques is capable to achieve efficient BER rate while keeping the sample size 'T_b' and characteristic exponent as 'α' as small as possible.

3.4. Prospective Research Pathways

Since, SPSK or stochastic noise based communications is a new field in comparison to conventional spread spectrum communications or unconventional chaotic communications, there are many prospective research pathways and ongoing issues which have immense potential for research. Due to the discussed benefits of α-stable noise as a random carrier in implementing SPSK techniques, significant interest have been seen in SαS and SkαS noise based stochastic communication systems in the last decade. Therefore, α-stable noise is now considered as the most convenient carrier to carry out stochastic communications; hence, immediate attention is required in this area. For that reason, many potential research pathways and ongoing issues have been discussed in this section where most of them have been addressed in the later chapters of this thesis.

Among the most issues, the one which was mostly being addressed in the last decade is to develop better receivers which can provide best possible BER performances so that practicality of stochastic communication systems can be increased. Therefore, optimized models of SαS and SkαS noise based SCSs are required.

Apart from analyzing SαS and SkαS noise based SCSs solely on the basis of BER performances, some common criterion is needed to measure the covertness of various SαS and SkαS noise based SCSs. Moreover, any clear cut criterion which is capable of quantifying the covertness of SαS and SkαS noise based SCSs would be a great contribution to this area. Similarly, all the investigations related to SαS and SkαS noise based SCSs have assumed perfect synchronization in the past where no exact method have been presented yet to synchronize SCSs. Therefore, any synchronization criterion, if introduced, can significantly boost the amount of research conducted in this field.

Unlike wise in chaotic communications, there are no attacks, algorithms and methods available to judge and predict the level of security derived from any proposed design of SαS and SkαS noise based SCS. Therefore, some attack is required which can be used to analyze various SαS and SkαS noise based SCSs from the perspective of an eavesdropper. Moreover, counter attack guidelines require an immediate attention.

The authors have addressed all these issue in the later chapters of the thesis where some of them have been left open for future research.

CHAPTER 4

OPTIMIZED MODEL OF ALPHA-STABLE NOISE BASED RANDOM COMMUNICATION SYSTEMS

The first aim of this chapter is to design optimized model of α-stable noise carrier based Random Communication System. As a second aim, the first synchronization method for RCS has been proposed by utilizing the classic concept of Pilot Assisted Synchronization (PAS).

4.1. Random Communication System through Maximum Extreme Value Method based Estimator

The proposed RCS is based on the skewed α-stable (α-stable) noise sequence which is chosen as the random carrier to modulate the binary message at the transmitter side. Antipodal characteristic of the skewness parameter beta (β) is exploited for decoding information at the receiver side to obtain a secure communication system. A fast estimator used in this thesis is based on Modified Extreme Value Method (MEVM) to extract the binary message from the signal received through the Additive White Gaussian Noise (AWGN) channel. Our proposed receiver is achieving better BER versus Mixed Signal to Noise ratio (MSNR) than previously introduced receivers which are based on Sinc and Logarithmic estimators. MEVM estimator is indeed less complex compared to the Sinc and Logarithmic estimators, hence, faster.

4.1.1. Introduction

A complete stochastic communication system based on SPSK was first introduced in Salberg & Hanssen (1999). In their system, two different ARMA processes were used to send binary messages. In Cek & Savaci (2009), the authors introduced SαS noise as a random carrier in their proposed random communication scheme and the characteristic exponent 'α' which is the impulsiveness measure of the data has been used for encoding the binary message. A sinc estimator introduced in Kuruoğlu (2001) was used in Cek & Savaci (2009) to estimate the binary message from the received signal. Later on, BER of the scheme introduced in Cek & Savaci (2009) was evaluated in Xu et al. (2014). However in Cek (2015), the random communication scheme was modified by using skewness parameter (β) of skewed α -stable noise as a random carrier and better performance was obtained. A new model of SαS communication system based on a logarithmic moment estimator was introduced recently in Xu et al. (2016). Both sinc estimator and logarithmic estimator used in Cek & Savaci (2009) and Xu et al. (2016) were first introduced in Kuruoğlu (2001). While sinc estimator is more simple and fast compared to the logarithmic estimator however the logarithmic estimator is more accurate in sense of BER and therefore the choice of estimator would depend on the type of communication data. However, the newly introduced receiver in this study uses MEVM given in Kuruoğlu (2001) to estimate the skewness parameter 'β' of the tail statistics of the received signal through AWGN channel. MEVM which estimates 'β' has been built on the Extreme Value Method (EVM) proposed in Tsihrintzis and Nikias (1996), where 'α' is estimated. In Kuruoğlu (2001), it is claimed that the EVM is the fastest among the proposed three estimators. But the tradeoff between computational complexity and better BER performance has to be done when choosing EVM for the decoding process where both computational complexity and BER efficiency depends on the sequence of length "K" and the number of segments "L" of the EVM estimator.

4.1.2. System Description

In this section, the need of having a fast estimator with least complexity and BER efficiency for random communication system using skewed α-stable distribution has been fulfilled with MEVM estimator. BER performance with respect to the parameters *(α,β,γ,μ)* of the skewed α-stable distribution has been simulated for the proposed random communication system. Perfect synchronization between the transmitter side and the receiver side is assumed in our proposed system. The proposed random communication system is shown in Figure 4.1.

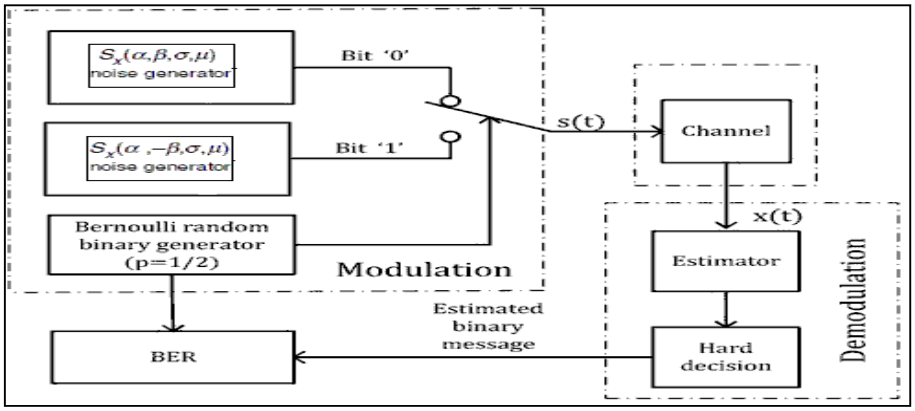


Figure 4.1. Block diagram of the Optimized RCS

4.1.2.1. Skewed Alpha-Stable Noise Shift Keying based Transmitter

The binary message sequence is taken from Bernoulli random variable that produces '1's and '0's with equal probability and considered as uncorrelated. However, the factor of correlation in bits to decode information is already exploited before in Xu et al. (2014) and and recently Xu at al. (2017). The binary message is encoded by skewness parameter 'β' of the α-stable Levy noise X which has distribution S_α (β, ɤ, μ) "i.e. X ~S_α (β, ɤ, μ)". X_0 ~S_α (β_0, ɤ, μ) is used to code message signal '0' and X_1~Sα (β_1, ɤ, μ) where $\beta_1 = - \beta_0$ is used to code message signal '1'.

The characteristic function of α-stable Levy noise X ~ S_α (β, ɤ, μ) having α-stable distribution is expressed in (2). Duration length of the samples x_0 & x_1 are denoted by T_b. N represents the number of noise samples per information bit and T_b is the duration for the consecutive noise samples and hence T_bN is the duration needed to encode single message bit. In Figure 4.2, the binary message sequence and the corresponding transmitted noise sequence with T_b = *1* and *N=1000* are shown. The noise sequence which has skewed α–stable Levy noise has been generated by the method given in Janicki and Weron (1994). Because of the infinite variance of skewed α–stable noise for $\alpha < 2$; few large amplitude samples can only be observable in the transmitted noise sequence in the bottom part of Figure 4.2 with the scale of 10^7.

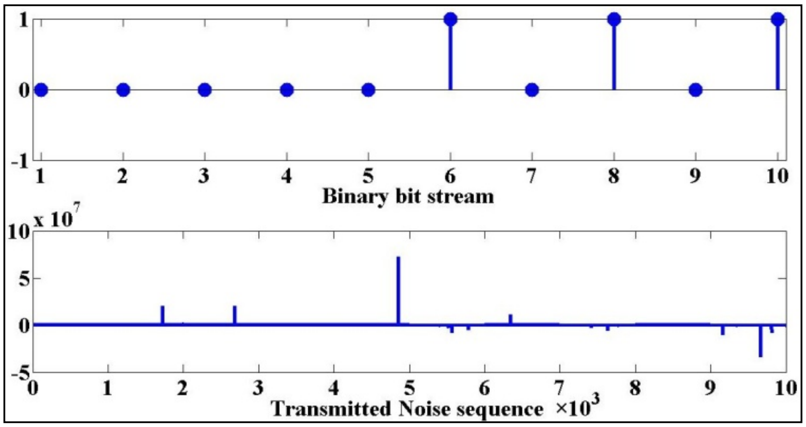


Figure 4.2. Binary Message sequence (Top), Transmitted Signal In time (Bottom); Bit length T_b=1, N = 1000 noise samples per information bit, T_bN=1× 10^3

4.1.3. Modified Maximum Extreme Value Method based receiver

The receiver is based on estimating the skewness parameter of the received signal from AWGN channel by MEVM Estimator given in Kuruoğlu (2001). The method proceeds by subdividing the received data $\{x_{1,}\ x_2,\ ....\ ,\ x_N\}$ in duration T_bN consisting of *N* samples into *L* non overlapping segments of length *K (i.e.* $K = N/L$*)*. The logarithms of the maximum and minimum samples from each segment *l* (where *l =1, 2, ... , L*) from total *L* segments are then computed and denoted by Y_{lmax} and Y_{lmin}.

$$Y_{lmax} \ = log\ \{max(x_{lK-K+i}|\ i \in 1,2, \dots, K)\} \qquad (33)$$

$$Y_{lmin} = log\,\{-min(x_{lK-K+i}|\, i \in 1,2,\dots,K)\} \qquad (34)$$

The sample means and corresponding variances of Y_{lmax} and Y_{lmin} and Estimates for β are then obtained as

$$Y_{max} = \frac{1}{L}\sum_{l=1}^{L} Y_{lmax} \;; \quad s_{max}^{2} = \frac{1}{L-1}\sum_{l=1}^{L}(Y_{lmax} - Y_{\max})^{2} \qquad (35)$$

$$Y_{min} = \frac{1}{L}\sum_{l=1}^{L} Y_{lmin} \;; \quad s_{min}^{2} = \frac{1}{L-1}\sum_{l=1}^{L}(Y_{lmin} - Y_{\min})^{2} \qquad (36)$$

$$\hat{\beta} = 1 - \frac{2}{\exp\,(\hat{\alpha}(S_{max} - S_{\min}))} \quad \text{where} \quad \hat{\alpha} = \frac{\pi}{2\sqrt{6}}\left(\frac{1}{Y_{max}} + \frac{1}{Y_{min}}\right) \qquad (37)$$

and the binary message is estimated using hard decision.

Bias in MEVM estimator:

MEVM estimator '$\hat{\beta}$' is not an unbiased estimator of β as mentioned in Kuruoğlu (2001) and Tsihrintzis and Nikias (1996). The bias of the MEVM estimator $\widehat{\beta}$ increases as alpha approaches to two (Gaussian case). Otherwise, it is capable of giving estimates close to maximum likelihood (ML) estimates as mentioned in Kuruoğlu (2001) and Tsihrintzis et al. (1996). Additionally, the bias of the MEVM estimator *'$\hat{\beta}$'* can be kept under control if large data sets (N) and number of segments (L) are used as proven in Table II in Tsihrintzis et al. (1996). And it can be seen in our results, that due to the utilization of large 'L and N', our proposed approach is giving good performance in the sense of BER.

Complexity and fastness of MEVM estimator:

In Xu at al. (2016), it was explained that the logarithmic estimator is faster compared to the SINC estimator. The sinc estimator is much complex because it requires the calculation of absolute and signed fractional moments and inversion of sinc function each time for decoding a single binary bit.

However, the logarithmic estimator also requires equating sample moments and the actual moments and then we may solve for the characteristic exponent and skewness parameter using the third-order moment for decoding a single binary bit which is considered as a drawback Kuruoğlu (2001).

Whereas, the simplicity of the MEVM estimator can be seen in (33-37) which requires the calculation of simple mean and variances of the observed data each time. It decreases the amount of computation and lessons the overall complexity of the receiver.

Hence, it is claimed as fast estimation approach than sinc and logarithmic estimators by Kuruoğlu (2001).

The received noise sequence through AWGN channel and the estimated beta parameters together with the corresponding estimated binary message have been shown in Figure 4.3.

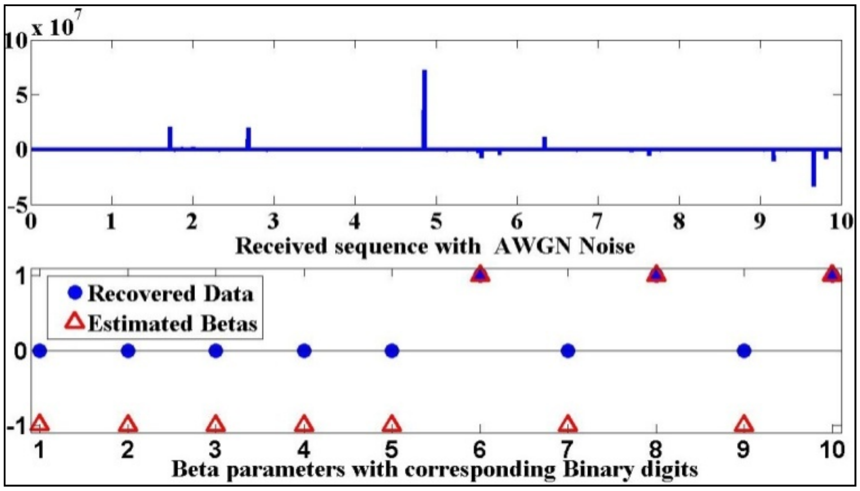


Figure 4.3. Received Signal from AWGN Channel in time Domain (Top), Estimated Beta parameters and recovered binary message (Bottom); Bit length T_b=1, N = 1000 noise samples per information bit, $T_bN=1\times 10^3$.

4.1.3. Performance Evaluation and Comparison

The length and number of segments termed as 'K and L' are very crucial factors and they determine the computational complexity level of our newly proposed receiver. MEVM has never been used before in the receiver to optimize BER performance and to maximize or minimize the computational complexity of the receiver in random communication systems. The minimum number of segments and the length of segments L_{min} and K_{min} , respectively are at least equal to two and the maximum number of segments and length of segments $\mathrm{L_{max}}$ and $\mathrm{K_{max}}$ are at most equal to $\frac{\mathrm{N}}{2}$ (i.e. $\mathrm{L_{min}} = \mathrm{K_{min}} = 2$ and $\mathrm{L_{max}} = \mathrm{K_{max}} = \frac{\mathrm{N}}{2}$).

In Figure 4.4, BER vs. MSNR performance of our proposed receiver has been shown where MSNR or Dispersion Ratio (DR) are defined as in Liu et al. (2009) while BER is the percentage of bits with errors divided by the total number of bits that have been transmitted.

$$\mathrm{MSNR}_{dB} = 10\log\frac{\gamma}{\gamma_G} \tag{38}$$

where γ and γ_G are the dispersion parameters of the information bearing α-stable random signal and the channel noise, respectively. It can be clearly seen that our newly proposed receiver is outperforming the receivers based on covariance method (COV) and Fractional lower-order covariance method (FLOC) proposed in Xu et al. (2014) and Cek (2015), respectively. Additionally, it is giving better BER for various values of 'K' of MEVM estimator hence resulting in various choices of complexity level. Also better BER can be obtained for $\alpha < 1.6$.

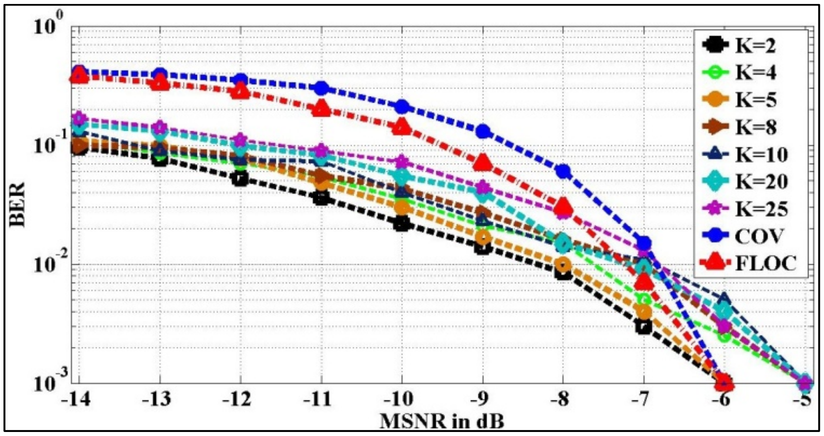


Figure 4.4. BER vs. MSNR (dB) with different 'L and K' of estimator in AWGN channel; transmitted bits=1000; where α = 1.6; (Where β_1 = - β_0= 1).

4.2. Synchronized Random Communication Systems

The Pilot Assisted Synchronization (PAS) method for RCSs has been proposed in this section. The pilot symbol which has α-stable distribution has been used to establish synchronization and to maintain covertness in RCSs. The introduced Synchronization Block (SB) consists of Fractional Lower order Covariance based Correlators (FLOCCs), Threshold Detectors (TDs) and the Synchronization Control Block (SCB). In order to measure the performance of the proposed SB, the performance criterion, i.e. Confidence Ratio (*CR*), has been proposed. The Reliability of the proposed SB can be enhanced by altering the Confidence Ratio (*CR*) and the Achieved Confidence Ratio (*ACR*) by using the FLOCCs and TDs in SB.

4.2.1. Motivation and Background

From the first stochastic process shift keying based RCS introduced in Salberg et al. (1999) to the recently introduced optimized model of RCS in Areeb and Savaci (2017), all RCSs studies mentioned above assume perfect synchronization. However, the method to achieve synchronization in RCSs has not been introduced. In order to fulfill the gap of synchronization issue in RCSs and to keep the synchronization error below the available synchronization error margin given in Ahmed and Savaci (2017b), in this section we have newly developed the concept of PAS for RCSs by FLOC method.

Since α-stable distributions do not have second and higher order statistics; FLOC method was introduced in Ma and Nikias (1996) to correlate α-stable noise signals. Hence, FLOC based receiver for α-stable noise based communication system was also introduced in Cek 2015. Similarly, an approach based on lag-frequency map, i.e. FLOC, enhanced FLOC, i.e. FLOC-LM, and its integrated versions have been utilised to detect faults in α-stable noise based mechanical system in Żak et al. (2017). Addtionally, a brief comparison of FLOC and Cauchy score functions based MUSIC algorithms in α-stable noise environments has been done in in Żhang et al. (2017). However, due to idea to utilize FLOC to synchronize RCSs, further concerns related to the performance of FLOC for complete range of parameters related to the α-stable noise, needs to be investigated; so that precise and accurate synchronization can be established in RCSs. Therefore, structure and performance of FLOC method in α-stable noise environments has been evaluated first.

4.2.2. Structure and Performance Evaluation of Fractional Lower-Order Covariance method in α-Stable noise environments

In order to address the above issues, in this sub-section, we have analyzed the effects of skewness and impulsiveness parameters of α-stable distributed noise on the FLOC method. The auto-correlation, i.e. auto-FLOC, of alpha stable noise signals with and without AWGN noise has been done to monitor the robustness of FLOC method. Different ranges of the parameters related to the α-stable distributed noise which resulted in maximum auto-FLOC values, have also been discovered. Additionally, a trend in auto-FLOC values has been observed which is dependent on the skewness and impulsiveness parameters of α-stable distributed noise. The results would help to optimize all types of communication systems which are based on α-stable noise and FLOC method.

4.2.2.1. Fractional Lower-Order Covariance method

If a given pair of *N* observation of α-stable distributed noise X ~ S_α *(β, γ, μ)* is expressed as $\{x[1], \dots, x[n]; n = 1,2, \dots, N\}$ then the auto-FLOC of X ~ $S_{1\leq\alpha\leq2}$ *(β, γ, μ)*, denoted by $R_d[k]$, is estimated in Ma and Nikias (1991) as

$$R_d[k] = \frac{\sum_{n= N_1+1}^{N_2} |x[n]|^a \,.\, |x[n+k]|^b . sign(x[n] \,.\, x[n+k])}{N_2 - N_1} \tag{39}$$

where $k = (\frac{-N}{2}, \frac{N}{2})$, N_1 = max (0, - k) , N_2 = min *(N* - k , N *)* and the fractional powers are $a = b = \frac{\alpha}{2}$ and $sign(x)$ is given (3).

Similarly, the signed FLOC for X ~ $S_{\alpha<1}$ *(β, γ, μ)*, denoted by '$R_d[k]$', is estimated in Ma and Nikias (1991) as

$$R_d[k] = \frac{\sum_{n=N_1+1}^{N_2} sign(\, x[n]\, .\, x[n+k])}{N_2 - N_1} \tag{40}$$

where the fractional powers 'a' and 'b' are taken as $a = b = 0$. Auto-correlation, i.e. auto-FLOC of non delayed alpha stable distributed noise signals can be obtained as $R_d[0]$ by (39, 40).

Remark: FLOC is applicable to both Gaussian and impulsive noise environments which makes it a robust and efficient delay estimation method, i.e. α can fluctuate between its defined range of (0, 2] as proved in Ma and Nikias (1991).

4.2.2.2. Performance Evaluation

The effects of impulsiveness and skewness parameters of α-stable distributed noise signal on FLOC method has been analyzed in Figures 4.5-4.8. Firstly, the FLOC of α-stable noise signal alone, i.e. X, with its non-delayed and delayed versions has been computed in Figures 4.5, 4.6.

Secondly, the FLOC of α-stable noise signal with AWGN noise, i.e. X+G, with its non-delayed and delayed versions has been computed in Fig 4.7, 4.8. It has been observed that auto-FLOC of 'X' and 'X+G', i.e. $R_d[k]$, increases or decreases in a specific trend when characteristic exponent α $(0 < \alpha \leq 2)$ and the skewness parameter β $(-1 \leq \beta \leq 1)$ of X fluctuates in some specific ranges. The used parameter values have been listed in the following section A.

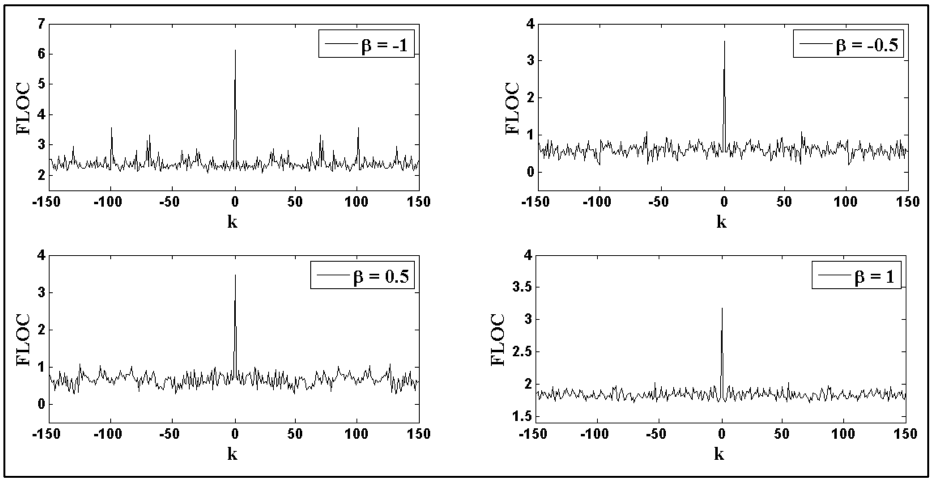


Figure 4.5. Performance of FLOC method for α-stable noise 'X' with α=0.5, γ = 1.0 and μ = 0

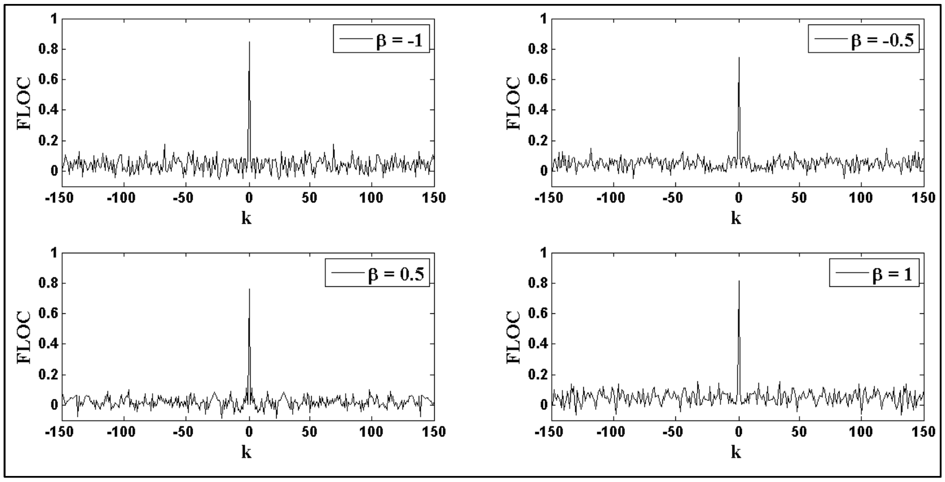


Figure 4.6. Performance of FLOC method for α-stable noise 'X' with α=1.5, γ = 1.0 and μ = 0

The discussion on the results and the observed trend of auto-FLOC, i.e. $R_d[0]$, of non-delayed signals 'X+G' has been summarized in Section B. The obtained results or the observed trend of α-stable noise signals in Table 4.1 are concluded by performing 10,000 Monte Carlo simulations or realizations. The resultant FLOC values on y-axis, i.e. R_d[k] shown in Figures 4.5-4.8, are actually the mean or average values of R_d[k].

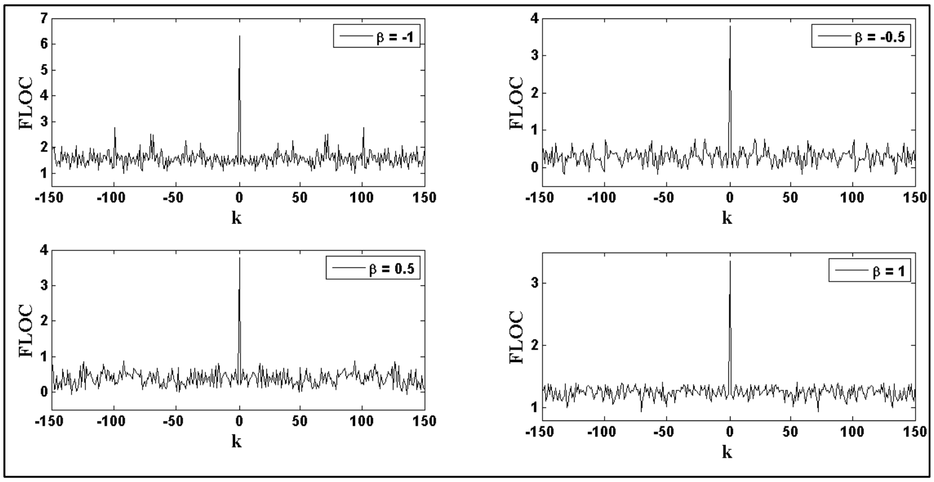


Figure 4.7. Performance of FLOC method for α-stable noise ‘X+G’ with α=0.5, μ = 0, MSNR = -4 dB

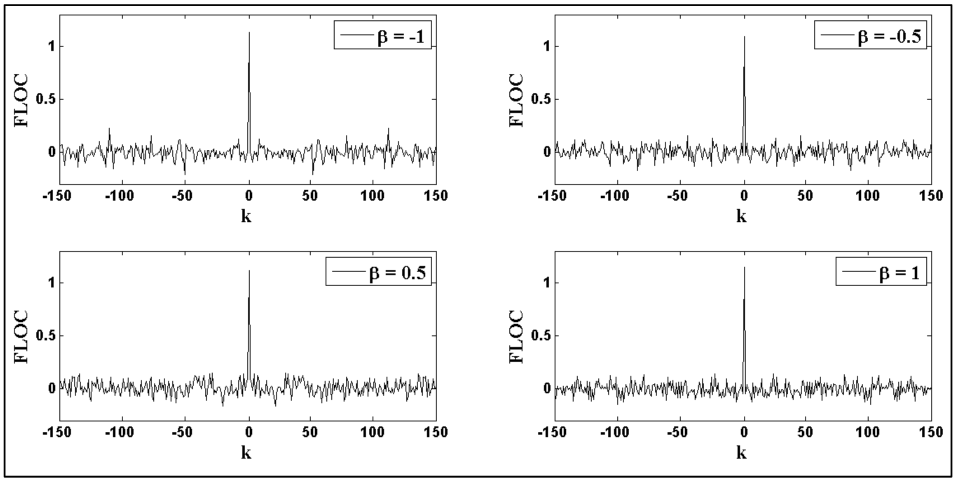


Figure 4.8. Performance of FLOC method for α-stable noise ‘X+G’ with α=1.5, μ = 0, MSNR = -4 dB

In order to define the amount of Gaussian noise, i.e. G~ $S_{\alpha=2}$ ($\beta=0, \gamma, \mu$), mixed with the α-stable noise signal, the generalized signal to noise ratio should be defined to measure the severity of the α-stable noise signal contaminated by Gaussian noise. Therefore, the MSNR or DR has been used. The mixture containing α-stable noise samples along with Gaussian noise samples is highly influenced or becomes more contaminated by Gaussian noise samples as we decrease the MSNR, i.e. by decreasing the dispersion parameter of α-stable noise signals or by increasing dispersion parameter of Gaussian noise, and vice versa.

Simulation Parameters:

The simulations shown in Figures 4.5 – 4.8 have been made for $N=300,$ location parameter μ = 0 and $MSNR$ = -4dB. The correlation of α-stable noise signal has been done by its delayed versions in a range k $(-150 < k \leq 150)$. The Figures 4.5, 4.6 and Figures 4.7, 4.8 shows the results for the correlation conducted by the FLOC method with and without AWGN noise, respectively. The simulations have been shown for various values of characteristic exponent α $(0 < \alpha \leq 2)$ and the skewness parameter β $(-1 \leq \beta \leq 1)$; where results for each individual value is shown and listed in Figures 4.5 – 4.8.

Experimental Results:

The FLOC of X and X+G increases with the decrement in α which means higher values of FLOC are observed as the α-stable noise X becomes more impulsive in nature which can be understood by comparing specifically the value $R_d[0]$ of Figure 4.5 with Figure 4.6 and of Figure 4.7 with Figure 4.8. Additionally, at lower values of α of α-stable noise X, higher FLOC is observed as β approaches its lowest value of β = -1.

Table 4.1. Trend of FLOC method in α-stable noise**.** ↑, ≈ and → are used to indicate ‘increasing’, ‘almost same’ and ‘approaching’ respectively

Impulsiveness ‘α’	**Skewness ‘β’**	**Trend of Auto-FLOC of non-delayed signals at ‘$R_d[0]$’**
α= 0.5	β_+ → 1	≈
	β_- → -1	↑
α= 1.5	β_+ → 1	≈
	β_- → -1	≈

As shown in Figures 4.5, 4.7, the auto-FLOC of X and X+G, for α=0.5, increases a bit or remains almost same as β_+ approaches its extreme value of β_+= 1, however, it increases abruptly as β_- approaches its extreme value of β_-= -1. On contrary in Figures 4.6, 4.8, the auto-FLOC of X and X+G, for α=1.5, remains almost same as both β_+ and β_- approaches their extreme values of β_+= 1 and β_-= -1, respectively. This trend is also summarized in Table 4.1. Additionally, maneuvering the MSNR would scale or normalized the absolute value of y-axis, i.e. FLOC values, for same α and β. However, the trend of FLOC on α-stable distributed noise signals would remain the same which has been shown in this section.

4.2.3. Overview of Pilot Assisted Synchronization

Synchronization is a vital step in designing any wire-line or wireless communication system. Especially, in wireless communication systems, synchronization is very important due to the presence of much intense channel impairments, e.g. noise, fading, interference, distortion and attenuation. The Pilot Assisted Transmission (PAT) is a method in which a transmitter and receiver communicate through known information bearing signals, i.e. Pilot Symbols (PSs), to overcome the channel impairments by exploiting channel estimation, receiver adaptation, and optimal decoding. The concept of PAS through PAT was firstly introduced in Cavers (1995) as Pilot Symbol Assisted Modulation (PSAM). Some of the other approaches on PAT were focused on fast varying channels Tong et al. (2004). Currently, PAT is an essential element in modern wireless communication systems, for instance, the GSM system uses 26 bits PSs and the TDMA standard includes PSs at the beginning of each packet Tong et al. (2004). WCDMA and CDMA-2000 are third generation wireless communication systems which send PSs with information signals simultaneously. Fourth generation broadband systems like HyperLAN II and IEEE 802.11 family also use PSs for communication Tong et al. (2004).

Also in the conventional Spread Spectrum (SS) communication systems, synchronization is achieved between transmitter and receiver through PSs known as Pseudo-Noise (PN) codes Polydoros and Weber (1984), Polydoros and Weber (1984b) and Peterson et al. (1995). The method to synchronize chaotic communication systems by PN sequences for the PAS was proposed in Jovic et al. (2007). The advantage of using PN sequences as PSs is good correlation but it lacks security Burel and Bouder

(2000). Therefore, in order to improve the security of the chaotic communication systems the PAS approach using Gold sequences, i.e. shifted PN sequences, as PSs were introduced Kaddoum et al. (2009). However, the PAS method based on a chaotic pilot in Vali et al. (2010) has improved the security by achieving complete masking.

Similarly, in Molecular Communication (MC), i.e. a biologically-inspired form of communication, where chemical signals are used to transfer information, synchronization is also vital to build diffusion-based MC systems Farsad et al. (2016). Most studies on MC systems have assumed perfect synchronization while recent researches focused on synchronization of MC systems. The studies in Zhou et al. (2005), Abadal and Akyildiz (2011), Abadal and Akyildiz (2011b), Moore and Nakano (2012) and Moore and Nakano (2013) have presented to achieve the PAS by using specific molecule types as PSs. In Zhou et al. (2005), two genes, i.e. *luxI* and *luxR*, are used as PSs in Synthetic Gene Regulatory Network (SGN). Similarly in Abadal and Akyildiz (2011) and Abadal and Akyildiz (2011b), the method of Biological bacterial Quorum sensing have been introduced in which the bacteria of different species are used as PSs for synchronization between the nodes of a nanonetwork. Additionally, in Moore and Nakano (2012) and Moore and Nakano (2013), the PAS method for molecular machine, i.e. a device with a size in the nano to micro-scale range, has been introduced where the pulses of inhibitory molecules, i.e. negative auto regulating molecules, are used as PSs. So, the PAS has been used in manmade communication systems as well as in the communication systems of nature.

4.2.4. System Description

In order to fulfill the gap of synchronization issue in RCSs and to keep the synchronization error below the available synchronization error margin given in Ahmed and Savaci (2017b), in this section we have newly developed the concept of PAS for RCSs. The proposed idea is inspired by the application of PAT and PAS in both manmade and natural communication systems discussed above. The proposed PAS method is based on the utilization of α-stable noise as the pilot sequence sampled from α-stable distribution. This pilot sequence is different from the random carriers which have been obtained from the α-stable distributions in the transmitter. The utilization of α-stable noise as the pilot sequence ensures secrecy during synchronization interval which is the main objective of RCSs. Since, the second-order and higher order moments of α-stable random variable do not exist, all existing time delay estimation methods, i.e. correlation and covariance, which are based on second-order statistics cannot be applied for the synchronization of RCS. Therefore, FLOCC has been used as the new measure of similarity between two α-stable distributions Ma and Nikias (1996). Hence, the SB consisting of FLOCCs and multiple TDs have been proposed for the receiver side to predict the exact accepting time of the data. Also, the criterion known as *CR* to measure the reliability of the proposed SB has also been proposed.

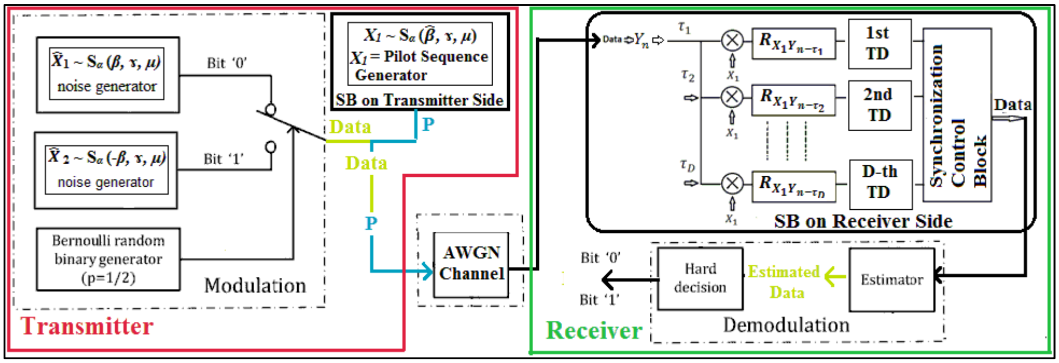


Figure 4.9. Block diagram of the RCS based on α-stable Levy noise along with the proposed Synchronization Blocks on Transmitter and Receiver side.

For synchronization, firstly, the pilot sequence pre known both by the transmitter and the intended receiver is produced in the 'SB on the transmitter side'. Then, the cut off threshold value based on the FLOC of the PSs is predetermined; which is also pre known both by the transmitter and the intended receiver. The number of FLOCCs and the number of TDs in the 'SB on the receiver side' is also pre decided both by the transmitter and the intended receiver. In proceeding subsections, the proposed synchronization method based on the pilot sequence which are also obtained from α-stable distributions are presented. Later on, the simulations have proved the achievement of the proposed SB.

4.2.4.1. Transmitter Block

The proposed SB which has been embedded in RCS has been shown in Figure 4.9. The pilot symbol X_1 in SB is also obtained from another α-stable distribution, i.e. $X_1 \sim S_\alpha(\hat{\beta}, \gamma, \mu)$, where $\hat{\beta} \neq \beta$.

Construction of the Pilot Symbol and Pilot Sequence:

Pilot symbol X_1 which is sent *'m'* consecutive times to construct the pilot sequence P_1 is described as

$$P_1 = [X_1, X_1, \ldots \ldots, X_1]_{1 \times mN} \quad (41)$$

where $$X_1 = [x_1 \; x_2 \ldots \ldots \ldots \; x_N]_{1 \times N} \quad (42)$$

and '*N'* represents the number of α-stable noise samples per pilot symbol. Every *n-th* pilot symbol 'X_n' is constructed from the elements of X_1 defined below as

$$X_n = [x_n \; \ldots \ldots \ldots \; x_{N-1+n}]_{1 \times N} \quad (43)$$

for $n = 1, 2 \ldots \ldots \ldots \ldots (m-1)N + 1$

and $$x_n = x_{uN+n} \quad (44)$$

for $u = 0, 1, 2 \ldots . m\text{-}1$

Hence *n-th* pilot sequence P_n is defined as

$$P_n = [X_n \, , X_n \ldots \ldots \ldots X_n \,]_{1 \times mN} \quad (45)$$

Fractional Lower Order Covariance for the Pilot Symbols:

The FLOC vector *'R'* consists of the FLOCs $R_{X_1 X_k}$ of the pilot symbol X_1 with the pilot symbols X_k which has been obtained as

$$R = [R_{X_1X_2} \;\; R_{X_1X_3} \dots\dots \; R_{X_1X_k} \dots\dots\dots\dots \; R_{X_1X_{N+1}}]_{1\times N} \tag{46}$$

where the FLOC $R_{X_1X_k}$ is estimated as in Ma and Nikias (1996)

$$R_{X_1X_k} = \frac{\sum_{n=N_1+1}^{N_2} |x_1[n]|^a .|x_k[n]|^b . sign(x_1[n].x_k[n])}{N_2 - N_1} \tag{47}$$

for $k = 2 \dots\dots\dots\dots N+1$

where $N_1 = 0$, $N_2 = N$ and the fractional powers are $a = b = \frac{\alpha}{2}$. Note that FLOCs between the *n-th* pilot symbol X_n and the *j-th* pilot symbol X_j satisfies the following relation

$$R_{X_nX_j} = R_{X_nX_{(uN+j)}} \tag{48}$$

for $u = 0, 1, \dots\dots m-1$ and $j = n+\ 1, \dots\dots N+n$.

If we assume that the additive channel noise is Gaussian then the noisy pilot symbols $X_n^{'}$ are assumed as

$$X_n^{'} = X_n + G \qquad \text{and} \qquad G \sim S_{\alpha=2}(\beta, \gamma, \mu) \tag{49}$$

and '*N'* represents the number of α-stable noise samples per pilot symbol. Every *n-th* pilot symbol 'X_n' is constructed from the elements of X_1 and then the new FLOC vector 'R_G' can be constructed as

$$R_G = [R_{X_1^{'}X_2^{'}} \;\; R_{X_1^{'}X_3^{'}} \dots\dots \; R_{X_1^{'}X_k^{'}} \dots\dots\dots\dots \; R_{X_1^{'}X_{N+1}^{'}}]_{1\times N} \tag{50}$$

Remark: FLOC is a robust time delay estimation method that performs well not only for the Gaussian noise environments but also in the presence of impulsive noise, i.e. α can be of any value within its admissible range (0, 2], which has been proved in Ma and Nikias (1996).

Cut-off Threshold (L_{th}):

The cut-off threshold has been pre-determined as

$$L_{th} = \frac{||R\,||_\infty + ||\,R_{\,red}\,||_\infty}{2} \tag{51}$$

where $||R\,||_\infty = \; max_{1\le i\le N}\;|r_i| = |r_L|$ and $R_{\,red}$ is the reduced vector obtained by deleting r_L from R.

This L_{th} is pre known both by the transmitter and the intended receiver which is used for hard decision in the threshold detection process.

The idea of choosing L_{th} as in (51) is that $||R\,||_\infty$ gives the highest FLOC value for $R_{X_1X_k}$ which is required as a threshold to the receiver for identification of the pilot symbol X_1. However, $||R_{\,red}\,||_\infty$ give the highest FLOC value for $R_{X_1X_k}$ which is required as a threshold to the receiver for identification of all other pilot symbols, except X_1. Hence, the computed mid value, i.e. L_{th}, between $||R\,||_\infty$ and $||R_{\,red}||_\infty$ is found to be the best criterion for accurate detection of X_1 on the receiver side.

\

4.2.4.2 Receiver Block

The SB on the receiver side, shown in Figure 4.9, consists of total *'D'* FLOCCs, TDs and the SCB for the pilot sequence tracking and acquisition. The choice of *'D'* is arbitrary which has been used to measure the reliability of the SB from newly introduced criterion known as '*CR*', explained in the following section.

FLOCCs and TDs:

The SB receives the pilot sequence *'Y_n'* as

$$Y_n \;\; = P_n \;\; + N_{channel} \tag{52}$$

Since, it is transmitted through AWGN channel and $N_{channel}$ is the actual channel noise added to the transmitted pilot sequence P_n which is defined below as

$$N_{channel} \sim S_{\,2}\,(0,\; \gamma_{Nchannel}=1,\; 0) \tag{53}$$

Note that in Y_n, the noisy sample data is different than X_n' because $N_{\,channel}$ is not known a priori while G in the transmitter side has been predicted as a channel noise a priori.

The *d-th* FLOCC starts taking samples of Y_n after a delay of 'τ_d' seconds where *'τ_d'* is the respective delay for accepting the first sample for the *d-th* correlator.

$$\tau_d = \frac{(d-1)\times T_{sample}}{D} \qquad (1 \leq d \leq D) \tag{54}$$

and T_{sample} is the duration between two consecutive noise samples.

Over detection, i.e. detection of one sample multiple times by a single TD during T_{sample} duration, can be avoided by the proper selection of τ_d's with the following criterion

$$\tau_D \; < T_{sample} \tag{55}$$

Some initial samples might be missed by the SB because of the random delay arising from the channel impairments like fading, multipath propagation etc. Therefore, the first received signal to SB might not be Y_1 and every FLOCC starts correlating the *N* received samples with first pilot symbol "X_1" from the time instant of reception. The FLOC procedure will then be repeated every T_{sample} seconds to look up for the required threshold level, i.e.L_{th}. The first threshold will be achieved when the threshold value from FLOC $R_{X_1 Y_{N+1}}$ will be obtained. The threshold can be achieved on more than one Threshold detector which will help the SCB to register it as first Pilot symbol acquisition.

Synchronization Control Block (SCB):

We have arbitrary chosen the number of pilot symbols *'m'* and total number of FLOCCs *'D'* equal to three and number of α-stable noise samples *'N'* equals to five hundred. In the flow diagram of SB, only *m-1* pilot symbols are identified and for the chosen values of *'m', 'N'* and *'D'* only two pilot symbols, i.e. *m-1*, are identified as shown in Figure 4.10. It illustrates the steps from noisy pilot samples reception and predicting the time instant of accepting the data samples.

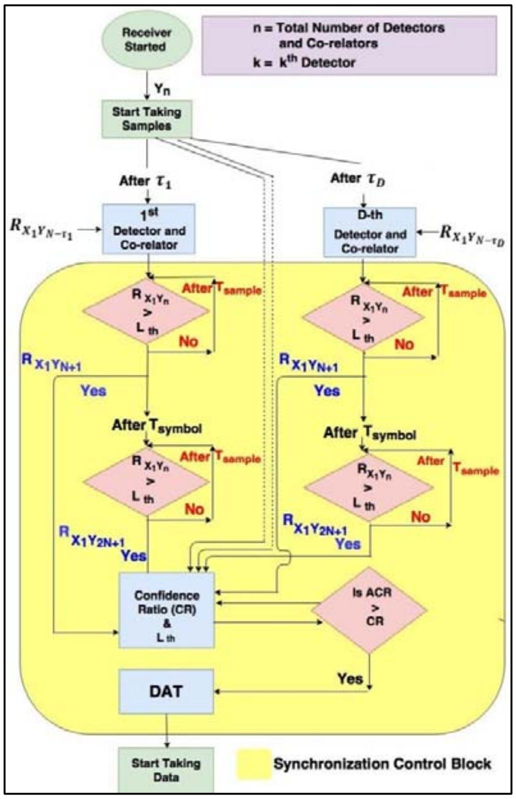


Figure 4.10. Flow diagram of the Synchronization Block on Receiver side

where the following definitions will further clarify Figure 4.10

Performance Measure of the Pilot Sequence:

In order to measure the performance of any pilot sequence, which is used to synchronize the RCSs, the following definitions are given below:

Required Confidence Ratio (RCR):

$$RCR \doteq \frac{D\,req}{D} \tag{56}$$

where 'D_{req}' is the required number of TDs that should achieve the required threshold, i.e. L_{th}, to claim pilot symbol acquisition and D_{req} is selected by the transmitter and the intended receiver.

Confidence Ratio (CR):

$$CR \doteq \frac{D_{ach}}{D} \tag{57}$$

where D_{ach} is the number of TDs that have achieved the required threshold, i.e. L_{th}.

Pilot Symbol Acquisition:

The first pilot symbol acquisition, i.e. S_{acq}^{1}, is obtained at the FLOC $R_{X_1 Y_{N+1}}$ with the condition $D_{ach} = D_{req}$.

Pilot Symbol Tracking Interval:

The *q-th* pilot symbol tracking interval, i.e. T_{tr}^{q}, continues until the time instant of *q-th* pilot symbol acquisition (i.e. S_{acq}^{q}) which is obtained at the FLOC $R_{X_1 Y_{qN+1}}$ with the condition $D_{ach} = D_{req}$.

The time instant for the *q-th* pilot symbol acquisition is defined below as

$$S_{acq}^{q} = \sum_{k=1}^{q} T_{tr}^{k} \tag{58}$$

for $q = 1, \dots \dots m - 1$

Data Acceptance Time (DAT):

The DAT tells the exact time instant, i.e. T_{data}, to start acceptance of the data after synchronization as

$$T_{data} = S_{acq}^{m-1} + T_{psy} \tag{59}$$

where T_{psy} is the duration of the pilot symbol.

Hence, the total duration required to establish synchronization, i.e. T_{sync}, in RCS by the proposed method can be found as

$$T_{sync} = T_{pro} + T_{data} \tag{60}$$

where 'T_{pro}' is the signal propagation time from transmitter to receiver.

Overlapping Margin ($\mathrm{OL_M}$):

The received PSs may be partially overlapped with each other. Assuming that, we have a specific percentage of overlapping between the noise samples of every pilot symbol denoted by 'OL_P' in the range $0 \leq OL_P \leq 1$ then every noise sample x_n of the pilot symbol X_n will be overlapped with x_{n-1} and x_{n+1} for the first and last "$\frac{\boldsymbol{OL_P}}{\mathbf{2}} \times T_{sample}$"

interval, respectively, as shown in Figure 4.11. The overlapping margin, i.e. OL_M, in the range $0 \leq OL_M \leq 1$, is the maximum percentage of overlapping, i.e. OL_P, which can be resisted by the proposed synchronization method for fixed '*D*' and 'τ_D' which is defined below as

$$OL_M < \frac{T_{sample} - \tau_D}{T_{sample}} \tag{61}$$

If OL_P is below OL_M for fixed '*D*', 'τ_D' and 'T_{sample} ' and τ_D is taken according to the criterion given in (55) then at least '*D-1'* FLOCCs and TDs will be able to detect the sample correctly from the non-overlapping region of every noise sample x_n of the pilot symbol X_n which is also shown in Figure 4.11. However, OL_M decreases with the increment in '*D*' and a tradeoff have to be maintained for this purpose. The utilized values of '*D* = 3' gives the leverage of overlapping margin up to 33%, i.e. $OL_M = 0.33$.

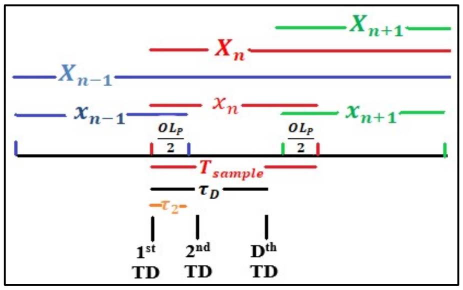


Figure 4.11. Overlapped sample $\mathbf{x_n}$ of the pilot symbol $\mathbf{X_n}$

To evaluate the overall performance of the proposed RCS, Bit Error rate (*BER*) vs. Mixed Signal to Noise Ratio (*MSNR*) performance has been analysed where *MSNR* or Dispersion Ratio (*DR*) is defined as in Ma and Nikias (1996) while *BER* is the percentage of bits with errors divided by the total number of bits that have been transmitted.

4.2.5. Simulation Results

.

The following simulations have been made for for *‘m=D=3’ and ’N=500’* as preselected parameters by the transmitter and the intended receiver.

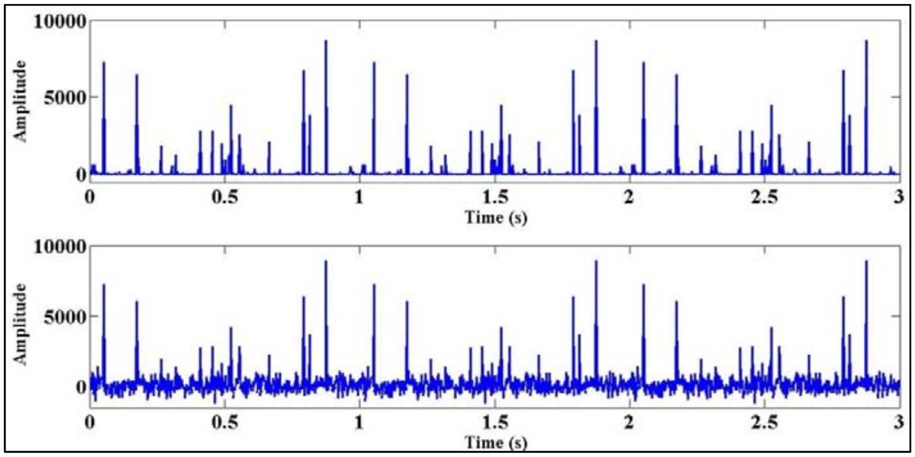


Figure 4.12. *a) Pilot Sequence* $\boldsymbol{P_1}$ *b) Noisy Pilot Sequence* $\boldsymbol{P_1'}$

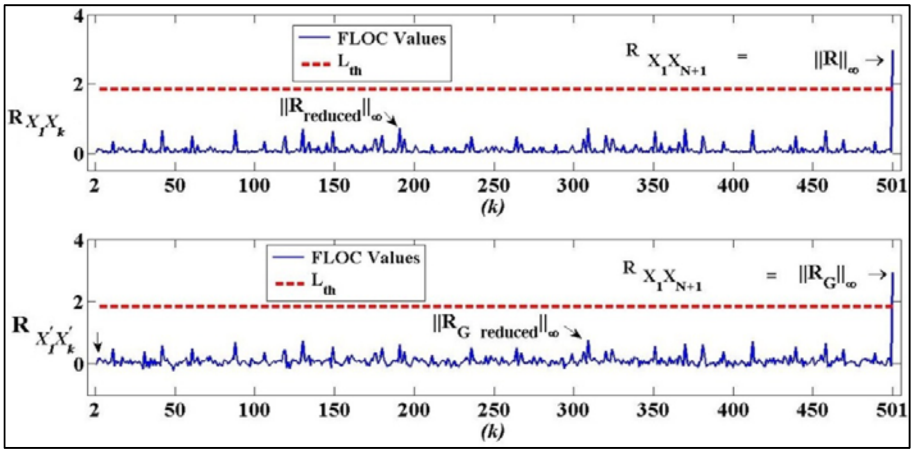


Figure 4.13. a) FLOCs of $\mathbf{X_1X_k}$ b) FLOCs of $\mathbf{X_1'X_k'}$

T_{psy} is chosen as one second therefore the corresponding T_{sample} is equal to $\frac{1}{500}$ second. D_{req} is chosen as two and hence *RCR* in (16) is 66 percent. The skewness parameter $\hat{\beta}$ equals to 1 and location parameter μ equals to 0 has been used throughout the this section while the characteristic exponent α equals to 1.6 and *MSNR* equals to -4 dB has been used to obtain Figure 4.12, 4.13, 4.14, 4.15.

Generation and FLOC of the Pilot Symbol and the Pilot Sequence:

The Pilot sequence P_1 and the noisy pilot sequence P_1', i.e. $P_1 + G$, are shown in the top and bottom of the Figure 4.12, respectively. The total duration of P_1' is three seconds since $T_{psy} = 1$ and $m=3$.

The FLOC values ($R_{X_1 X_k}$) between the pilot symbol X_1 and the pilot symbols X_k of P_1 are shown. Similarly in Figure 4b, the FLOC values ($R_{X_1' X_k'}$) between the noisy pilot symbol $X_1^{'}$ and the pilot symbols $X_k^{'}$ of $P_1^{'}$ are shown.

The value of L_{th} of R and R_G is also shown in Figure 4.13a and 4.13b, respectively.

Performance of the proposed PAS method and SB on receiver side:

The performance of the proposed SB on the receiver side is shown in this section. The three sampled versions of the received signal Y_n for FLOCCs are shown in Figure 4.14., which are obtained by the delay criteria in (54, 55). As explained above, the first received signal to SB might not be Y_1 and hence Y_{260} has been chosen arbitrary as the first received Y_n to the SB. Therefore, from the total duration of 3 seconds, i.e. $m \times N = 3 \times 500$ samples, of the pilot sequence, the first 0.5 seconds, i.e. 259 samples approximately, are considered as not being received to the SB on receiver side while the later 2.5 seconds, i.e. 1241 samples, is considered as being received for decoding and establishing synchronization.

The outputs of TDs and L_{th} are shown in Figure 4.15a and in Figure 4.15b the first pilot symbol interval T_{tr}^1 ends at S_{acq}^1 when outputs of TDs are bigger than L_{th}. According to Figure 4.15a, the output of two TDs crossed the L_{th} after 0.4 seconds approximately, hence resulting in CR of 66 percent therefore it has been registered as First acquisition, i.e. $S_{acq}^1 = 0.4\,sec$. Similarly, $S_{acq}^2 = 1.4\,sec$ is made after $T_{tr}^2 = 1\,sec$ and hence after two, i.e. $m - 1$ acquisitions, the DAT gives the exact time of data acceptation, i.e. $T_{data} = 2.4\ sec$, in (59).

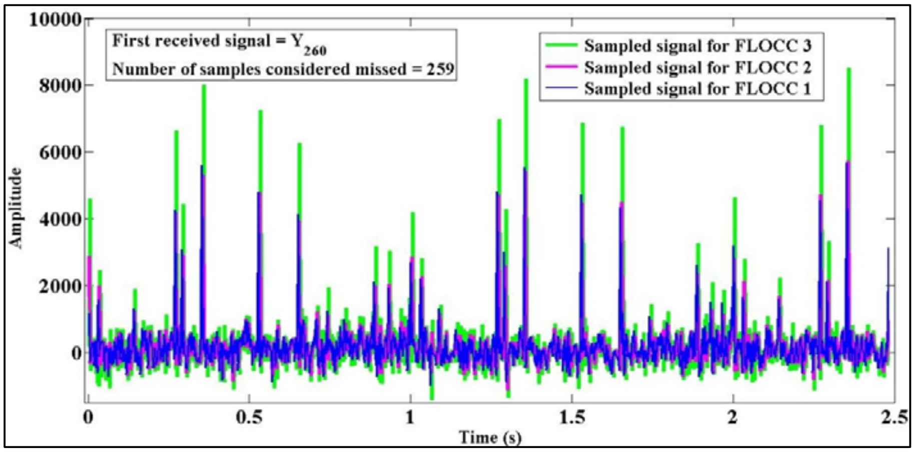


Figure 4.14. Received signals $\mathbf{Y_n}$ through AWGN channel

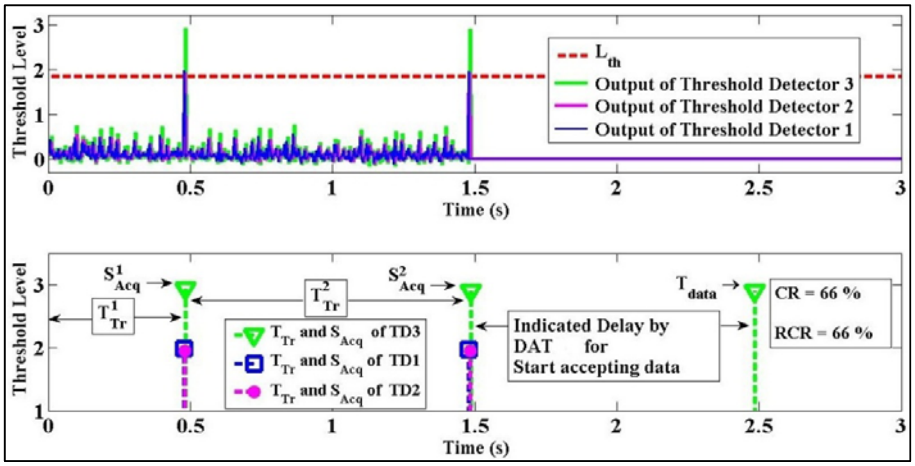


Figure 4.15. a) Output of Threshold Detectors b) Output of Synchronization Control Block

4.2.6. BER Performance Evaluation

The BER vs. MSNR performance of the proposed system for various characteristic exponents has been shown in Figure 4.16. The proposed system has shown efficient performance as it is capable to achieve the targeted BER of 10^{-3} even with increased characteristic exponents, i.e. decreased impulsiveness. Moreover, the BER at any specific $MSNR$ can be improved further by decreasing the characteristic exponent.

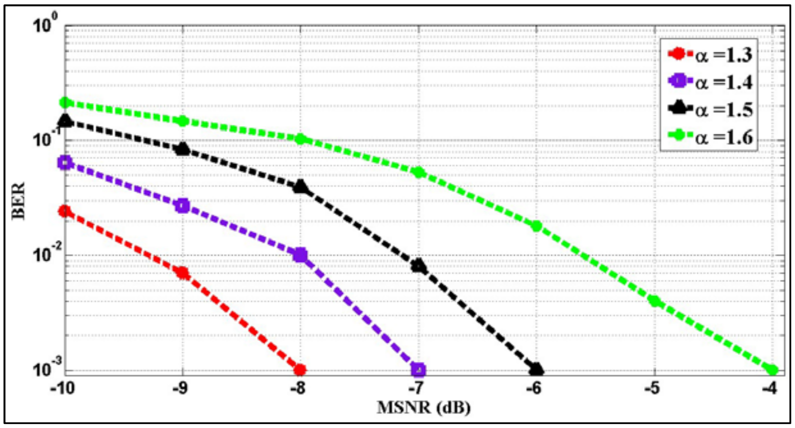


Figure 4.16. BER vs. MSNR for different characteristic exponents 'α'

Effects of number of FLOCCs and TDs on CR:

The number of TDs and FLOCCs in SB affect the Confidence Ratio (CR). The increase in the number of TDs and FLOCCs increase the CR as shown in Figure 4.17. Hence the confidence of the proposed synchronization scheme increases. The criterion '*CR versus D'* can be used to check the performance of any pilot sequence in establishing synchronization in RCS in comparison to the proposed pilot sequence obtained from α-stable noise. Also, the performance of the pilot sequences obtained from same or different noise distributions in different channels can also be analyzed.

Since, the Pilot Symbols have α-stable distributions with infinite variance; it keeps the layer of security in preventing intruders during the synchronization interval. Also, the number of Pilot Symbols in the Pilot Sequence and the number of TDs in the SB are chosen a priori, both by the transmitter and the intended receiver; therefore, these parameters, besides increasing the security level, also allow the users to adjust the RCS according to the channel impairments. Moreover, using different impulsiveness parameter, i.e. characteristic exponent 'α', and the skewness parameter, i.e.$\hat{\beta}$, might bring capability to adjust the security of RCS for various channel conditions.

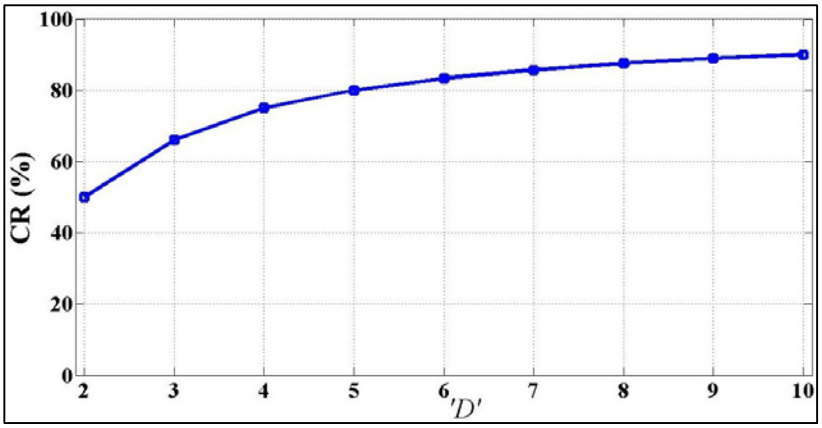


Figure 4.17. Confidence Ratio versus Number of detectors and FLOCCs in SB (CR versus D)

Due to the utilization of α- stable noise, which has infinite variance, both as a random carrier and as a pilot symbol; the proposed PAS method for RCS might therefore, be more secure in comparison to different noise based and chaotic pilot symbol based synchronization methods. The new criteria *CR* and *RCR* in SB can also be used to measure the performance of any PAS methods for spread spectrum based communication systems.

4.2.7. Optimization Criterion for Synchronized RCS

Previously, the concept of PAS and FLOC has been incorporated together to synchronize α-stable noise based communication system which gave birth to SRCS. In this section, an optimization criterion, i.e. FLOC Margin, has been proposed to improve the efficiency of the FLOCCs at the receiver side, hence, resulting in enhanced BER performance of SRCS. Since, the characteristic exponent and impulsiveness parameter are mainly responsible in generating and shaping up the required pilot sequence, therefore, the effects of these parameters on BER performance has also been observed by fluctuating them in their respective ranges. It has been shown that the proposed optimization criterion increases the BER efficiency of SRCS and also reveals the specific range of the characteristic exponent and impulsiveness parameter which can be exploited to achieve the optimum performance.

4.2.7.1. Optimization Criterion

It is known that L_{th} is pre-computed in SRCS to permit the intended receiver to initiate the threshold detection process and facilitate in taking the hard decision. Since, L_{th} is decided by the maximum and minimum FLOC values for $R_{X_1X_k}$, i.e. $||R||_\infty$ and $||R_{red}||_\infty$, respectively, therefore, it is necessary to study the effects of maneuvering the difference between $||R||_\infty$ and $||R_{red}||_\infty$ by fluctuating α and β in their respective ranges. The idea will help in improving the detection process of the intended receiver by identifying the requisite pilot symbol X_1 much easily among all other un-requisite pilot symbols X_k. Similarly, the best values of α and β can also be determined which can be used to increase the difference between $||R||_\infty$ and $||R_{red}||_\infty$, hence, resulting in optimized SRCS's BER performance.

FLOC Margin:

The proposed optimization criterion, i.e. FLOC Margin, denoted by 'M', is defined as

$$\mathrm{M} = ||R||_\infty - ||R_{red}||_\infty \tag{62}$$

The SRCS would be considered as optimized as big the M, i.e. as bigger difference between $||R||_\infty$ and $||R_{red}||_\infty$, hence, resulting in better BER performance. In contrast, M close to zero, i.e. as the difference between $||R||_\infty$ and $||R_{red}||_\infty$ becomes smaller, results in worst BER performance of SRCS.

Optimized Parameter values:

According to the proposed criterion of FLOC Margin, the values of α and β which correspond to greater M are expected to give optimized BER performance, hence, referred as Optimized Parameter Values, i.e. OPV, of SRCS. Both M and OPV can be used to obtain optimum BER performance in SRCS, i.e. RCS synchronized by α-stable pilot sequence, and also for all other RCSs.

The performance of the SRCS has been evaluated in accordance to the proposed criterion of M and OPV by BER vs. MSNR. Similarly, the BER is computed as the faulty number of bits divided by the total number of transmitted bits in the logarithmic scale where a total of one thousand bits have been transmitted and compared to obtain the BER vs. MSNR.

4.2.7.2. Performance Evaluation

The associated parameters of SRCS have been taken as '*m=D=3' and 'N=500'* which are pre-decided between the transmitter and the intended receiver. The *MSNR* have been taken as -4 dB to acquire Figure 4.18, 4.19, 4.20, 4.21.

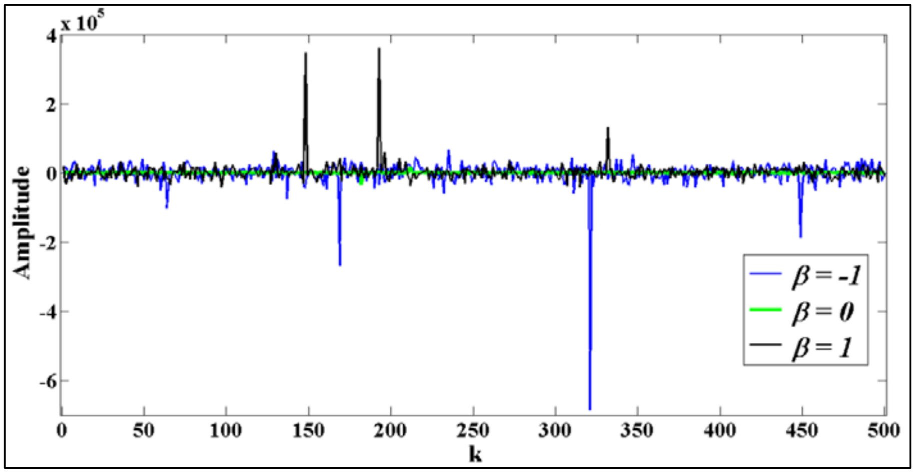


Figure 4.18. Pilot Sequences taken from S $_{\alpha=0.5}$ (β, **γ**=1, μ=0)

Pilot Sequence Analysis:

As shown in Figures 4.18 and 4.20, various versions of the noisy Pilot symbol X_1, i.e. $X_1 + G$, have been generated by varying α and β. It has been observed that the amplitude of X_1 increases with the decrease in α, i.e. X_1 becomes more impulsive, and as β approaches to zero, i.e. X_1 becomes less skewed. As a consequence shown in Figures 4.19 and 4.21, the difference between $||R\,||_\infty$ and $||R_{\ red}\,||_\infty$, increases with the decrease in α and as β approaches to zero, hence, resulting in bigger M. Similarly, the difference between $||R||_{\infty}$ and $||R_{red}||_{\infty}$, decreases with the increase in α and as β approaches to its extreme value of absolute one, hence, resulting in smaller M. B

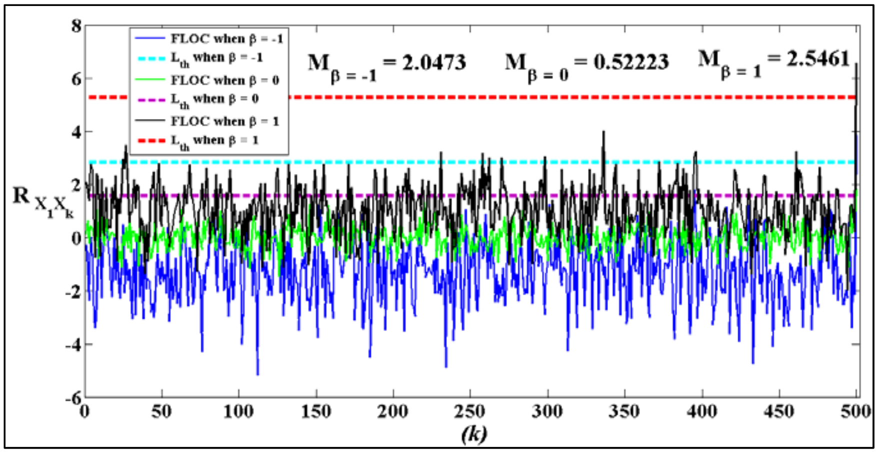


Figure 4.19. FLOCs of X_1X_k for Pilot Sequences taken from S $_{\alpha=0.5}$ (β, γ=1, μ=0) with corresponding threshold margins 'M'

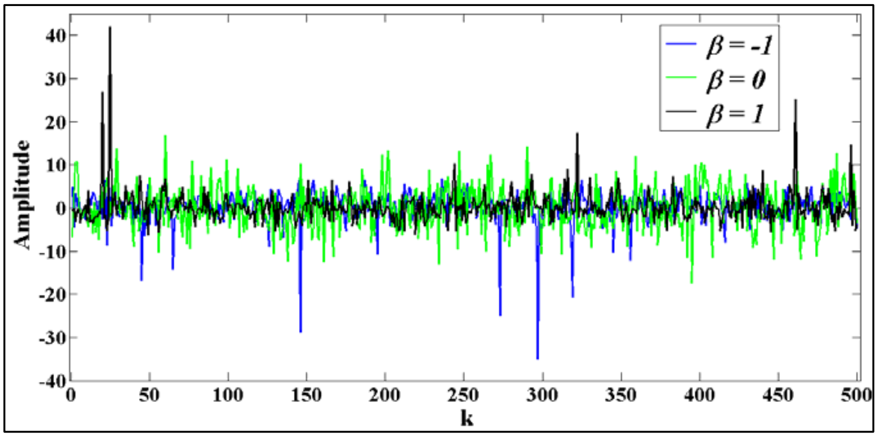


Figure 4.20. Pilot Sequences taken from S $_{\alpha=1.5}$ (β, **γ**=1, μ=0)

BER Improvement:

It is predicted by the proposed optimization criterion, that the versions of the noisy pilot symbols X_1 possessing bigger M in Figure 4.19, i.e. X_1 ~ S$_{\alpha=0.5}$ (β=*1,* ɤ, μ)

and $X_1 \sim S_{\alpha=0.5}$ (β=-1, Υ, μ), and in Figure 4.21, i.e. $X_1 \sim S_{\alpha=1.5}$ (β=1, Υ, μ) and $X_1 \sim S_{\alpha=1.5}$ (β=-1, Υ, μ), should give better BER performance of SRCS. Therefore, it can be seen in Figure 4.22, that slanting β of X_1 towards its extreme left, i.e. β = - 1, or towards its extreme right, i.e. β = 1, results in efficient BER performance of SRCSs. However, decreasing β or slanting β of X_1 towards its mid value, i.e. β = 0, results in worst BER performance of SRCSs. Similarly, increasing the impulsiveness of X_1, i.e. decreasing α, results in efficient BER performance of SRCSs. However, decreasing the impulsiveness of X_1, i.e. increasing α, results in worst BER performance of SRCSs

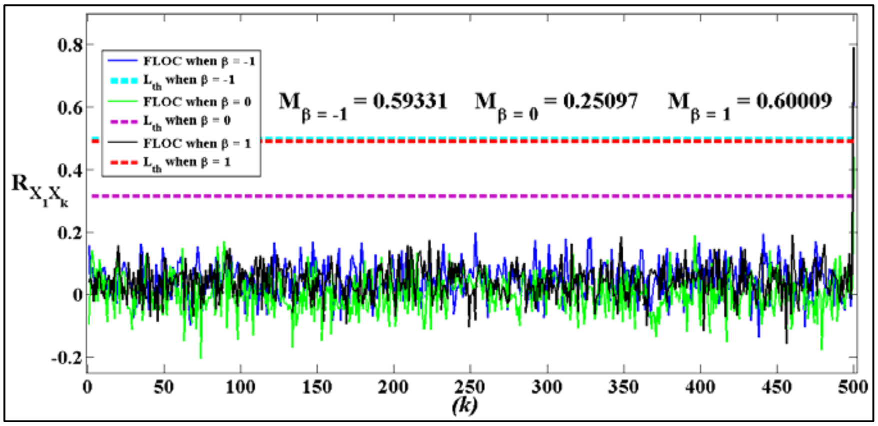


Figure 4.21. FLOCs of X_1X_k for Pilot Sequences taken from S $_{\alpha=1.5}$ (β, γ=1, μ=0) with corresponding threshold margins 'M'

The optimization of Fractional lower order covariance based synchronization method for Random communication systems has been performed by the proposed criterion, i.e. FLOC Margin. The introduced criterion assists the transmitter and the intended receiver in pre-deciding the specific value of characteristic exponent 'α' and impulsiveness parameter 'β' for pilot sequence generation. By choosing the parameter values of 'α' and 'β' from the prescribed range, the detection ability of the Fractional lower order covariance based Correlators can be enhanced to the optimum level, hence, the received pilot sequence can be filtered out and recognized comfortably by the intended receiver. Therefore, precise synchronization can be established in minimum duration by utilizing the proposed criterion.

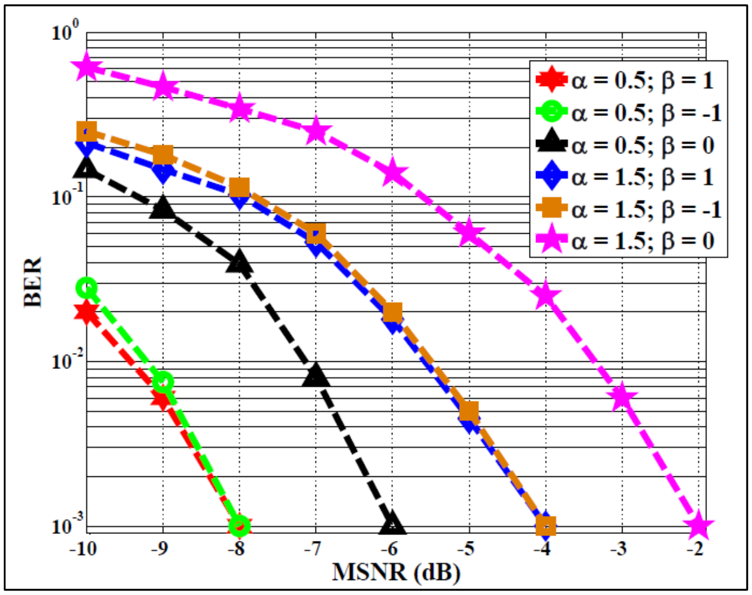


Figure 4.22. BER vs. MSNR performance of S-RCS for various 'α' and 'β' after optimization

Since, Synchronized Random Communication Systems utilizes the pilot sequence which has been generated from α-stable distribution; therefore, the proposed criterion has been made to increase the performance of the FLOCCs. However, the concept can be applied to other threshold based communication systems as well**.**

CHAPTER 5

SECURITY AND COVERTNESS OF ALPHA-STABLE NOISE BASED RANDOM COMMUNICATION SYSTEMS

This chapter first considers the problem of the absence of any criterion to compare the security and covertness of the α-stable noise based RCSs. In this regard, security performance, the criterion to measure the security level of RCS, i.e. Security Performance Tradeoff Characteristics (SPTC), has been introduced. Similarly, the authors have revisited Skewed α-stable Noise Shift Keying (SkαS-NSK) based RCSs, proposed in chapter 4, in the presence of an imperfectly synchronized eavesdropper. Later on, the criterion to compute eavesdropper probability and covertness value have been proposed to measure the covertness level of RCSs in the presence of an eavesdropper who has no knowledge of synchronization method used by the transmitter and the intended receiver.

Since there is no attack available to judge the actual existing vulnerabilities of α-stable noise based RCS, therefore, secondly, this chapter also introduces a novel blind recognition method to detect the presence of real-valued SαS and SkαS random carrier signals in AWGN channel from the perspective of an eavesdropper. The attack has helped in determining the most suitable values of the associated parameters of the carrier signal to ensure security while utilizing RCSs.

To address the determined vulnerabilities of RCSs, an inverse system approach has been used to construct α-stable noise driven transmitter and receiver which has produced maximum covertness value on our proposed covertness criteria among α-stable noise carrier based RCSs.

5.1. Motivation and Background

As discussed in chapter 3, the incremental improvement in BER performance of RCSs in the last decade is due to the fact that every proposed model has utilized different estimator based receiver to achieve efficient BER. In this regard, the proposed optimized model of RCS in Chapter 4 has the most optimum BER performance. However, there is no criterion to compare the security and covertness of α-stable noise based RCSs. Thus, this area has an immense potential which can help in enhancing the security of RCSs. Therefore, two new criteria related to security, i.e. SPTC, and covertness, i.e. measure of covertness, has been introduced in sections given below.

5.2. Security Performance Tradeoff Characteristics of RCSs

Random communication schemes always face a classical trade-off problem of balancing between an acceptable BER and the possibility of interceptors to decode our message but no criterion has been introduced yet to reflect it. The scheme can be defined as the RCS for a specific impulsiveness parameter '$\boldsymbol{\alpha}$' and MEVM estimator parameters 'L and K'. In the sequel, the SPTC for determining the security of the proposed random communication scheme based on the following definitions have been newly introduced.

Definition 1: Security Parameter '$\Delta\boldsymbol{\beta}$'

Security parameter $\Delta\boldsymbol{\beta}$ is used to obtain the security performances of the schemes and is defined as

$$\Delta\boldsymbol{\beta} \triangleq \boldsymbol{\beta}_{\mathbf{1}} - (-\boldsymbol{\beta}_{\mathbf{0}}) \tag{63}$$

Definition 2: Security Level '$\boldsymbol{S_L}$'

$\boldsymbol{S_L}$ is the required security level chosen by the users for the percentage of security required and it lies within $\mathbf{0} \leq \boldsymbol{S_L} \leq \mathbf{1}$.

Definition 3: Security Boundary function 'B (.)'

SPTC can give an optimal boundary based on the Security Boundary function which can be considered as a BER function with respect to the security parameter *'$\Delta\beta$'* and is denoted by $B(\Delta\beta)$ and lies with in $0 \leq B(\Delta\beta) \leq 1$.

For the chosen S_L the security boundary function *B (.)* has been constructed from the following iterative relation given below in (64)

$$B\left(\Delta\beta^{(k+1)}\right) = B\left(\Delta\beta^{(k)}\right) \ . \ \Delta\beta^{(k+1)} \ . \ (1 - S_L) \qquad (64)$$

where

$$\Delta\beta^{(k)} = (\ 0.2\ ) \ . \ k \qquad k\ = 0,\ 1.....10 \qquad 0 \leq \Delta\beta^{(k)} \leq 2 \qquad (65)$$

with initial condition $B\left[\ \Delta\beta^{(0)}\right] = 1$ which is actually the achievable Maximum BER for the random communication system.

Definition 4: Strength of the Security Boundary 'S_{sb}'

S_{sb} is the sum of all BER's obtained from the security boundary function with respect to the corresponding $\Delta\beta^{(k)}$of the security boundary i.e.

$$S_{sb} \ = \sum_k B_{S_L}(\Delta\beta^{(k)}) \qquad (66)$$

where $B_{S_L}(.)$ corresponds to security boundary function *B(.)* for the specific security level S_L. This is actually approximation of the area under the *B (.)*

$$S_{sb} \ \cong \frac{1}{0.2} \int_{k=0}^{10} B_{S_L}(\Delta\beta) \ . \ (\Delta\beta) \qquad (67)$$

Definition 5: Strength of the scheme 'S_s'

S_s is the sum of all values obtained from $B_s(.)$ with respect to corresponding $\Delta\beta^{(k)}$ for that specific scheme

$$S_s \ = \sum_k \ \ B_s(\Delta\beta^{(k)}) \qquad (68)$$

where $B_s\ (.)$ corresponds to the function which gives BER for the specific scheme at each $\Delta\beta^{(k)}$.

Definition 6: Secure Scheme

The schemes whose $B_s\,(.)$ lie above the security boundary $B_{S_L}(.)$ are not secure while the schemes whose $B_s\,(.)$ lie below the security boundary $B_{S_L}(.)$ are considered as secured as shown in Figure 5.1.

Since some of the schemes intersect the security boundary so they cannot be classified according to the above definition. Therefore, the following definition for such schemes has been given below.

Definition 7: Cost of any Scheme 'C_s'

The Cost of a scheme 'C_s' can be calculated to determine the security especially for those schemes which are intersecting the security boundary

$$C_s \triangleq S_s - S_{sb} \tag{69}$$

Negative cost indicates secure scheme and positive cost indicates vulnerable scheme. The absolute value of the C_s indicates either more secure or more vulnerable scheme. SPTC with security boundaries '$B_{S_L}(.)$' for all security levels 'S_L' obtained from the above security boundary function *B (.)* as given in (64) is shown in Figure 5.1.

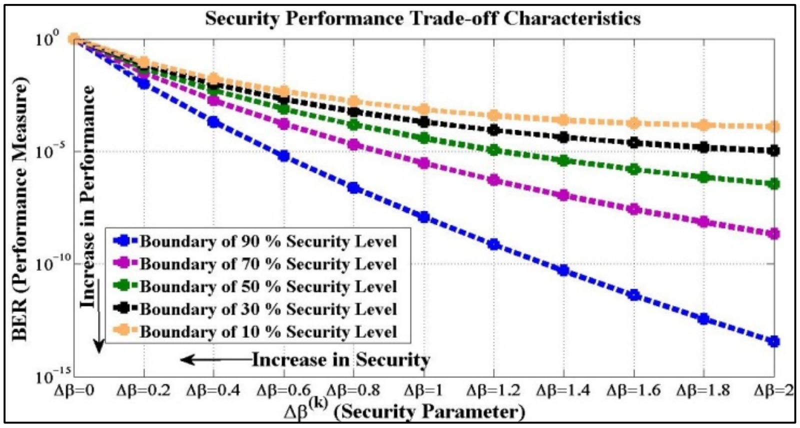


Figure 5.1. BER vs. Security Parameter (Δβ) with different S_L

5.2.1. Security Analysis of the proposed Optimized model of RCS

The results based on above criteria for our system have been shown in Figure 5.2. The increase in Δβ (i.e. the increase in the differences of the skewness of the noise distributions of the related binary messages) results in better BER. By decreasing the Δβ makes it difficult for an eavesdropper to decode the binary message since the amount of positive and negative samples for the corresponding binary messages are getting almost equal (i.e. the distributions of the coresponding binary messages are more similar). Therefore, in Figure 5.1, Δβ is also labelled as 'security parameter' on x-axis while the BER on y-axis is labelled as 'performance measure'.The increase in the impulsiveness of the noise data (i.e decrease in 'α') would result in the heavy tail of the corresponding noise distribution used to encode the binary message. Hence, making it easy for the MEVM estimator to estimates the beta parameters from the mixture of AWGN noise *(i.e. α =2)* and the transmitted α-stable noise *(i.e. $\alpha \neq 2$)* which results in better BER. While the decrease in impulsiveness of the noise data will make the system more secure by mixing the samples of the transmitted signal for the corresponding binary message extremely close to the samples of AWGN channel.

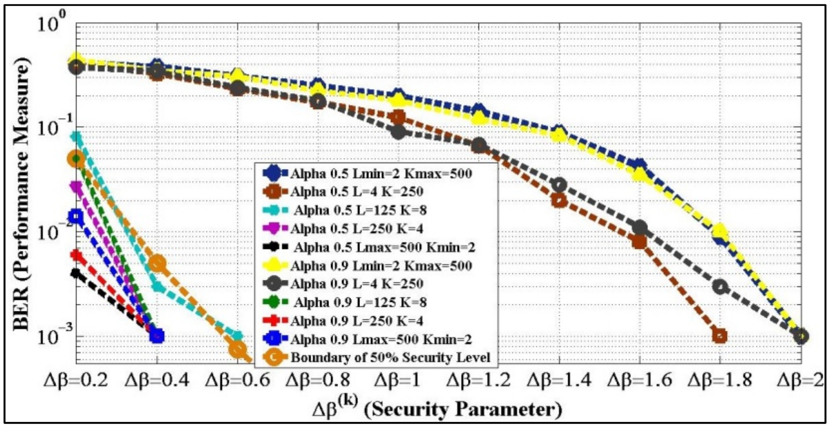


Figure 5.2. BER vs. Security Parameter (Δβ) with different 'α' parameters and 'L & K' of estimator; transmitted bits=1000; S_L =0.50

The cost of all schemes "C_s" for their coresponding S_s have been given in Table 5.1. As mentioned earlier, the schemes whose BER's are below the security boundary have their costs in negative and hence more secure. Also, the scheme like "$\alpha = 0.5$, L=125, K=8" whose BER's intersects the security boundary has negative cost. So the scheme "$\alpha = 0.5$, L=125, K=8" can be considered as secured which cannot be known without C_s just by looking at Figure 5.2

Table 5.1. Cost of Different schemes for their corresponding Strengths

	Name of Scheme	S_{sb}	S_s	C_s
$\alpha = 0.5$	L_{min}=2 K_{max}=500	0.0559	1.1862	1.1303
	L=4 K=250	0.0559	0.7334	0.6775
	L=125 K=8	0.0559	0.0180	- 0.0379
	L=250 K=4	0.0559	0.0058	- 0.0501
	L_{max}=500 K_{max}=2	0.0559	0.0084	- 0.0475
$\alpha = 0.9$	L_{min}=2 K_{max}=500	0.0559	1.1020	1.0460
	L=4 K=250	0.0559	0.7346	0.6787
	L=125 K=8	0.0559	0.0108	- 0.0451
	L=250 K=4	0.0559	0.0124	- 0.0435
	L_{max}=500 L_{max}=2	0.0559	0.0032	- 0.0527

.

Increment in L or decrement in K increases the computational complexity and vice versa. So accuracy and complexity tradeoff would depend on the type of communication data.

Conclusive remarks:

Our proposed optimized model of RCS based on MEVM estimator for skewed α-stable distribution shift keying is not only fast and outperforms the receivers based on

COV and FLOC given in the Chapter 4. Our proposed receiver also introduces the advantage of variable computational complexity and performs extremely well based on the newly introduced security criterion ‘SPTC’ to compare the random communication systems which are based on α-stable noise parameter modulation.

5.3. Measure of Covertness for RCSs

Random Communication Systems and the optimized models of RCSs discussed in the Chapter 3 and Chapter 4, respectively, have assumed perfectly synchronized transmitter and receiver. However in this section, instead of assuming perfect synchronization approach in RCSs, the effects of imperfect synchronization (IS) on SkαS-NSK based RCS have been observed through simulations. The BER performance of the eavesdropper with respect to his synchronization error in SkαS-NSK based RCS, has been analyzed. An expression for the probability of an eavesdropper to decode the binary information (i.e., Eavesdropping Probability) in SkαS-NSK based RCS, has been derived. The criterion (i.e., Covertness Value) to measure the covertness level of RCSs has also been proposed. The BER performance of an eavesdropper provides an approximate margin of synchronization error if it can be overcome by an eavesdropper then he can achieve the decoding (i.e., eavesdropping) process.

5.3.1 Aspect of Imperfect Synchronization

Synchronization not only plays a key role in establishing successful communication link between transmitter and receiver but it also helps in boosting the performance in all types of communication systems. Especially, in Spread Spectrum (SS) based communication systems IS has a huge impact on the performance. As the average BER which is the basic performance measure in digital communication systems, the efforts to analyze the impact of IS on BER started to gain attention at the beginning of 1970’s Stiff1er (1971). However in Todorovic (1989), a comprehensive analysis for the impact of IS on single carrier Direct Sequence Spread Spectrum (DS-SS) communication system was performed in which the expressions for the upper and lower bound of BER were also derived. In Jos et al. (2010), an accurate analytical model for Overloaded Direct Sequence Code Division Multiple Access (DS-CDMA) system under IS was presented. Moreover in He et al. (2010), the multi-tone (i.e., multi-carrier) DS-SS communication systems were also examined by changing the synchronization parameter. So, the factor of IS has been investigated in all types of spread spectrum based communication systems.

Also in collaborative communication, in which a number of wireless transmitters collaboratively transmit the same message signal to the common target receiver, the effects of imperfect frequency and phase synchronization were also monitored to increase the BER performance in Naqvi et al. (2009) and Naqvi et al. (2009b).

Similarly in Power Systems (PSs), the time synchronization sensors known as “Phasor Measurement Units” were analyzed for imperfect phase synchronization to improve the PS’s state estimation performance in Yang et al. (2013). Likewise in neural communication networks, which have interconnected group of nodes in the vast network of neurons in the brain, the factor of average synchronization time error has also been used to analyze the security of cryptographic methods in Mislovaty et al. (2004).

Random Communication System is newly evolving branch of Spread Spectrum based covert communication. All previous investigations on RCS’s have assumed perfect synchronization between the transmitter “Alice” and the receiver “Bob”. However, no approach has been proposed yet to evaluate the covertness of the RCS’s in the presence of an eavesdropper “Willie” with synchronization uncertainty.

5.3.2. Approach to Measure Covertness in RCSs

Since true level of covertness cannot be guaranteed by utilizing a stochastic process as a random carrier and assuming perfect synchronization scenario between Alice and Bob, therefore in this section, we have evaluated the covertness of the SkαS-NSK based RCS by analyzing the BER performance of an eavesdropper “Willie” who imperfectly synchronizes with the transmitter “Alice” and tries to decode (eavesdrop) the binary information. Therefore, an expression known as “Eavesdropping Probability” is introduced to calculate the probability of Willie to successfully decode the binary information which has been transmitted by Alice. Moreover, the covertness level of the SkαS-NSK based RCS, used by Alice and Bob to communicate secretly, is also evaluated by the derived expression known as "Covertness value". The BER performance of Willie also provides an approximate margin of synchronization error, owned by Alice and Bob to covertly communicate by using SkαS-NSK based RCS and should be overcome by Willie to successfully continue the hacking process.

The SkαS-NSK based RCS's transmitter and Modified Extreme Value Method (MEVM) based receiver for covert communication between Alice and Bob has been originally proposed in Ahmed et al. (2017) and that work has been modified, as shown in Figure 5.3, to observe the presence of an eavesdropper Willie and compute his BER performance. Similarly, the covertness level of the modified SkαS-NSK based RCS can also be evaluated now on the basis of Willie's BER performance due to his uncertain knowledge about the synchronization method used by Alice and Bob.

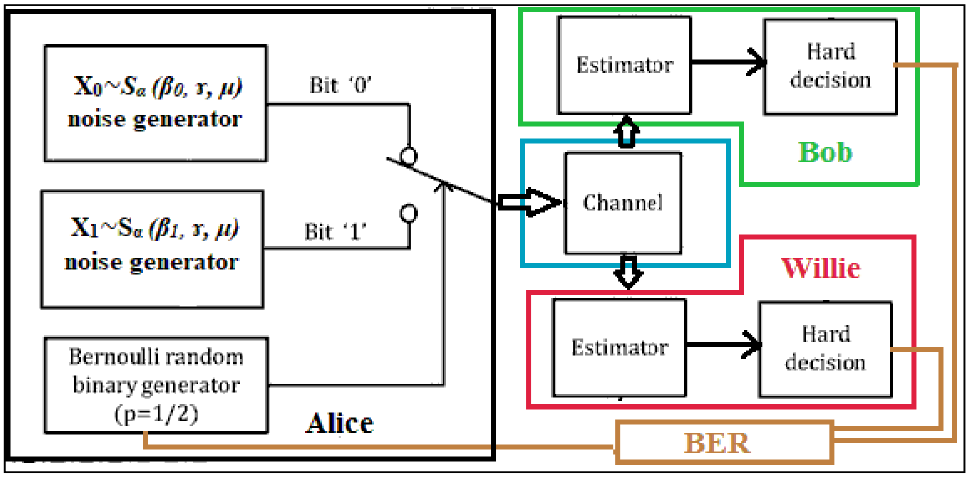

$X_0 \sim S_\alpha(\beta_0, \gamma, \mu)$ noise generator
Bit '0'
$X_1 \sim S_\alpha(\beta_1, \gamma, \mu)$ noise generator
Bit '1'
Bernoulli random binary generator (p=1/2)
Alice
Estimator
Hard decision
Bob
Channel
Willie
Estimator
Hard decision
BER

Figure 5.3. Block diagram Modified SkαS-NSK based RCS

Eavesdropper 'Willie' in Noise Shift Keying based RCS:

It is assumed that the intended receiver "Bob" and the eavesdropper "Willie" use the same receiver proposed in Areeb et al. (2017). Additionally, it is also assumed that both of them know the transmitted duration or length of a single noise sample denoted by " T_b", transmitted number of noise samples per binary information bit denoted by *"N"* and duration needed to decode single binary information bit denoted by "T_s" (i.e., $T_s = T_b N$). Bob is assumed to be perfectly synchronized with Alice and knows the exact time instant to accept the noise samples for the corresponding first binary information bit. However, Willie has no knowledge of the exact time instant to accept the noise samples for the corresponding binary information bits therefore Willie would face a synchronization error which would result in increased BER.

Apart from the choice of stochastic processes as random carrier, the actual method to obtain synchronization between Alice and Bob in RCS is still an open issue. Therefore in this section, we have focused on investigating how the imperfectly synchronized Willie can listen to the modified SkαS-NSK based RCS used by Alice and Bob.

Assuming that, we have a synchronization error denoted by δ in the range $0 \leq \delta \leq 1$ and Alice has transmitted the binary information bits as logic '101….', then the corresponding noise sequences "$S_\alpha(\beta_1, \gamma, \mu)$, $S_\alpha(\beta_0, \gamma, \mu)$, $S_\alpha(\beta_1, \gamma, \mu)$.........." have been transmitted. Since Willie is imperfectly synchronized with Alice and have no knowledge of the exact time instant to accept the noise samples for the corresponding initial transmitted binary information bit 1, Willie would wrongly receive totally N samples of which (1- δ) N samples are from the distribution $S_\alpha(\beta_1, \gamma, \mu)$ *(i.e.,* $x_i \sim S_\alpha(\beta_1, \gamma, \mu)$*)* and δN samples are from the other distribution $S_\alpha(\beta_0, \gamma, \mu)$ *(i.e.,* $y_i \sim S_\alpha(\beta_0, \gamma, \mu)$*)* in the duration T_s which is represented as below

$$\{x_1 \dots\dots\dots x_{(1-\delta)N}, y_1 \dots\dots\dots y_{\delta N}\} \qquad (70)$$

Similarly for the second transmitted binary message bit '0', the Willie will again wrongly receive total N samples of which (1- δ) N samples are from the distribution $S_\alpha(\beta_0, \gamma, \mu)$ *(i.e.,* $y_i \sim S_\alpha(\beta_0, \gamma, \mu)$ and δN samples are from the other distribution $S_\alpha(\beta_1, \gamma, \mu)$ *(i.e.,* $x_i \sim S_\alpha(\beta_1, \gamma, \mu)$*)* which is represented as below

$$\{y_1 \dots\dots\dots y_{(1-\delta)N}, x_1 \dots\dots\dots x_{\delta N}\} \qquad (71)$$

However, Bob is perfectly synchronized with Alice and knows the exact time instant to accept the noise samples for all corresponding transmitted binary information bits. Hence, Alice will receive the transmitted binary information bits as '101.......' which was originally sent by Alice. Therefore, Bob would face negligible or ideally erratic bits while Willie would face increased BER with respect to the variation in the synchronization error 'δ'.

5.3.2.1. Performance of an Eavesdropper

Willie denoted by "$BER_W(\delta_i)$" for the corresponding *i-th* synchronization error 'δ_i' is considered as a BER function with respect to the synchronization errors *"δ_i"* which lies with in $\frac{1}{n} \leq BER_W(\delta_i) \leq 1$ (where 'n' is the total number of transmitted binary message bits by Alice).

The $BER_W(\delta_i)$ also provides an approximate margin of synchronization error, own by Alice and Bob to covertly communicate by using SkαS-NSK based RCS.

5.3.2.2. Performance of the Intended Receiver

Since there is no synchronization error between Alice and the intended receiver 'Bob' therefore the BER of Bob, denoted by "BER_B", has been practically considered equal to $\frac{1}{n}$.

5.3.2.3. Eavesdropping Probability 'P_E'

It is assumed that the intended receiver "Bob" and the eavesdropper "Willie" uses the same receiver proposed in Areeb and Savaci (2017). Additionally, it is also assumed that both of them knows the transmitted. The *i-th* probability of an eavesdropper 'Willie' to decode the transmitted binary information bits with respect to synchronization errors δ_i is named as "Eavesdropping Probability" denoted by "$P_E(i)$" and it is defined as

$$P_E(\delta_i) = \frac{BER_W(\delta_i)}{BER_B} \tag{72}$$

which lies with in $0 \leq P_E(\delta_i) \leq 1$.

5.3.2.4. Covertness Value 'C_V'

The criterion to measure the covertness of the RCS used by Alice and Bob is named as "Covertness Value" denoted by " C_V " which is defined be as

$$C_V \ = \sum_i P_E(i) \tag{73}$$

The RCS used by Alice and Bob would be considered as covert as big the C_V. However, C_V close to zero implies less covert RCS. The absolute C_V indicates either more covert or more vulnerable RCS which can be used to analyze the covertness level.

5.3.2.5. Synchronization Error Margin 'SE_M'

The synchronization error margin denoted by "SE_M" is the *i-th* synchronization error 'δ_i' when the BER function "i.e., $BER_W(\delta_i)$" of Willie initially drops by $\frac{1}{n}$ in the range $0 \leq \delta_i \leq 1$ which is defined below as

$$SE_M = \delta_i \mid \ BER_W(\delta_i) < \frac{1}{n} \tag{74}$$

5.3.3. Covert Analysis of Optimized model of RCS

Simulation results for the covertness analysis of Alice and Bob's SkαS-NSK based RCS in the presence of an eavesdropper Willie, in accordance to the proposed criteria, has been done in this section. One thousand bits (i.e., $n = 1000$) has been used in simulations to obtain BERs. Different values of Δβ and α have been used to obtain results so that best parameters values can be found which should be recommended to Alice to covertly communicate with Bob when using SkαS-NSK based RCS.

In Figure 5.4, the BER performance of an eavesdropper Willie "$BER_W(\delta_i)$" with respect to all possible synchronization errors "δ_i", are shown. The increases in the differences of the skewness of the noise distributions of the related binary information bits (i.e., increase in Δβ) by Alice has resulted in better $BER_W(\delta_i)$. The distributions of the corresponding binary messages are more similar (i.e., decrease in Δβ) by Alice has worsened the $BER_W(\delta_i)$ since the amount of positive and negative samples for the corresponding binary information bits are getting almost equal. Therefore, small value for Δβ is recommended for Alice to covertly communicate with Bob when using SkαS-NSK based RCS.

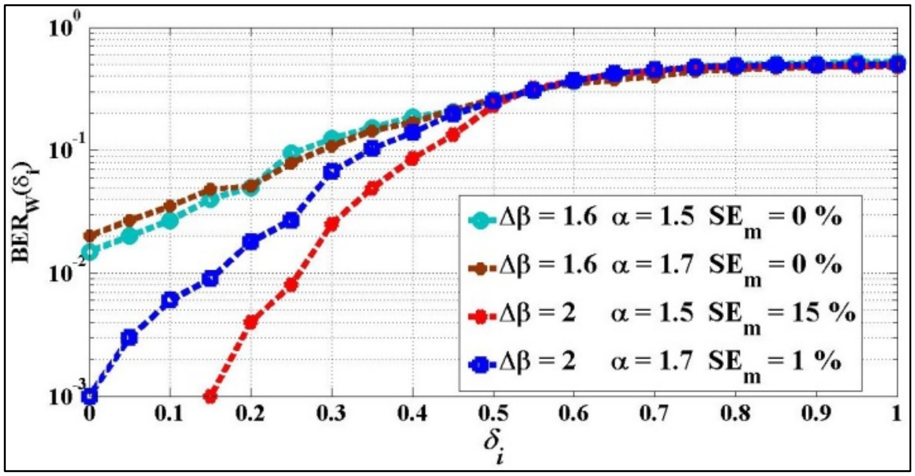


Figure 5.4. Performance of an eavesdropper Willie

However, decrease in α by Alice would result in the heavy tail of the corresponding noise distribution used to encode the binary information bits hence making it easy for the MEVM based receiver to estimate the beta parameters from the mixture of AWGN noise in the channel *(i.e., α =2)* and the transmitted α-stable noise *(i.e., α≠2)* which has resulted in better $BER_W(\delta_i)$. Therefore, higher value of α ($\alpha \to 2$)

is recommended for Alice to covertly communicate with Bob when using SkαS-NSK based RCS.

The resulted SE_M's for corresponding combinations of Δβ and α in Alice and Bob's SkαS-NSK based RCS has also been shown in Figure 5.5. It has been observed that Willie has less margin of synchronization error when Alice and Bob are using SkαS-NSK based RCS with small Δβ and higher α. Therefore from the resulted values of SE_M's in Figure 5.5, the recommendation for Alice and Bob is to utilise smaller value for Δβ and higher value for α, when using SkαS-NSK based RCS.

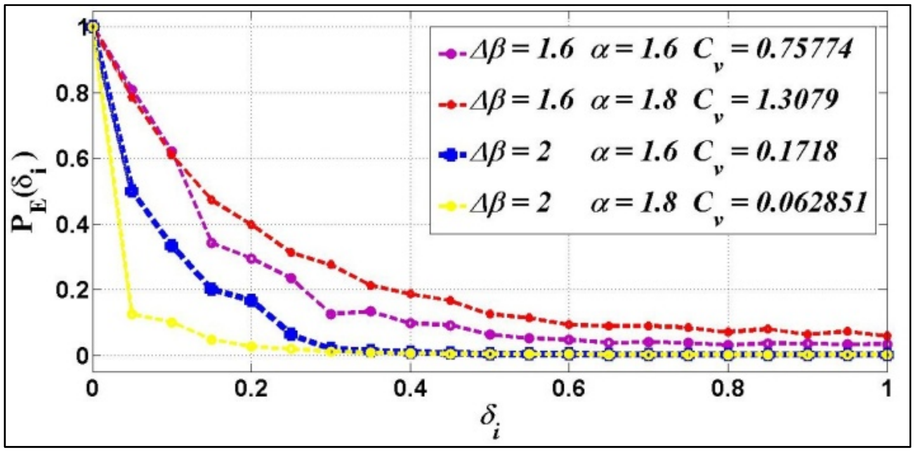


Figure 5.5. Covertness of Alice and Bob's SkαS-NSK based RCS

Based on the performance of an eavesdropper Willie, the eavesdropping probability "$P_E(i)$" with respect to all possible synchronization errors "δ_i" is shown in Figure 5.4. The covertness level (i.e., C_V) of Alice and Bob's SkαS-NSK based RCS is also shown in Figure 5.5. It is seen that Willie can decode the binary information successfully even with synchronization error up to some extent, if large Δβ and smaller α is used by Alice to communicate with Bob in RCS. Therefore Alice and Bob should select small Δβ and higher α in SkαS-NSK based RCS.

Conclusive Remarks:

We have revisited SkαS-NSK based RCSs in the presence of an imperfectly synchronized eavesdropper. The eavesdropper probability and covertness value have been proposed to measure the covertness level in the presence of an eavesdropper who has no knowledge of synchronization method used by transmitter Alice and intended receiver Bob. The SkαS-NSK based RCS shows promising results against eavesdropping with respect to synchronization errors if the recommended parameters values are used.

The impulsiveness and skewness parameters of α-stable noise can be maneuver on the transmitter side to improve the overall covertness level of SkαS -NSK based RCS which is a benefit of using α-stable noise as a carrier. Moreover, the optimum values for the impulsiveness and skewness parameters can be found by using the introduced criteria which can help Alice and Bob to communicate covertly when using SkαS -NSK based RCS. The parameters also help to achieve the desired anti covert probability and covertness value for the SkαS -NSK based RCS.

5.4. Fractional Lower-Order Auto-Covariance based Attack for Alpha-stable noise based RCSs

Invisibility of α-stable noise as carrier signals, in additive white Gaussian noise (AWGN) channel, is a key factor to ensure covert transmission by employing random communication systems (RCSs). This section introduces a novel blind recognition method for an eavesdropper to detect the presence of real-valued symmetric and skewed α-stable random carrier signals in AWGN channel. The introduced method is based on the proposed random carrier signal recognizer (RCSR) which consists of fractional lower-order auto-covariance block (FLOACB), threshold control block (TCB) and the random carrier signal recognition indicator (RCSRI). The proposed RCSR first detects the possible presence of α-stable random carrier signals and then recognize the impulsiveness and skewness parameters, exploited by the transmitter and the intended receiver, to extract covertly conveyed binary information. However, the determined covert range can be adopted to perform secure transmission by RCSs. The simulation results reflect the simplicity of the proposed method as it is capable to perform effectively in real-time by utilizing extremely less number of observed samples.

5.4.1. Introduction

In this section, the first blind detection, recognition and data extraction method for α-stable carrier signals has been proposed and analyzed from the perspective of an eavesdropper; where detection means to judge the possible presence of the carrier signals during real-time data reception in AWGN channel; signal recognition means to correctly recognize the associated parameters of α-stable carrier signals and data extraction means to extract the hidden binary information from the associated parameters by applying some hard decision rule. The part related to detection in the proposed idea is inspired from the auto-correlation based blind recognition method for chaotic carrier signals Sobhy and Shehata (2001). Since, the second and higher order statistics do not exist for α-stable distributions, any auto-correlation based blind recognition method is not applicable for blind recognition of α-stable carrier signals. Therefore, in this section, fractional lower-order covariance has been utilized to propose the first random carrier signal recognizer (RCSR) in the literature which follows the three step procedure to detect and recognize α-stable carrier signals and then extract the hidden binary information in real time. In the following sub-section, auto-correlation based blind recognition method for chaotic carrier signals have been briefly reviewed. Later on, the proposed three step procedure based on the introduced fractional lower-order auto-covariance block (FLOACB), threshold control block (TCB) and random carrier signal recognition indicator (RCSRI) have been explained. The results are shown in the later Section which is followed by conclusive remarks.

5.4.2. Prior Art

The auto-correlation based blind recognition method for chaotic carrier signals which has inspired us to propose the first blind recognition method for α-stable carrier signals has also been reviewed in this sub-section.

5.4.2.1. Blind Recognition of chaotic carrier signals by auto-correlation function

Chaotic carrier signals do not possess the capability to become invisible in AWGN channel hence their existence can always be revealed by an eavesdropper. This weak link resulted in many signal processing techniques which can retrieve the information from chaotic carrier signals Short (1994), Short, K.M. (1996), Sobhy and Shehata (2001), Alvarez et al. (2004) and Alvarez et al. (2004b); where auto-correlation based blind recognition technique is one of the first and simplest among them Sobhy and Shehata (2001). The first step of the method is to recognize the type of specific system used to generate noise like chaotic carrier signals. It can be done after producing a thumbprint of the utilized chaotic system in ways i) by finding the specific strange chaotic attractor from signal iteration plot; which is a plot of a signal with a delayed version of itself [see Fig. 1, 2 in Sobhy and Shehata (2001)]; ii) or by plotting the auto-correlation function of the time series; where every chaotic system has a unique auto-correlation plot [see Fig. 3 in Sobhy and Shehata (2001)]. Then the comparison of the produced thumbprint with already compiled library of plots can recognize the type of the utilized chaotic system.

After the recognition of the specific chaotic system, in the second step, the eavesdropper can extract the hidden binary information by generating the mimicked inverse system. The parameters of the inverse system can then be optimized to minimize the output and thus separate the chaotic signal and underlying binary information (see Fig. 9 in Sobhy and Shehata (2001)). Although other techniques are also available in Alvarez et al. (2004) and Alvarez et al. (2004b), but this simple two-step signal processing technique given in Sobhy and Shehata (2001) is sufficient for an eavesdropper to bring down the security of most commonly used chaotic communication systems.

5.4.3. Description of the Attack

In comparison to the two-step, i.e. recognition and extraction, method discussed above for blind recognition of chaotic carrier signals, α–stable carrier signals require one extra step which is to first detect the possible presence of α-stable carrier signals in the channel. After that, the type or associated parameter of α–stable carrier signals should be recognized which should be followed by the extraction of the binary information as a last step. Following the above prepared guidelines, blind recognition technique for α-stable carrier signals has been explained in this section. The three steps, i.e. detection, recognition and extraction by an eavesdropper, can be achieved by the proposed random carrier signal recognizer (RCSR). Before discussing the system model, two important concepts, utilized to establish the RCSR, has been given in the sequel.

5.4.3.1. Fractional lower-order auto-covariance of α-stable noise Signals

The Fractional lower-order auto-covariance (FLOAC) of α-stable random noise signal X can be defined as

$$R_d[k] \triangleq \boldsymbol{E}\ \{(x[i])^a \cdot (x[i+k])^b\} \tag{75}$$

for $0 \leq a < \frac{\alpha}{2}$ and $0 \leq \beta < \frac{\alpha}{2}$. Similarly, the estimated FLOAC of X can be computed as

$$\hat{R}_d[k] = \hat{R}_{XX}[k] \ = \frac{\sum_{i=L_1+1}^{L_2} |x[i]|^a \,.\, |x[i+k]|^b .\, sign(\, x[i] \,.\, x[i+k])}{L_2 - L_1} \tag{76}$$

The non-delayed FLOAC value, i.e. $\hat{R}_d[0]$ or $\hat{R}_{XX}[0]$, of α-stable random noise signal X has significant importance. It has played a key role in establishing pilot-assisted synchronization for RCSs as it provides the capability to differentiate between the requisite pilot symbol and all other non-requisite pilot symbols by accurately separating the estimated value $\hat{R}_d[0]$ and all other estimated $\hat{R}_d[k]$ due to the presence of large difference between them Ahmed and Savaci (2018). Moreover, it has also been shown in Ahmed and Savaci (2019). that the value $\hat{R}_d[0]$ of α-stable random noise signal X varies as the associated impulsiveness and skewness parameter of the utilized X are varied.

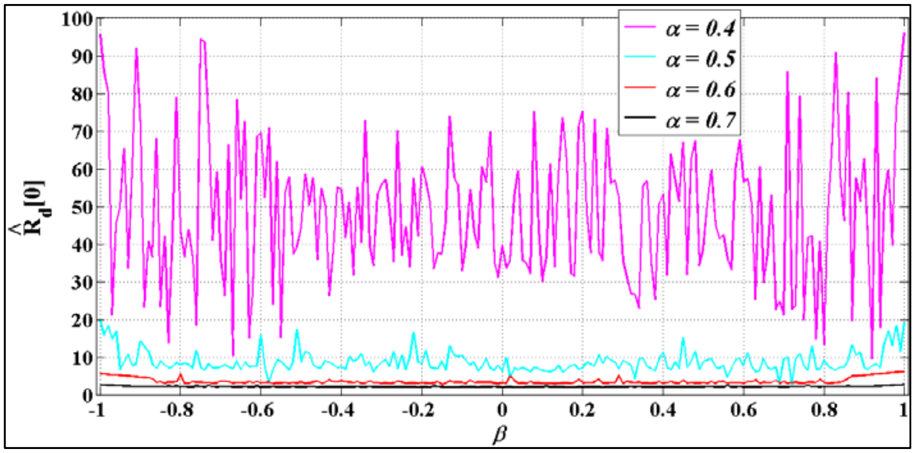


Figure 5.6. Non-delayed FLOAC '$\widehat{\mathrm{R}}_{\mathrm{d}}[0]$ or $\widehat{\mathrm{R}}_{\mathrm{XX}}[0]$' of X ~ $\mathrm{S}_{0.4\leq\alpha\leq0.7}$ (-1≤β ≤1, $\gamma = 1$, μ=0); for different α's

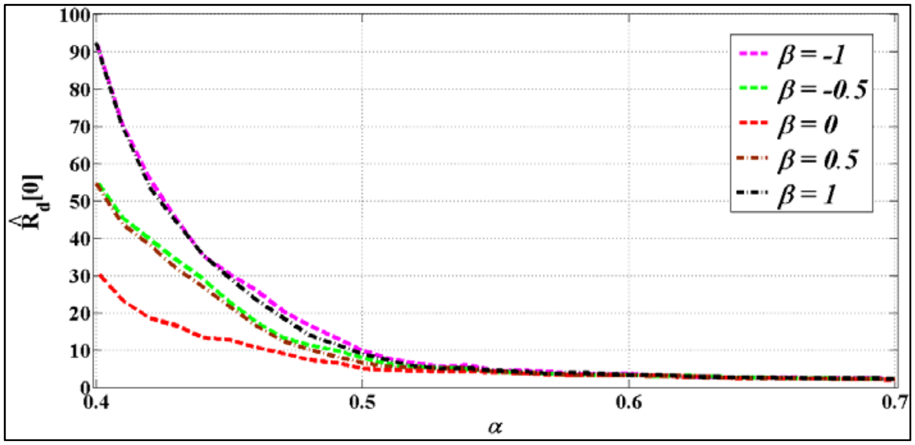


Figure 5.7. Non-delayed FLOAC '$\widehat{\mathrm{R}}_{\mathrm{d}}[0]$ or $\widehat{\mathrm{R}}_{\mathrm{XX}}[0]$' of X ~ $\mathrm{S}_{0.4\leq\alpha\leq0.7}$ (-1≤β ≤1, $\gamma = 1$, μ=0); for different β's

The detailed analysis related to non-delayed FLOAC has been presented in Figure 5.6-5.9; where it has been observed that $\hat{R}_d[0]$ increases (decreases) if X has been generated with smaller α (larger α), i.e. high impulsiveness (low impulsiveness), and larger $|\beta|$ (smaller absolute β), i.e. β heavily skewed either towards right or left (β not skewed). These observations related to FLOAC of α-stable noise signal X, in Ahmed and Savaci (2018) and Ahmed and Savaci (2019), have helped to optimize the detection process of synchronized RCSs Ahmed and Savaci (2018b).

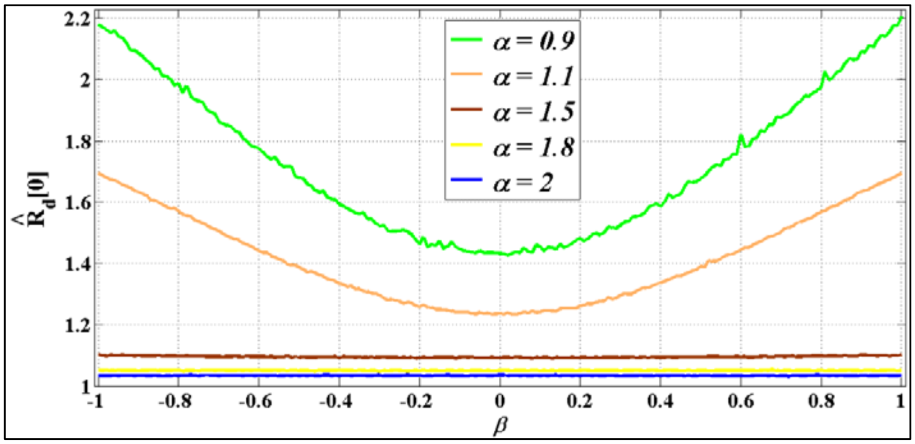


Figure 5.8. Non-delayed FLOAC '$\widehat{R}_d[0]$ or $\widehat{R}_{XX}[0]$' of X ~ $S_{0.7\le\alpha\le2}$ (-1≤β ≤1, γ = 1, μ=0); for different α's

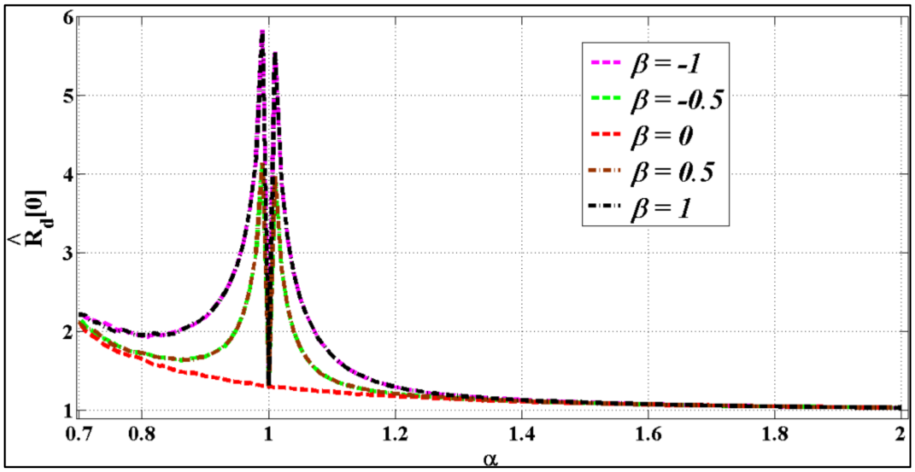


Figure 5.9. Non-delayed FLOAC '$\widehat{R}_d[0]$ or $\widehat{R}_{XX}[0]$' of X ~ $S_{0.7\le\alpha\le2}$ (-1≤β ≤1, γ = 1, μ=0); for different β's

5.4.3.2. Compiled library of FLOAC matrix

Since, it has been observed in Figure 5.6-5.9 that every different value of α and β results in a different and unique value of $\hat{R}_d[0]$, therefore, they can be referred as $\hat{R}_d[0]_{\alpha\beta}$ or $\hat{R}_{XX}[0]_{\alpha\beta}$. By utilizing all possible combinations of α and β, a complete compiled library of $\hat{R}_d[0]_{\alpha\beta}$ has been developed in the form of FLOAC matrix denoted by '**F**' which is defined below as

$$\mathbf{F} \triangleq \begin{array}{c|c} & \boldsymbol{\beta_1} \quad \cdots \quad \boldsymbol{\beta_v} \\ \hline \begin{matrix}\boldsymbol{\alpha_1}\\ \vdots \\ \boldsymbol{\alpha_u}\end{matrix} & \begin{bmatrix} a_{11} & \cdots & a_{1v} \\ \vdots & \ddots & \vdots \\ a_{u1} & \cdots & a_{uv}\end{bmatrix} \\ & \qquad\qquad u \times v \end{array} \tag{77}$$

for

$$a_{ij} \triangleq R_d[0]_{\alpha_i\beta_j} \tag{78}$$

where

$$\alpha_i \triangleq i \cdot \Delta\alpha \tag{79}$$

for $i = 1, 2, \dots \dots, u$ and

$$\Delta\alpha \triangleq \frac{2}{u} \tag{80}$$

Similarly

$$\beta_j \triangleq \{(j-1) \cdot \Delta\beta\} - 1 \tag{81}$$

for $j = 1, 2, \dots \dots, v$ and

$$\Delta\beta \triangleq \frac{2}{v-1} \tag{82}$$

The complexity and accuracy of the proposed FLOAC matrix '**F**' is directly proportional to its dimensions, i.e. the chosen values of u and *v.* In this section, the **F** generated from u=*20* and *v=21* has been utilized.

5.4.3.3. Considered Transmitter and Channel

The generalized system model of α-stable noise based RCSs have been considered to evaluate the performance of the proposed blind recognition method for α-stable random carrier signals. The model includes random carrier signal recognizer (RCSR) and its sub-parts, i.e. FLOACB, TCB and RCSRI; where the considered transmitter and the channel have been explained first.

The generalized α-stable noise signal generator has been used as a transmitter where different values of the impulsiveness parameter 'α' and the skewness parameter 'β' can be used to generate α-stable carrier signals which contain covertly conveyed binary information. The transmitter sends α-stable random noise signals $X_m$where the utilized pulse length '*N*', i.e. number of noise samples representing one binary information bit, contains *N*=2000 samples $\{x_{11},\ x_{12}\ \dots\ ,\ x_{1N}\}$. The pulse length *N* is assumed to be pre-known only to the transmitter and to the intended receiver in RCSs. Since, it has been shown in Ahmed and Savaci (2017b) that if an eavesdropper is aware of the exact pulse length then it is possible to detect and recognize α-stable carrier signals in the AWGN channel as well as extract the underlying hidden binary information by one of the signal recognition techniques proposed in Ma and Nikias (1996), Tsihrintzis and Nikias (1996), Kuruoğlu (2001) and Kannan and Ravishanker (2007). However, there is no method available which can perform blind recognition, i.e. detection, recognition and extraction, of α-stable carrier if the pulse length is not known.

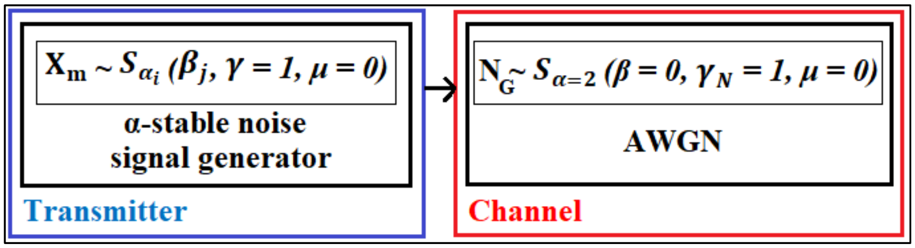

$X_m \sim S_{\alpha_i}(\beta_j, \gamma = 1, \mu = 0)$
α-stable noise
signal generator
Transmitter
$N_G \sim S_{\alpha=2}(\beta = 0, \gamma_N = 1, \mu = 0)$
AWGN
Channel

Figure 5.10. System model of the considered transmitter and the channel

The additive white Gaussian noise has been considered as the channel noise 'N_G' which can be defined

$$N_G \sim S_{\alpha=2}(\beta = 0, \gamma_N = 1, \mu = 0) \tag{83}$$

5.4.3.4. Random Carrier Signal Recognizer

The proposed RCSR requires no a priori knowledge of the α-stable random carrier signals utilized by the transmitter and the intended receiver for covert transmission. The RCSR consists of FLOACB, TCB and RCSRI. The α-stable random carrier signals are detected by the combined efforts of FLOACB and TCB. The RCSRI recognizes the impulsiveness and the skewness parameters by utilizing the introduced compiled library of non-delayed FLOAC values, i.e. FLOAC matrix F in (77), followed by extracting the hidden binary information by using the proposed hard decision rule.

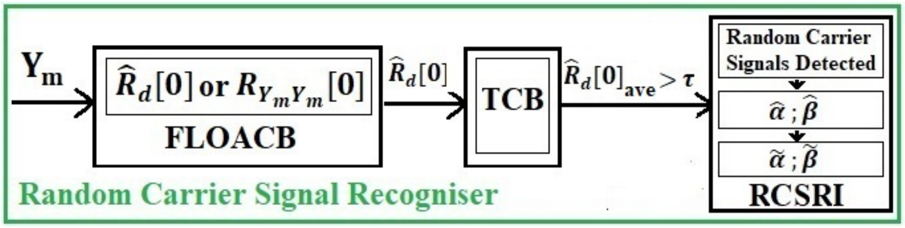

Y_m
$\hat{R}_d[0]$ or $R_{Y_mY_m}[0]$
FLOACB
$\hat{R}_d[0]$
TCB
$\hat{R}_d[0]_{ave} > \tau$
Random Carrier
Signals Detected
$\hat{\alpha}$; $\hat{\beta}$
$\tilde{\alpha}$; $\tilde{\beta}$
RCSRI
Random Carrier Signal Recogniser

Figure 5.11. Block Diagram of the RCSR

FLOAC matrix F in (77), followed by extracting the hidden binary information by using the proposed hard decision rule.

The RCSR receives the sequence '$\mathrm{Y_m}$' as

$$\mathrm{Y_m} = \begin{cases} \mathrm{X_m} + \mathrm{N_G}, if\ random\ carrier\ signals\ are\ present \\ \mathrm{N_G} \qquad , if\ random\ carrier\ signals\ are\ absent \end{cases} \tag{84}$$

where $\mathrm{Y_m}$ is the mixture of α-stable random carrier signals with the additive white Gaussian noise '$\mathrm{N_G}$' (AWGN) in the channel, if there is presence of information bearing α-stable random carrier signals in the channel at that specific time instant, otherwise $\mathrm{Y_m}$ is only $\mathrm{N_G}$ in the channel.

An outline of the proposed method has also been explained in the form of process flow graph in Figure 5.10. It illustrates all the steps, beginning from the time instant of process initialization, which are related to α-stable random carrier signals detection, recognition and extraction steps carried out by FLOACB, TCB and RCSRI.

Fractional lower-order auto-covariance block (FLOACB):

Some part of the first step, i.e. detection by an eavesdropper, has been performed by the proposed FLOACB. The FLOACB starts computing the estimated $\hat{R}_d[0]$ or $\hat{R}_{Y_m Y_m}[0]$ exactly after accepting $\mathrm{N_a}$ samples from the time instant of initialization, i.e. receiving the first sample of $\mathrm{Y_m}$, and this process is then repeated after every T_s duration, i.e. duration between the consecutive samples of $\mathrm{Y_m}$; where $\mathrm{N_a}$ is the assumed pulse length assumed by an eavesdropper to extract single binary information bit whereas N is the actual pulse length utilized by both the transmitter and the intended receiver. All the methods introduced in the literature whether related to the recognition of α-stable random carrier signals Ma and Nikias (1996), Tsihrintzis and Nikias (1996) and Kuruoğlu (2001) or to the RCSs in Cek and Savaci (2009), Cek (2015), Cek (2015b), Xu et al. (2016), Xu et al. (2017), Ahmed and Savaci (2017), Ahmed and Savaci (2017b) and Ahmed and Savaci (2018) has utilized pulse length greater than 500 as it is difficult to utilize pulse length 'N' less than 500 if accurate estimation of the involved α or β is required. However, the eavesdropper has assumed $\mathrm{N_a}$ being equals to 100, 200 and 300 as the proposed method does not need accurate estimation of α and β, it rather depends on the computed intervals of these associated parameters which can be found by utilizing the proposed hard decision rule given in the sequel.

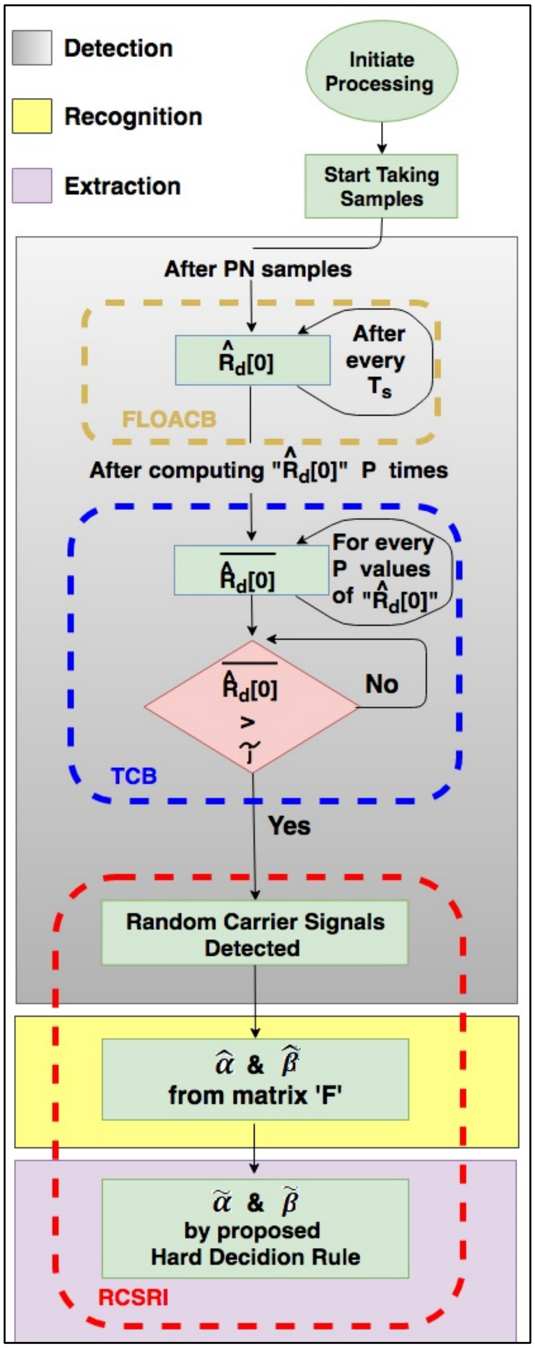

Detection
Recognition
Extraction
Initiate Processing
Start Taking Samples
After PN samples
$\hat{R}_d[0]$
After every T_s
FLOACB
After computing "$\hat{R}_d[0]$" P times
$\overline{\hat{R}_d[0]}$
For every P values of "$\hat{R}_d[0]$"
$\overline{\hat{R}_d[0]}$ > $\tilde{\Upsilon}$
No
TCB
Yes
Random Carrier Signals Detected
$\hat{\alpha}$ & $\hat{\beta}$ from matrix 'F'
$\tilde{\alpha}$ & $\tilde{\beta}$ by proposed Hard Decidion Rule
RCSRI

Figure 5.12. Process flow diagram of the RCSR

Threshold Control Block (TCB):

The remaining part of the first step, i.e. detection by an eavesdropper, has been performed by the proposed TCB. Since, the FLOACB starts sending consecutive $\hat{R}_d[0]$ values to TCB exactly after accepting N_a samples from the time instant of initialization, therefore, the TCB also starts computing the average non-delayed FLOAC value, i.e. $\hat{R}_d[0]_{ave}$, according to the criterion defined below

$$\hat{R}_d[0]_{ave} \ = \frac{1}{N_a} \sum_{i=1}^{N_a} \hat{R}_d[0]\,(i) \tag{85}$$

where $\hat{R}_d[0](i)$ is the ith $\hat{R}_d[0]$ value sent by the FLOACB to TCB and N_a is arbitrarily chosen value of the unknown pulse length. The process of computing $\hat{R}_d[0]_{ave}$is continuously repeated for every new N_a values of $\hat{R}_d[0]$ received by the TCB.

Random carrier signal recognition indicator (RCSRI):

If for pre-selected threshold 'τ', $\hat{R}_d[0]_{ave} \ > \tau$ is achieved at some time instant, then the information bearing α-stable carrier signals are considered as detected and the Y_m are forwarded to RCSRI for the remaining steps, i.e. recognition and extraction by an eavesdropper; where τ can be chosen as any a_{ij}= $R_d[0]_{\alpha_i\beta_j}$from the pre-known compiled library of non-delayed FLOAC values, i.e. FLOAC matrix 'F', in order to detect specifically those transmitted α-stable carrier signals which have been generated by utilizing $\alpha(0 < \alpha < \alpha_i)$ and β $(-1 \leq \beta_j \ < \ j)$ or $(\beta_j \ \leq j \leq 1)$. The threshold $\tau = 1.1$ has been chosen from the F which has been used throughout this section as the targeted α-stable carrier signals are those which have been generated by utilizing α $(0 < \alpha < 1.5)$ and $\beta(-1 \leq \beta \leq 1)$.

Computing the Characteristic exponent ($\hat{\alpha}$) and the Impulsiveness parameter ($\hat{\beta}$):

In the second step, i.e. recognition by an eavesdropper has been performed by the RCSRI. It first compares the value $\hat{R}_d[0]_{ave} > \tau$ with all the elements of the FLOAC matrix '**F**' and selects the closest one. For example $a_{34} \ = R_d[0]_{\alpha_3\beta_4}$ enables the RCSRI to declare $\hat{\alpha}$ as α_3 and $\hat{\beta}$ as β_4 from the associated element a_{34} of F according to (77).

Computing the interval of Characteristic exponent ($\hat{\alpha}$) and Impulsiveness parameter ($\hat{\beta}$):

In RCSs Kannan and Ravishanker (2007), Casarin (2004), Diego et al. (2009) [13-20, 23], Cek and Savaci (2009), Cek (2015), Cek (2015b), Xu et al. (2016), Xu et al (2017) and Ahmed and Savaci (2018), binary shift keying is performed by transmitting two different α-stable noise carrier signals by either modulating the impulsiveness parameter 'α', i.e. $X_1 \sim S_{\alpha_1}$ *(β, γ, μ)* as '0' and $X_2 \sim S_{\alpha_2}$ *(β, γ, μ)* as '1', or by modulating the skewness parameter 'β', i.e. $X_1 \sim S_\alpha$ *(β_1, γ, μ)* as '0' and $X_2 \sim S_\alpha$ *(β_2, γ, μ)* as '1' where $\beta_2 = -\beta_1$. The difference $\Delta\alpha$, i.e. α_2- α_1, in symmetric α-stable (SαS) noise based RCS and $\Delta\beta$, i.e. $\beta_2 - (\beta_1)$, in skewed α-stable (SkαS) noise based RCS are always kept large to minimize the error in the extraction of binary information bits '0' and '1' at the intended receiver side as the extraction strictly depends upon the accurate estimation of $\hat{\alpha}_1$, $\hat{\alpha}_2$ or $\hat{\beta}_1$, $\hat{\beta}_2$. Since, instead of exact estimation, the proposed method selects $\hat{\alpha}$ and $\hat{\beta}$from **F**, therefore, a separate hard decision rule is also proposed to determine the interval of the selected $\hat{\alpha}$ and $\hat{\beta}$ which are referred as I_α and I_β which are computed according to the criteria defined as

$$I_\alpha = \begin{cases} I_\alpha \geq \hat{\alpha}; & if\ \hat{\alpha} \geq \alpha_\tau \\ I_\alpha \leq \hat{\alpha}; & if\ \hat{\alpha} < \alpha_\tau \end{cases} \tag{86}$$

$$I_\beta = \begin{cases} I_\beta > \beta_\tau; & if\ \hat{\beta} > \beta_\tau \\ I_\beta \leq \beta_\tau; & if\ \hat{\beta} \leq \beta_\tau \end{cases} \tag{87}$$

where fixed thresholds $\alpha_\tau(\alpha_1 < \alpha_\tau < \alpha_2)$ and $\beta_\tau(\beta_1 \leq \beta_\tau \leq \beta_2)$are used to take hard decision for retrieving binary information bits '0' and '1' as a third step, i.e. extraction by an eavesdropper. The thresholds $\alpha_\tau = 1$ and $\beta_\tau = 0$ has been used throughout this section.

5.4.4. Simulation Results

The proposed blind recognition method has been tested on twelve different types of α-stable carrier signals which have been generated from the possible combination of chosen three different impulsiveness parameters, i.e. α =0.7, 1.1 and 1.5, and four skewness parameters, i.e. β = -1, 0.7, -0.7, 1. To label the intensity of the α-stable carrier signals, i.e. X ~ S_α *(β, γ = 0.5, μ)* contaminated by the AWGN, i.e. N ~ $S_{\alpha=2}$ *(β = 0, γ_N = 1, μ = 0)*, mixed signal to noise ratio (MSNR) defined in Kuruoğlu (2001) equals to -3dB has been used where the location parameter μ has been kept to 0. Since γ = *0.5* and μ = *0* has been used throughout to generate X therefore the notation

X ~ S_α *(β)* has been used in Figure 5.13, 5.14 and 5.15 for clarity.

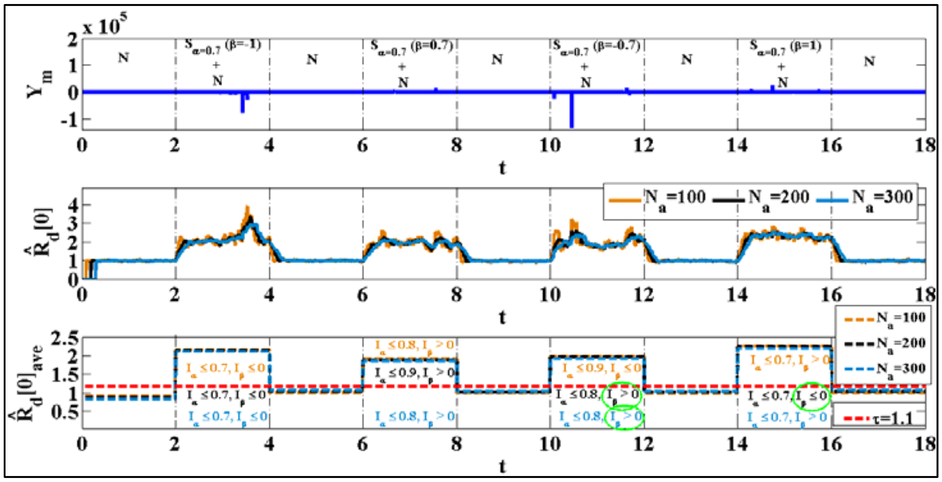


Figure 5.13. Blind recognition of $S_{=0.7}$ (β = -1), $S_{\alpha=0.7}$ (β = 0.7), $S_{\alpha=0.7}$ (β = -0.7) and $S_{\alpha=0.7}$ (β = 1) with different 'N_a'; where τ = 1.1.

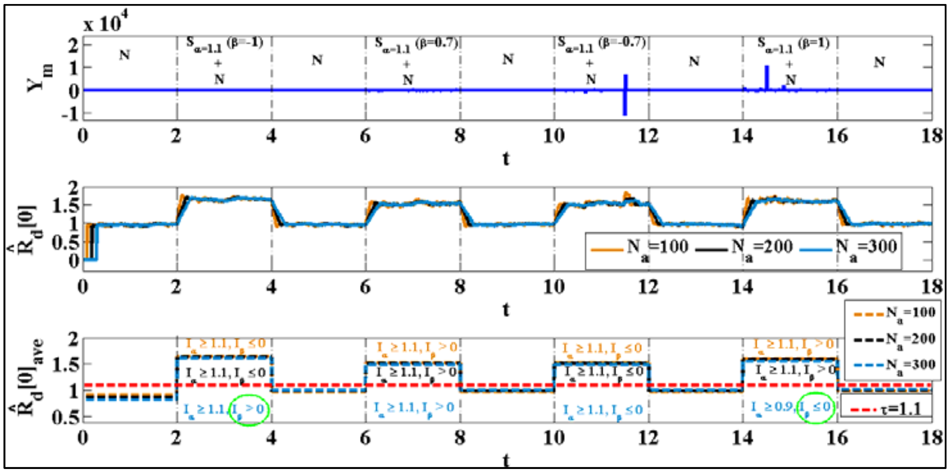


Figure 5.14. Blind recognition of $S_{=1.1}$ (β = -1), $S_{\alpha=1.1}$ (β = 0.7), $S_{\alpha=1.1}$ (β = -0.7) and $S_{\alpha=1.1}$ (β = 1) with different 'N_a'; where τ = 1.1

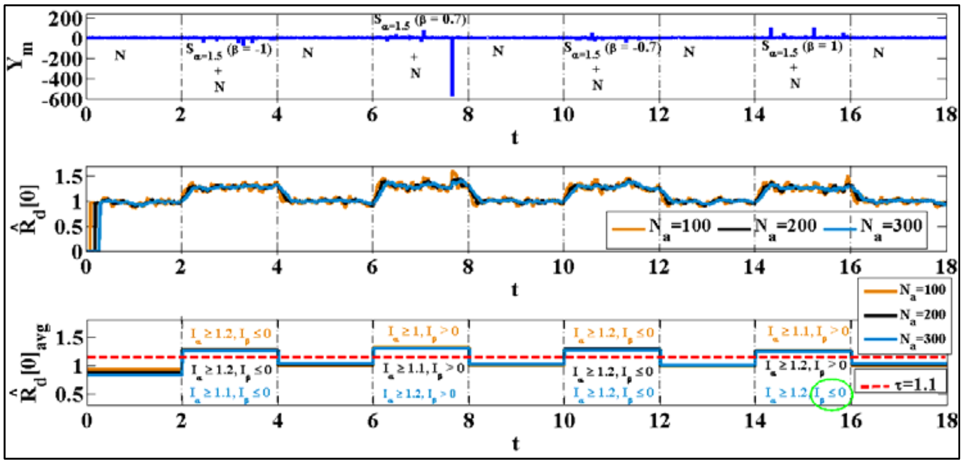


Figure 5.15. Blind recognition of $S_{=1.5}$ (β = -1), $S_{\alpha=1.5}$ (β = 0.7), $S_{\alpha=1.5}$ (β = -0.7) and $S_{\alpha=1.5}$ (β = 1) with different 'N_a'; where τ = 1.1

In Figure 5.13, the received sequence Y_m contains AWGN 'N_G' alone as well as N_G added with four different types of α-stable carrier signals, i.e. $S_{\alpha=0.7}$ *(β = -1)*, $S_{\alpha=0.7}$ *(β = 0.7)*, $S_{\alpha=0.7}$ *(β = -0.7)* and $S_{\alpha=0.7}$ *(β = 1)*. The α-stable carrier signals have been generated by utilizing the same impulsiveness parameter, i.e. α = 0.7*,* in combination with four different skewness parameters, i.e. β = -1, 0.7, -0.7, 1. It can be seen that the whole received sequence Y_m looks like AWGN in the real time which reminds the capability of α-stable carrier signals to become invisible in AWGN channel. As the presence or absence of the information carrying α-stable carrier signals in the received signal 'Y_m' is a priori unknown, therefore the blind recognition can be considered impossible.

However, as it is shown in Figure 5.13 that the computed $\hat{R}_d[0]$ according to the proposed method confirms the presence of α-stable carrier signals in Y_m. Moreover, the intervals of the present α-stable carrier signals have also been correctly detected in real time. The accuracy of the detection is more or less the same for the three utilised values of N_a. Similarly, the computed $\hat{R}_d[0]_{ave}$ has provided an enhanced view of the detected α-stable carrier signals in Y_m. It should be noted that the computed $\hat{R}_d[0]_{ave}$ during the interval of detected $S_{\alpha=0.7}$ *(β = -1)* and $S_{\alpha=0.7}$ *(β = 1)* is higher than the $S_{\alpha=0.7}$ *(β = 0.7)* and $S_{\alpha=0.7}$ *(β = -0.7)* which follows the pattern obtained in Figure 5.6, 5.7, 5.8 and 5.9. The determined intervals of I_α and I_β have also been shown in Figure 5.13, 5.14 and 5.15 where all the I_α have been correctly determined which proves the capability of the proposed method to extract the binary information in SαS noise based RCSs by utilising any value of N_a. However, three I_β out of twelve, highlighted in green ellipse in Figure 5.13, are found as incorrect, therefore extraction of the binary information in SkαS noise based RCSs can be carried out by utilising lesser value of N_a, i.e. $N_a = 100$.

The result for the received sequence Y_m containing α-stable carrier signals, i.e. $S_{\alpha=1.1}$ *(β = -1),* $S_{\alpha=1.1}$ *(β = 0.7),* $S_{\alpha=1.1}$ *(β = -0.7)* and $S_{\alpha=1.1}$ *(β = 1)*, generated with higher α, i.e. $\alpha = 1.1$, and previously used β have been shown in Figure 5.14. Similarly, Y_m containing α-stable carrier signals generated with much higher α, i.e. $\alpha = 1.5$, and previously used β, i.e. $S_{\alpha=1.5}$ *(β = -1),* $S_{\alpha=1.5}$ *(β = 0.7),* $S_{\alpha=1.5}$ *(β = -0.7)* and $S_{\alpha=1.5}$*(β = 1)* have been shown in Figure 5.15. It can be seen that all the I_α in Figure 5.14 and 5.15 have also been correctly determined where the error in I_β have been reduced to one when the transmitted α-stable carrier signals are generated with $\alpha = 1.5$. It has to be considered that the above results are obtained by utilizing F generated from *u=20* and *v=21*; where much better results are expected if much higher order F have been used by choosing values of u and v.

5.4.5. Prescribed Covertness Range

It can be seen in Figure 5.13-5.15 that there is a difference in the value of $\hat{R}_d[0]_{ave}$ during the presence of α-stable carrier signals in comparison to the value of $\hat{R}_d[0]_{ave}$ during the absence of α-stable carrier signals. This difference enables the RCSR to differentiate between information carrying α-stable carrier signals and the AWGN noise. However, this difference, which is due to the difference between the members of F, i.e. $a_{ij} = R_d[0]_{\alpha_i\beta_j}$, in (77), starts to decrease when α of the transmitted α-stable carrier signals starts to increase and vice versa. Moreover, this difference starts to decrease drastically for $\alpha > 1.5$; hence detection of α-stable carrier signals, generated with $\alpha > 1.5$, is extremely difficult. This is the reason that the threshold 'τ' equals to 1.1 from Table 1, which correspond to $R_d[0]_{\alpha=1.5,\ -1\leq\beta\leq1}$ has been chosen to perform the blind recognition of those α-stable carrier signals which have generated with $\alpha \leq 1.5$ and $-1 \leq \beta \leq 1$.

Therefore, in order to establish secure communication by employing RCSs with $\alpha > 1.5$ and the lesser absolute β should be utilized while generating α-stable carrier signals. These intervals for α and β can be said as covertness range for α-stable noise based RCSs; where choosing α and β under this range will ensure cover transmission by employing RCSs. However, the further investigations should be done to optimize the proposed method to blindly recognize α-stable carrier signals in the covertness range as well.

5.4.6. Counter Measures Guidelines

A three-step procedure for the blind recognition of α-stable random carrier signals has been introduced for the first time. The proposed method has been analyzed from the perspective of an eavesdropper who has no a priori knowledge of the utilized α-stable carrier signals. It is concluded from the simulations that the RCSs utilizing α-stable carrier signals generated with smaller α (highly impulsive) and larger absolute β (heavily skewed towards right or left) are prone to the proposed method. The only way to perform secure transmission, by utilizing α-stable noise based RCSs, is to use the related parameters of the α-stable carrier signals, i.e. α and β, according to the proposed covertness range given in the results.

5.5. Random Communication System based on Alpha-Stable noise driven Inverse System

Following the counter measures proposed in the last section to strengthen α-stable noise based RCS; an inverse system approach has been adopted to propose a more protected RCS. In the proposed random communication system, the α-stable noise as a random carrier drives the transmitter which is modeled by the linear dynamical system and the skewness parameter of the random carrier encodes the binary messages. By selecting the receiver as the inverse system of the transmitter, the output of the receiver is ensured to be α-stable noise whose skewness parameters are then estimated to decode the binary messages. The response of a linear system to an α-stable process is again α-stable process, however, the skewness parameters of the response differs from that of the input which can only be recovered at the output of the inverse system. Hence, estimation of skewness parameter by an eavesdropper, without using the inverse system, will not reveal the true binary messages while the intended receiver truly decodes the binary messages. The improvement in security is shown by comparing the bit error rate performances of the intended receiver and an eavesdropper. Additionally, the proposed inverse system based RCS has shown greater covertness values on the proposed covertness scale, introduced in previous section, than previously proposed SRCS and optimized model of RCSs.

5.5.1. Motivation and Background

Physical layer security of digital communication systems is considered as a key factor in ensuring covert transmission. Attempts to use SkαS distributed noise as a random carrier or building skewed α-stable distributed noise based communication systems, i.e. RCSs, to achieve the required purpose began in 2015 Cek (2015). Different receivers have also been utilized to enhance the performance of RCSs Xu et al. (2015). However, the most optimized model of the RCS based on SkαS-NSK has been introduced recently in Ahmed and Savaci (2017). In RCSs, decoding the received signal is impossible without knowing the pulse length, i.e. duration of a single binary information bit. However, if the exact pulse length can be found then it would be possible for an eavesdropper to retrieve the binary messages hidden in the transmitted α-stable noise signals by one of the estimation methods given in Kuruoğlu (2001). Therefore, the true level of covertness cannot be assured in the previously proposed RCSs in Cek (2015), Xu et al. (2015) and Ahmed and Savaci (2017).

5.5.2. System Description

In this section, the newly developed RCS, as shown in Figure 5.16, includes the mth-order LTI dynamical system with Sk-αSNSK signal generator (SG) at the transmitting end ‘Alice’ while the intended receiver ‘Bob’ uses the inverse LTI dynamical system of the transmitter with the MEVM based estimator. As a result, the parameters needed to decode the information carrying α-stable input has been increased from single parameter, i.e. pulse length, to the state parameters of the utilized LTI dynamical system as well. The BER performances of Bob and an eavesdropper ‘Willie’ reflects that Willie is unable to retrieve the hidden binary messages even if he knows the pulse length, as he is not aware of the state parameters of the LTI system used by Alice. In comparison to Willie, Bob is achieving more efficient BER performance as expected from any covert communication system.

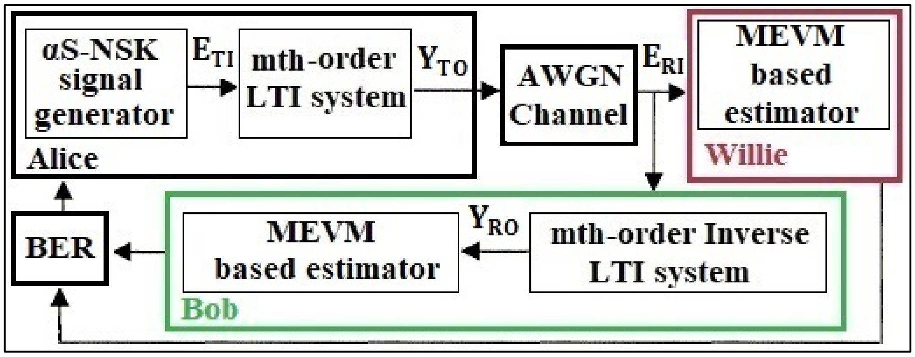


Figure 5.16. Block diagram of the proposed RCS based on the inverse system

The inspiration to use linear inverse dynamical system in the context of RCS has come through the steps: i) the analytical results obtained in Grigoriu (1995) says that the skewness parameter of the output of LTI system changes in terms of the transfer function of the LTI system and the skewness and scale parameters of α-stable random input; ii) hence, at the transmitter’s output, the skewness parameter of the transmitter’s input cannot be decoded, therefore estimating the skewness parameter of the transmitter’s input is only possible at the corresponding inverse system’s output. In the sequel, α-stable noise is briefly introduced and then the transmitter and the receiver shown in Figure 5.16 are presented.

5.5.2.1. Linear Time Invariant System based Transmitter

Alice: The transmitter consists of Sk-αSNSK SG and a second-order LTI system. The Sk-αSNSK SG generates random noises E_{TI_1}, i.e. E_{TI_1} ~ S_α (-β_{TI}, γ_{TI}, μ), and E_{TI_2}, i.e. E_{TI_2} ~ S_α (β_{TI}, γ_{TI}, μ) to encode the binary messages '0' and '1', respectively, by exploiting the antipodal characteristics of skewed α-stable distribution; where β_{TI} equals to 1 or -1 have been used to represent the distribution skewed to the right or to the left, respectively. The duration needed to encode a single binary message bit is T_bN, i.e. the pulse length; where T_b is the length of a single noise sample and N is the number of generated noise samples to encode a single binary message bit represented as $\{e_{TI_1,}e_{TI_2}, \ldots., e_{TI_N}\}$.

The signals generated from the Skα-SNSK SG are then applied to the transmitter which is mth-order LTI dynamical system containing m state variables, p inputs and q outputs, represented as $\mathscr{R}$ = [A B C D] in Kailath (1980); where A∈ $R^{m\times m}$, B∈ $R^{m\times p}$, C∈ $R^{q\times m}$ and D ∈ $R^{p\times q}$. In the proposed RCS, we have chosen the representation A = $\begin{bmatrix} 0.98 & -0.01 \\ -0.01 & 0.98 \end{bmatrix}$, B= $\begin{bmatrix} -0.06 \\ 2.19 \end{bmatrix}$, C = $[0 \quad -0.16]$, and D = $[-0.33]$ which yielded the best BER performance for the intended receiver among the many arbitrary selected system representations $\mathscr{R}$s and their corresponding inverse systems. As it is proven in Grigoriu (1995) that the output of $\mathscr{R}$ = [A B C D] to an α-stable input is also α-stable, i.e. the input E_{TI} ~ S_α (β_{TI}, γ_{TI}, μ) results in the output Y_{TO} ~ S_α (β_{TO},γ_{TO}, μ); where E_{TI} and Y_{TO} represent the input and output of the transmitter $\mathscr{R}$, respectively. However, the fact that $\beta_{TI} \neq \beta_{TO}$, as proven in Grigoriu (1995), assures that the binary messages encoded by the skewness parameter of the input could not be truly estimated by an eavesdropper even if he is perfectly synchronized with the transmitter and knows the pulse length as well.

The arbitrary binary message stream consisting of five binary information bits with the corresponding generated α-stable noise sequence E_{TI} consisting of E_{TI_1}, E_{TI_2},..., E_{TI_5} and the transmitted α-stable noise sequence Y_{TO} are shown in Figure 5.17; where α = 1.5, β_{TI} = 1, γ_{TI} = 1 and μ = 0 are used to generate E_{TI}.

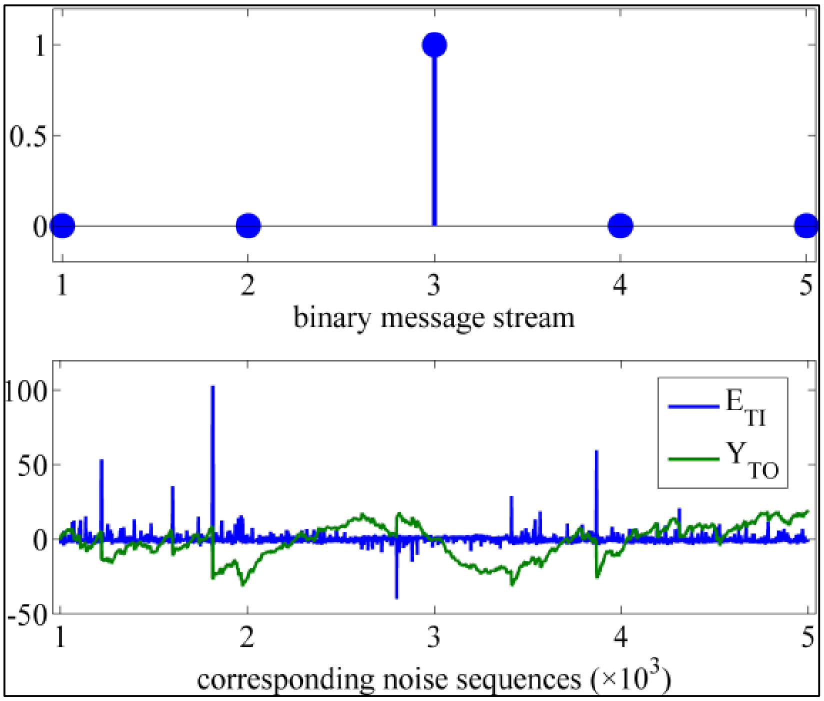


Figure 5.17. Binary messages by Alice (Upper), generated and transmitted noise sequences by Alice in time domain (Lower); T_b=1, N = 1000, T_bN=1×10^3

5.5.2.2. Corresponding Inverse Systems based Receiver

Bob and Willie: The α-stable noise sequence at the input of the receiver is E_{RI} = Y_{TO} + G, which is accessible to Bob and also to Willie; where the additive white gaussian noise in the channel is G ~ $S_{\alpha_G=2}(\beta=0, \gamma_G=1, \mu=0)$. Since, Bob is aware of the transmitter '$\mathcal{R}$' he can design his receiver as the inverse system of $\mathcal{R}$ as given in Kailath (1980), i.e. $\mathcal{R}_I = [A - BD^{-1}C \quad BD^{-1} \quad -D^{-1}C \quad D^{-1}]$. By applying the received sequence E_{RI} to his receiver $\mathcal{R}_I$, Bob can estimate the skewness parameter $\hat{\beta}_{TI}$ from his output Y_{RO} by subdividing the received data $\{y_{RO_1}, y_{RO_2}, \ldots, y_{RO_N}\}$ holding a single binary message bit, consisting of N samples during the pulse length T_bN, into L=25 non-overlapping segments of length K=40 *(i.e.* $K = N/L$*)*. The logarithms of the maximum and minimum samples from each segment l =*1,2,* .... , L from total L segments are calculated and represented below by Y_{l-max} and Y_{l-min} as

$$Y_{l-max} \;= log\,\{max\big(y_{RO_{lK-K+i}}\big|\, i \in 1,2,\dots,K)\} \qquad (86)$$

$$Y_{l-min} \;= log\,\{-min\big(y_{RO_{lK-K+i}}\big|\, i \in 1,2,\dots,K)\} \qquad (87)$$

The means, i.e. Y_{max} & Y_{min}, and corresponding variances, i.e. s_{max}^{2} & s_{min}^{2}, of the received data are then computed which is followed by an estimate for β_{TI}, i.e. $\hat{\beta}_{TI}$, to decode a single binary message bit as '0' ('1') if $\hat{\beta}_{TI} < 0$ ($\hat{\beta}_{TI} \geq 0$).

$$Y_{max} = \frac{1}{L}\sum_{l=1}^{L} Y_{l-max} \;;\; s_{max}^{2} = \frac{1}{L-1}\sum_{l=1}^{L}(Y_{l-max} - Y_{\max})^{2} \qquad (88)$$

$$Y_{min} = \frac{1}{L}\sum_{l=1}^{L} Y_{l-min} \;;\; s_{min}^{2} = \frac{1}{L-1}\sum_{l=1}^{L}(Y_{l-min} - Y_{\min})^{2} \qquad (89)$$

$$\hat{\beta}_{TI} = 1 - \frac{2}{\exp\,(\hat{\alpha}(S_{max} - S_{\min}))} \quad \text{where} \quad \hat{\alpha} = \frac{\pi}{2\sqrt{6}}\Big(\frac{1}{Y_{max}} + \frac{1}{Y_{min}}\Big) \qquad (90)$$

Even though there is not any method, algorithm or attack to crack the hidden pulse length, i.e. T_bN, of $\mathrm{E_{RI}}$ or $\mathrm{Y_{RO}}$ but, considering the worst case scenario, we have assumed that both Bob and Willie know T_b and N. Therefore, Willie could also utilise the same MEVM based estimator, explained above in (1-5), to retrieve the binary message stream by estimating $\hat{\beta}_{TI}$ but from the data $\{e_{RI_1,} e_{RI_2}, \dots, e_{RI_N}\}$ of the received signal $\mathrm{E_{RI}}$ while Bob is estimating from $\mathrm{Y_{RO}}$. The received noise sequences $\mathrm{E_{RI}}$ and $\mathrm{Y_{RO}}$, respectively, utilized by Bob and Willie with their retrieved binary message streams and the corresponding estimated skewness parameters, have been shown in Figure 5.18.

5.5.3. BER Performance Evaluation

It has been shown in Figure 5.18, that the transmitted binary message stream is irretrievable from the $\hat{\beta}_{TI}$ estimated by an eavesdropper. However, in order to accurately evaluate the proposed RCS, the BER performances of Bob and Willie have also been computed against the channel MSNR; where $\mathrm{MSNR}_{dB} = 10\log\frac{\gamma_{TI}}{\gamma_G}$ in Kuruoğlu (2001).

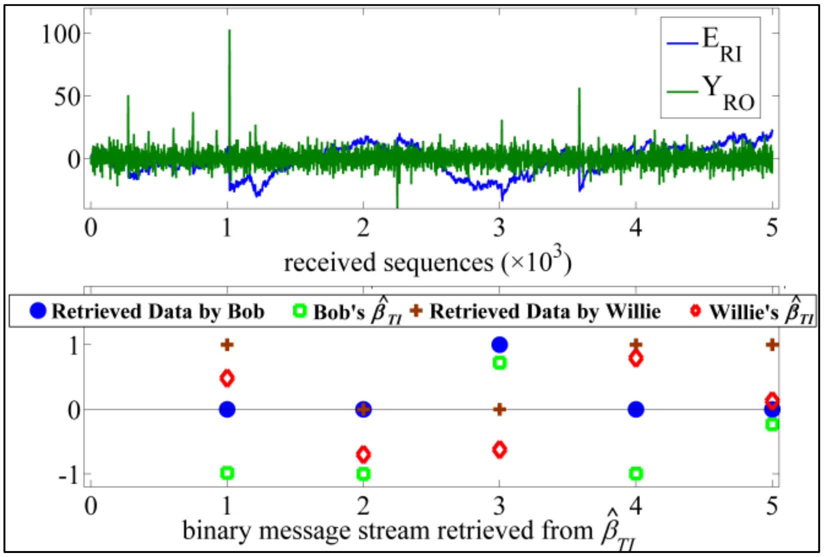


Figure 5.18. Received signals from AWGN Channel in time domain (Upper),estimated skewness parameters and retrieved binary messages by Bob and Willie (Lower); T_b=1, N = 1000, T_bN=1×10^3

According to the BER performances of Bob and Willie, for the chosen L and K, one can conclude that the intended receiver will always outperform an eavesdropper by a large BER margin, for the same value of the impulsiveness parameter ‘α’ utilized by Alice. The BER performance degrades for higher values of α while it gets closer to that of the Gaussian noise, i.e. $\alpha_G = 2$, present in the channel and vice versa. Moreover, as shown in Figure 5.19, much more efficient performance is expected when the greater values of L are utilized.

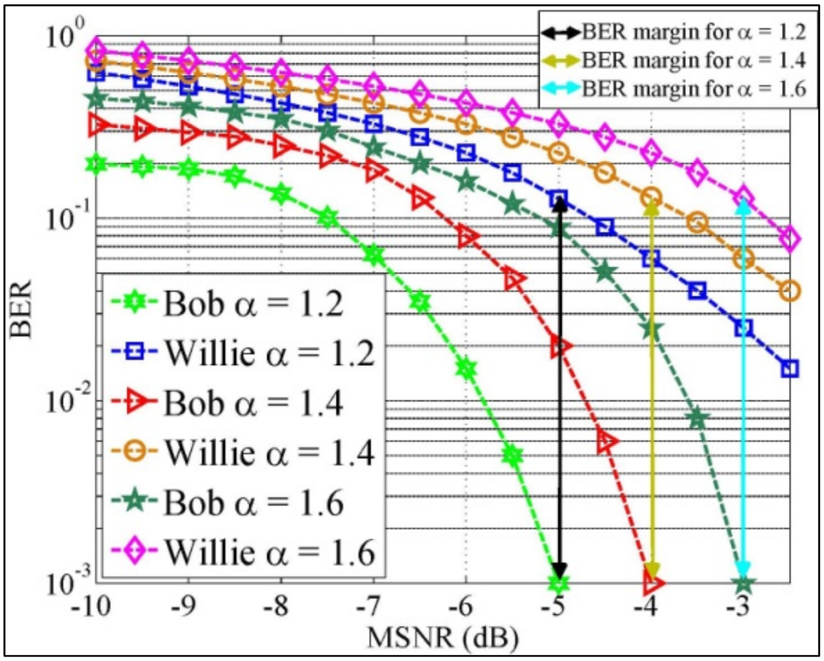


Figure 5.19. BER vs. MSNR (dB) performances of Bob and Willie for the different characteristic exponents utilized by Alice; number of transmitted bits=1000

5.5.4. Covertness Analysis

In comparison to the covertness analysis of the optimized model of RCS in Figure 5.4, the performance of an eavesdropper has decreased drastically if the newly proposed inverse system based RCS is used by the transmitter and the intended receiver which can be seen in Figure 5.20. In contrast to the BER performance of an eavesdropper for optimized model of RCS in Figure 5.4, the eavesdropper is not even able to achieve the BER of 10^{-1} in the inverse system based RCS.

Additionally, the covertness value C_v for the newly proposed inverse system based RCS, as shown in Figure 5.2, has increased significantly in contrast to the C_v for optimized model of RCS, as shown in Figure 5.5, which shows the usefulness and benefit of adopting inverse system approach for RCSs.

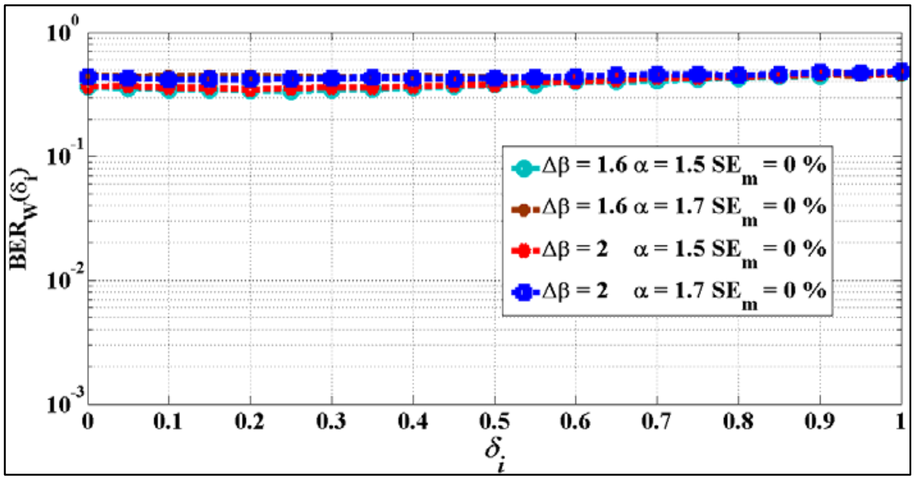


Figure 5.19. Performance of an eavesdropper Willie

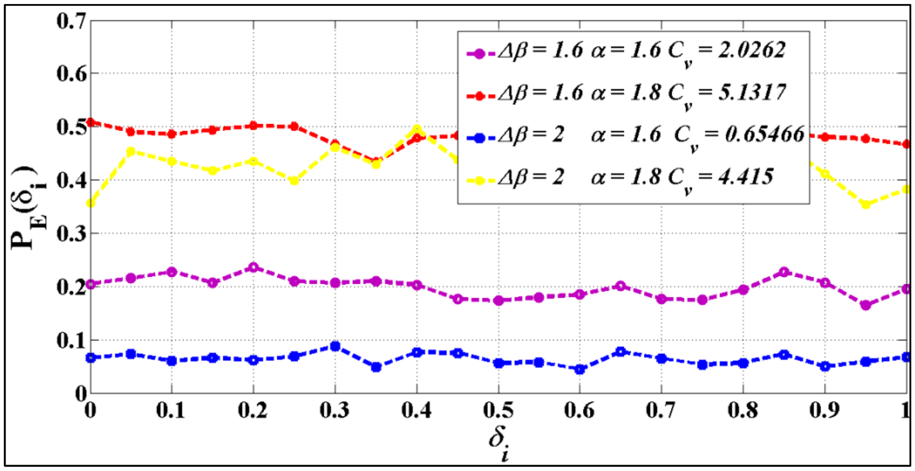


Figure 5.20. Covertness of Alice and Bob's SkαS-NSK based RCS

Conclusive Remarks:

The covertness of the previously proposed RCSs has been built solely on the hidden pulse length which is required for the decoding process, however, the inverse system approach presents the new RCS where the transmitter is a LTI dynamical system driven by α-stable noise which acts as a random carrier and the output of the inverse system of the transmitter is the input to the MEVM estimator for the intended receiver. According to the BER results of Bob and Willie, the intended receiver achieves better performance compare to the previous RCSs and the security complexity has been increased due to the utilization of the inverse system.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1. Conclusion

This thesis presented the research work done to enhance the physical layer security in transmission by employing the unconventional communication systems. For this purpose, firstly, the literature review of the existing conventional communication systems, i.e. spread spectrum communication systems, and unconventional communication systems, i.e. chaotic communication systems, has been carried out which is followed by a brief revision of all the potential security issues and concerns that has been raised previously by the researchers conducting studies on these systems, hence, the authors established the need for an alternate way of communication to achieve the desired level of security at the physical layer. For these reasons, this thesis has proposed α-stable noise carrier based random communication systems as a potential candidate to achieve the required purpose.

The research in this thesis was based on three objectives i) decreasing the computational complexity of RCSs while enhancing the BER performance by introducing better receiver designs and introducing method to establish synchronization in RCSs; ii) proposing criterion for evaluation and quantification of the security and covertness of RCSs and practically testing the security of RCSs in real-time from the perspective of an eavesdropper by introducing any attack for RCSs, consequently, the counter measure guidelines to improve the security from the potential attack should also be suggested; iii) adopting inverse system approach to introduce an α-stable noise driven linear time invariant system based transmitter and its corresponding inverse system based receiver to overcome the security deficiencies highlighted after achieving the previous objectives.

The significance of security in wireless communication systems has been stated at the beginning of the Chapter 1 which is followed by an overview on how the concept of enhancing physical layer security has been evolved from spread spectrum and chaotic communications to α-stable noise based random communication systems. The detailed introduction of α-stable distribution and the related properties has also been included in this chapter. The chapter 2 is divided in to two parts i) conventional communication systems; ii) Unconventional communication systems, where spread spectrum communications and chaotic communications has been covered in detail which also provides the security analysis of these systems. As a result, significant security deficiencies have been found in both spread spectrum and chaotic communication systems, therefore, we have proposed to utilize random communication systems as an alternate way to enhance physical layer security.

Therefore, in Chapter 3, the origin, significance and benefits of random communication systems has been discussed in the initial sections which is followed by the literature review of all the previous investigations related to α-stable noise carrier based random communication systems. Different receiver designs based on different estimators and their corresponding deficiencies has been pointed out which has clearly helped in proposing optimized models for α-stable noise carrier based RCS in order to achieve the first objective in Chapter 4.

In Chapter 4, keeping in mind the previously introduced α-stable noise based random communication systems; new receiver design based on MEVM estimator has been proposed which has clearly outperformed its previous counterparts. The proposed MEVM estimator based receiver has enhanced the BER performance with decreased computational complexity. Moreover, the proposed receiver has also been extended to establish synchronization for the first time in RCSs by exploiting the concept of pilot assisted synchronization where the general behavior of fractional lower-order covariance in AWGN channel has been analyzed and exploited for the required purpose.

In Chapter 5, the first security performance tradeoff characteristics of RCSs have been presented to analyze the security of RCSs with respect to their achieved BER performances. Similarly, measure of covertness has also been introduced to quantify the covertness of RCSs. Both introduced criteria can now be used to compare RCSs which could not be done before. Moreover, it has been found that the proposed optimized model of RCS has performed extremely well on the developed security scale. Similarly, the blind identification attack, introduced in this chapter, would help in discovering the underlying vulnerabilities of different RCSs where the advised covertness range would help in further enhancing the physical layer security of α-stable noise based random communication systems. However, the proposed RCS based on α-stable noise driven inverse systems is assumed to be invulnerable to the blind identification attack as it has outperformed the previously proposed optimized model RCS and it can be considered as the most secure version of α-stable noise carrier based RCS.

6.2. Future Work

A lot of research work related to α-stable noise based random communication systems has been documented in this thesis but still there is always some space for improvement and up-gradation. Therefore, the derived possible future research directions from the work presented in this thesis have been given as follows:

Regarding the potential future research pathways related to the first objective, firstly, the efforts to enhance the BER performance of RCSs would never come to an end and attempts to introduce more better receivers, outperforming the previous one, would continue to be seen in future as well. For this purpose, different estimators could be developed or utilized which will further upgrade the BER performance of RCSs. Secondly, since there is no clear mechanism to quantify or measure the complexity of the utilized estimators in designing the receiver for α-stable noise based RCSs and the complexity of RCSs is being judged by the quantity of equations required to obtain the modulated parameter of α-stable noise at the receiver end, therefore, some accurate and mathematical criterion is needed for this purpose so that RCSs can be clearly compared on the basis of computational complexity. Thirdly, instead of utilizing estimators, any other approach to demodulate the modulated parameter of α-stable noise could also be seen.

Similarly, related to the second objective, more criteria capable of measuring the security of RCSs should be introduced. Similarly, the security of the discussed α-stable noise based RCSs should also measured in different channels as well. However, existing criteria, e.g. secrecy capacity and outage probability, to measure the security of conventional communication systems should be applied to analyze the security of α-stable noise based RCSs if does not contradict with the principles of α-stable noise, otherwise, the reason for implacability would also be an interesting concept. Moreover, instead of the proposed fractional lower order covariance matrix based attack, some other mechanism could also be utilized to propose more real-time attacks to discover the vulnerabilities of RCSs.

Finally, some interesting future research related to the third objective can also be done which includes i) utilizing higher-order inverse systems in RCS based on α-stable noise driven inverse systems and analyzing its effects on BER and security of the proposed system; ii) utilizing multiple LTI system in the design of RCS based on α-stable noise driven inverse system would be a vital attempt to increase the complexity of RCSs which could eventually result in enhanced covertness. Apart from achieving enhanced physical layer security from RCSs, its applicability can also be tested in future vehicular, molecular and electromagnetic nano-scale communications as well; the results could help in improvement of these fields which are currently at their infancy. Since, this field is new and not many researchers are working in this field, therefore, it has more room for improvement which will be seen in near future.

REFERENCES

Abadal S. and Akyildiz, I. F. (2011), ‘Bio-inspired synchronization for nanocommunication networks’, *Proc. 2011 Global Telecommunications Conference - Wireless Networking Symposium*, Houston, TX, USA, pp. 1–5.

Abadal S. and Akyildiz, I. F. (2011b), ‘Automata modeling of quorum sensing for nanocommunication networks’, *Nano Communication Networks*, 2, (1), pp. 74-83.

Abel, A. and Schwarz, W. (2002), ‘Chaos communications-principles, schemes, and system analysis’, *Proceedings of the IEEE*, 90, (5), pp. 691-710.

Abdallah, C., Dawson, D. M., Dorato, P. and Jamshidi, M. (1991), ‘Survey of robust control for rigid robots’, *IEEE Control Systems*, 11, (2), pp. 24–30.

Agnelli, F., Mazzini, G., Rovatti, R. and Setti, G. (2001), ‘A first experimental verification of optimum MAI reduction in chaos-based DS-CDMA systems’, in *Proc. Int. Symp. Circuits and Systems*, 3, Sydney, Australia, pp. 137–140.

Ahmed, A. and Savaci, F. A. (2017), ‘Random Communication System Based on Skewed Alpha-Stable Levy Noise Shift Keying’, *Fluctuation and Noise Letters*, , 16, (3), 1750024. 28

Ahmed, A. and Savaci, F. A. (2017b), ‘Measure of Covertness based on the imperfect synchronization of an eavesdropper in Random Communication Systems’, *10th Int. Conf. on Elec. and Elec. Eng. (ELECO)*, Bursa, Turkey, pp. 638-641. 29

Ahmed, A. and Savaci, F.A. (2018), ‘Synchronisation of alpha-stable levy noise-based Random Communication System’, *IET Communications*, 12, (3), pp. 276-282. 30

Ahmed, A. and Savaci, F.A. (2018b), ‘On Optimizing Fractional Lower-order Covariance based Synchronization Method for Random Communication Systems’, In *26th IEEE Signal Process. and Comm. Applications Conf. (SIU2018)*, Izmir, Turkey. 31

Ahmed, A. and Savaci, F.A. (2019), ‘Structure and Performance Evaluation of Fractional Lower-Order Covariance Method in Alpha-Stable Noise Environments(In-press)’, *Recent Advances in Electrical & Electronic Engineering*, 11

Alvarez, G., Montoya, F., Romera, M., and Pastor, G. (2004), ‘Breaking parameter modulated chaotic secure communication system’, *Chaos, Solitons & Fractals*, 21, pp. 783–787.

Alvarez, G., Montoya, F., Romera, M., and Pastor, G. (2004b), ‘Breaking two secure communication systems based on chaotic masking’, *IEEE Transactions on Circuits and Systems II: Express Briefs*, 51, (10), pp. 505-506.

Anfinsen, S.N. (2001), ‘A detection theoretical approach to digital communications using autoregressive process shift keying’, *PhD thesis*, University of Tromso.

Banerjee, S. and Agrawal, M. (2013), ‘Underwater acoustic communication in the presence of heavy-tailed impulsive noise with bi-parameter Cauchy-Gaussian mixture model’, In *IEEE Ocean Electronics (SYMPOL),* pp. 1-7.

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

Berber, S. and Feng, S. (2013), ‘Chaos-based physical layer design for WSN applications’, In *Proc. CIRCOM*, 2, pp. 157-162.

Burel, G. and Bouder, C. (2000), ‘Blind estimation of the pseudo-random sequence of a direct sequence spread spectrum signal’, *Proc. 21st Century Military Commun. Conf. (MILCOM)*, Los Angeles, CA, pp. 967-970.

Burel, G. (2000), ‘Detection of spread spectrum transmissions using fluctuations of correlation estimators’, In *IEEE Int. Symp. on Intelligent Signal Processing and Communication Systems (ISPACS'2000)*, 11, pp. B8. Honolulu, Hawaii, USA.

Cambanis, S., Samorodnitsky, G. and Taqqu, M.S. (1991), ‘*Stable Processes and Related Topics*’, Progress in Probability Series, 25, ISBN 0-8176-3485-1, Birkhäuser, Boston.

Carroll, T. L. and Pecora, L. M. (1991), ‘Synchronizating chaotic circuits’, *IEEE Trans. Circuits Syst.,* 38, (4), pp. 453456.

Casarin, R. (2004), ‘Bayesian inference for mixtures of stable distributions’, *Working paper No. 0428*, CEREMADE, University Paris IX.

Cavers, J. K. (1995), ‘Pilot symbol assisted modulation and differential detection in fading and delay spread', *IEEE Trans. on Communications*, 43, (7), pp. 2206–2212.

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

Cek, M.E. (2015) 'Covert communication using skewed α-stable distributions', *IET Electronics Letters*, , 51, (1), pp. 116-118.

Cek, M.E. (2015b), 'M-ary alpha-stable noise modulation in spread-spectrum communication', *Fluctuation & Noise Letters*, 14, (3), 1550022.

Chien, T.I. and Liao, T.L (2005), 'Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization', *Chaos, Solitons & Fractals*, 24, (1), pp. 241-255.

Chua, L. O (1980), 'Dynamic nonlinear networks: State-of-the-art', *IEEE Trans. Circuits Syst.*, 27, (11), pp. 1059-1087.

Diego, S.G., Kuruoglu, E.E. and Diego, P. R. (2009), 'Finite mixture of α-stable distributions', *Digital Signal Processing*, 19, (2), pp. 250-264.

Dedieu, H., Kennedy, M. P. and Hasler, M. (1993), 'Chaos shift keying: Mod-ulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits', *IEEE Trans. Circu. Syst. II, Anal. Digit. Sig. Process.*, 40, (10), pp. 634–642.

Dmitriev, A., Starkov, S. and Yemetz, S. (1998), 'Chaotic communication using digital signal processors', In *Proc. Int. Symp. Nonlinear Theory and Applications*, 3, Crans Montana, Switzerland, pp. 1093–1096.

Dmitriev, A., Kyarginsky, B., Panas, A. and Starkov, S. (2001), 'Direct chaotic communication system. Experiments', In *Proc. International Workshop on Nonlinear Dynamics in Electronic Systems*, Delft, The Netherlands, pp. 157–160.

Farsad, N., Guo, W., Chae, C. B. and Eckford, A. (2015), 'Stable distributions as noise models for molecular communication', In *IEEE Global Communications Conference (GLOBECOM),* pp. 1-6.

Farsad, N., Yilmaz, H.B., Eckford, A., Chae, C.-B. and Guo, W. (2016), 'A comprehensive survey of recent advancements in molecular communication', *IEEE*

Communication Surveys Tutorials., 2016, 18, (3), pp. 1887–1919.

Feller, W. (1971), '*An Introduction to Probability Theory and its Applications'*, Vol. 2, 2nd edition, Wiley, New York.

Fukunaga, K. and Krile, T. E. (1969), 'Calculation of Bayes recognition error for two multivariate Gaussian distribution', *IEEE Transactions on Computers,* 100, (3), pp. 220-229.

Gibson, J.D (1993), *Digital and Analog Communications,* Prentice-Hall.

Gnedenko, B. V. and Kolmogorov, A. N. (1954), '*Limit distributions for sums of independent random variables*', Addison-Wesley, Reading, MA.

Grigoriu, M. (1995), 'Linear systems subject to non-Gaussian α-stable processes', *Probabilistic engineering mechanics*, 10, (1), pp. 23-34.

Gu, C. and Cao, X. (2012), 'Research on information hiding technology', In *Proc. Int. Conf. Consum. Electron., Commun. Networks (CECNet)*, Three Gorges, China, pp.2035-2037.

Guo, W., Qiu, T., Tang, H. and Zhang, W. (2008), 'Performance of RBF neural networks for array processing in impulsive noise environment', *Digital Signal Processing*, 18, (2), pp. 168-178.

Hasler, M. and Schimming, T. (2002), 'Optimal and suboptimal chaos receivers', In *Proc. IEEE*, 90, (5), pp. 733-746.

Hayes, S., Grebogi, C. and Ott., E (1993), 'Communication with chaos', *Physical Review Letters*, 70, (20), pp. 3034.

He, H., Lu, J., Chen, J., Qiu, X. and Benesty, J. 2014, 'Robust blind identification of room acoustic channels in symmetric alpha-stable distributed noise environments', *The Journal of the Acoustical Society of America*, 136, (2), pp. 693-704.

He, X., Zhang, X. and Yang, B. (2010), 'The effect of imperfect carrier synchronization on the performance of multi-tone DSSS', In *12th IEEE International Conference on Communication Technology,* Nanjing*, ICCT.,* pp. 637-643.

Hughes, L. (2000), ‘Alpha-stable models of multiuser interference’, *Proc. Int. Sym. Information Theory*, Sorrento, Italy, p. 383.

Janicki, A. and Weron, A. (1994), ‘Simulation and chaotic behaviour of a-stable stochastic processes’, CRC Press, Marcel Dekker.

Jos, S., Kumar, P. and Chakrabarti, S. (2010), ‘An Accurate Analytical Model for Overloaded DS-CDMA under Imperfect Synchronization’, in *2010 IEEE 71st Vehicular Technology Conference,* Taipei, *VTC.,* pp. 1-4.

Jovic, B., Unsworth, C. P., Sandhu, G. S. and Berber, S. M. (2007), ‘A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems’, Signal Processing, 87, (7), pp. 1692-1708.

Kailath, T. (1980), ‘*Linear systems'*, 156, Englewood Cliffs, NJ: Prentice-Hall.

Kaddoum, G., Roviras, D.,Chargé, P. and Fournier-Prunaret, D. (2009), ‘Robust synchronization for asynchronous multi-user chaos-based DS-CDMA’, *Signal Procesing.*, 2009, 89, (5), pp. 807-818.

Kaddoum, G., Richardson, F. and Gagnon, F. (2013), ‘Design and analysis of a multi-carrier differential chaos shift keying communication system’, *IEEE Trans. Commun.*, 61, (8), pp. 3281-3291.

Kaddoum, G. (2016), ‘Wireless chaos-based communication systems: A comprehensive survey’, *IEEE Access*, *4*, pp.2621-2648.

Kannan, N. and Ravishanker, N. (2007), ‘High resolution estimation for sub-Gaussian stable signals in a linear array model’, *IET Signal Processing*, 1, (1), pp. 35-42.

Discrete-time chaotic encryption systems. Part II: Continuous- and discrete-value realization’, In *Proc. Int. Workshop Nonlinear Dynamics in Electronic Systems*, Seville, Spain, pp. 27–32.

Kennedy, M. P., Kolumbán, G., Kis, G. and Jákó, Z. (2000), ‘Performance evaluation of FM-DCSK modulation in multipath environments’, *IEEE Transactions on Circuits Systems I, Fundamentals Theory Applications*, 47, (12), pp. 1702–1711.

Kennedy, M. P., Rovatti, R. and Setti, G. (2000b), '*Chaotic Electronics in Telecom-Munications*', London, U.K.: CRC Press.

Kolumbán, G., Kennedy, M. P. and Chua, L. O. (1997), 'The role of synchronization in digital communications using chaos. I. Fundamentals of digital communications', *IEEE Transaction on Circuits Systems I, Fundentals Theory Applications*, 44, (10), pp. 927–936.

Kosko, B. and Mitaim, S. (2010), 'Stochastic resonance in noisy threshold neurons', *Neural networks*, vol. 16, (5), pp. 755-761.

Kocarev, L., Halle, K. S., Eckert, K., Chua, L. O. and Parlitz, U. (1992), 'Experimental demonstration of secure communications via chaotic synchronization', *Int. J. Bifurcation and Chaos,* 2, (3), pp. 709-713.

Kong, L., Kaddoum, G. and Taha, M. (2015), 'Performance analysis of physical layer security of chaos-based modulation schemes' In *IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),* pp. 283-288.

Kurian, A. P., Puthusserypady, S. and Htut, S. M. (2005), 'Performance enhancementof DS/CDMA system using chaotic complex spreading sequence'. *IEEE Trans. Wireless Commun.*, 4, (3), pp. 984-989.

Kuruoğlu, E. E. (2001), 'Density parameter estimation of skewed alpha-stable distributions', *IEEE Transactions on Signal Process*ing, 49, (10), pp. 2192–2201.

Król, K., Azzinnari, L., Korpela, E., Mozsàry, A., Talonen, M. and Porra, V. (2001), 'An experimental FM-DCSK chaos radio system', In *Prococeedings of European Conference on Circuit Theory and Design*, 3, Espoo, Finland, pp. 17–20.

Lau, F. C. M. and Tse, C. K. (2003), '*Chaos-Based Digital Communication Systems'*, Heidelberg, Germany: Springer-Verlag.

Liu, W. H. Wang, Y. Y., Wang, B., Huang, B. Q. and Qiu, T. S. (2009), 'Stochastic Resonance Based Latency Delay Estimation for Weak Evoked Potentials with Impulsive Noises', *Ninth IEEE ICCIT*, Xiamen, pp. 252-257.

Lynnyk, V. and Celikovsky, S. (2010), 'On the anti-synchronization detection for the generalized Lorenz system and its applications to secure encryption', *Cybernetika*, 46, (1), pp. 1-18.

Ma, X. and Nikias, C.L. (1996), ‘Joint estimation of time delay and frequency delay in impulsive noise using fractional lower order statistics’, *IEEE Trans. Signal Process.*, 44, (11), pp. 2669–2687.

Ma, X. Y. (1996b), ‘Robust signal processing in impulsive noise with stable distributions: estimation, identification and equalization’, *Dissertation, University of Southern California*, Los Angeles.

Mislovaty, R., Klein, E., Kanter, I. and Kinzel, W. (2004), ‘Security of neural cryptography", In *11th IEEE International Conference on Electronics, Circuits and Systems (ICECS),* Tel Aviv, pp. 219-221.

Moore, M. and Nakano, T. (2012), ‘Synchronization of inhibitory molecular spike oscillators’, *Bio-Inspired Models of Networks, Information, and Computing Systems*, 103, pp. 183–195.

Moore, M. and Nakano, T. (2013), ‘Oscillation and synchronization of molecular machines by the diffusion of inhibitory molecules’, *IEEE Transactions on Nanotechnology*, 12, (4), pp. 601-608.

Naqvi, H., Berber, S. and Salcic, Z. (2009), ‘Performance analysis of collaborative communication with imperfect frequency synchronization and AWGN in wireless sensor networks’, *Communication and Networking (CCIS),* pp. 114-121.

Naqvi, H., Berber, S. and Salcic, Z. (2009b), ‘Performance analysis of collaborative communication in the presence of phase errors and AWGN in wireless sensor networks’, in *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC*), Leipzig, pp. 394-398.

Nikias, C.L. and Petropulu, A. P. (1993), ‘*Higher-order spectra Analysis: a Nonlinear Signal Processing Framework’,* Prentice-Hall, Englewood Cliffs.

Nikias, C.L. and Shao, M. (1995), ‘*Signal Processing with Alpha-Stable Distributions and Applications*’*,* Wiley, New York.

Oppenheim, A. V., Wornell, G.W., Isabelle, S.H and Cuomo, K.M. (1992), ‘Signal processing in the context of chaotic signals’, In *Acoustic Speech and Signal Processing (ICASSP)*, San Francisco, CA, USA, pp. 117-120.

Parlitz, U., Chua, L.O., Kocarev, L., Halle, K.S. and Shang, A. (1992), ‘Transmission of digital signals by chaotic synchronization’, *International Journal of Bifurcation and Chaos*, *2,* (04), pp.973-977.

Pecora, L. M. and Carroll, T. L. (1990), ‘Synchronization in chaotic systems’, *Physics Review Letters*’, 64, (8), pp. 821–823.

Pecora, L.M. and Carroll, T.L. (1991), ‘Driving systems with chaotic signals’, *Physical Review A*, 44, (4), p. 2374.

Pecora, L.M. and Carroll, T.L. (1991b), ‘Synchronized chaotic signal and systems’, In *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP-92).,* 4, pp. 137-140.

Peterson, R. L., Zeimer, R. E. and Borth, D. E. (1995), *Introduction to Spread Spectrum Communications*, Englewood Cliffs, NJ, USA: Prentice-Hall.

Pickholtz, R., Schilling, D. and Milstein, L. (1982), ‘Theory of Spread-Spectrum Communications - A Tutorial’, *IEEE Trans. on Communications*, 30, (5), pp. 855-884.

Polydoros, A. and Weber, C. (1984), ‘A Unified Approach to Serial Search Spread-Spectrum Code Acquisition - Part I: General Theory’, *IEEE Transactions on Communications*, 32, (5), pp. 542-549.

Polydoros, A. and Weber, C. (1984b), ‘A Unified Approach to Serial Search Spread-Spectrum Code Acquisition - Part II: A Matched-Filter Receiver’, *IEEE Transactions on Communications*, 32, (5), pp. 550-560.

Rajan, A. and Tepedelenlioglu, C. (2010), ‘Diversity combining over Rayleigh fading channels with symmetric alpha-stable noise’, *IEEE Transactions on Wireless Communications*, 9, (9), pp. 2968-2976.

Salberg, A.B. and Hanssen, A. (1999), ‘Secure digital communications by means of stochastic process shift keying’, In *Proc. Int. Conf. Signals, Systems*, *and Computers*, PacificGrove, USA, pp. 1523–1527.

Salberg, A.B. and Hanssen, A. (2000), ‘Stochastic process shift keying: A novel modulation method for secure digital communications’, In *IEEE 10th European Signal Processing Conference,* pp. 1-4.

Salberg, A-B. and Hanssen, A. (2001), ‘Subspace detectors for stochastic process shift keying’, In *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'01)*, 4, pp. 2549-2552.

Salehi, M. and Proakis, J. (2007), *Digital Communications*, New York, NY, USA: McGraw-Hill.

Samorodnitsky, G. and Taqqu, M.S. (1994), '*Stable non-gaussian random processes*', Chapman & Hall/CRC.

Scharf, L.L. (1991), '*Statistical Signal Processing: Detection, Estimation, and Time Series Analysis',* Addison-Wesley.

Shannon, C. E. (1949), 'Communication in the presence of noise', In *Proceedings Of the IRE*, 37, (1), pp. 10-21.

Short, K.M. (1994), 'Steps toward unmasking secure communications', *International Journal of Bifurcation and Chaos*, 4, (04), pp. 959-977.

Short, K.M. (1996), 'Unmasking a modulated chaotic communications scheme', *International Journal of Bifurcation and Chaos*, 6, (02), pp. 367-375.

Sobhy, M. I. and Shehata, A. E. (2001), 'Methods of attacking chaotic encryption and countermeasures', In *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'01),* 2, pp. 1001-1004.

Sushchik, M., Rulkov, N., Larson, N., Tsimring, L., Abarbanel, H., Yao, K. and Volkovskii, A. (2000), 'Chaotic pulse position modulation: A robust method of communicating with chaos', *IEEE Communication Letters*, 4, (4), pp. 128–130.

Stiff1er, J.J. (1971), '*Theory of Synchronous Communications'*, Prentice-Hall, Englewood Cliffs, New Jersey.

Tsatsanis, M.K. and Giannakis, G.B. (1997), 'Blind Estimation of Direct Sequence Spread Spectrum Signals in Multipath', *IEEE Transactions on Signal Processing*, 45, (5), pp. 1241- 1252.

Todorovic, B. M. (1989), 'The impact of imperfect code synchronization on bit error rate in DS-SS systems: upper and lower bound', In *Electrotechnical Conference, 1989. Proceedings. 'Integrating Research, Industry and Education in Energy and Communication Engineering',* Lisbon, *MELECON.,* pp. 524-527.

Tong, L., Sadler, B. M. and Dong, M. (2004), 'Pilot-assisted wireless transmissions: general model, design criteria, and signal processing', *IEEE Signal Processing*

Magazine, 21, (6), pp. 12-25.

Tsihrintzis, G. A. and Nikias, C. L. (1996), ‘Fast estimation of the parameters of alpha-stable impulsive interference’, *IEEE Trans. Signal Process.*, 44, (6), pp. 1492–1503.

Vali, R., Berber, S. M. and Nguang, S. K. (2010), ‘Effect of Rayleigh fading on non-coherent sequence synchronization for multi-user chaos based DS-CDMA’, *Signal Processing*, 90, (6), pp. 1924-1939.

Vali, R., Berber, S. M. and Nguang, S. K. (2012), ‘Accurate derivation of chaosbased acquisition performance in a fading channel’, *IEEE Trans.Wireless Commun.*, 11, (2), pp. 722-731.

Vali, R., Berber, S. M. and Nguang, S. K. (2012b), ‘Analysis of chaos-based code tracking using chaotic correlation statistics’, *IEEE Trans. Circuits Syst. I*, 59, (4), pp. 796-805.

Wang, J., Kuruoglu, E. E. and Zhou, T. (2011), ‘Alpha-stable channel capacity’, *IEEE Communications Letters*, 15, (10), pp. 1107-1109.

Win, M., Pinto, P. and Shepp, L. (2009), ‘A mathematical theory of network interference and its applications’, *Proc. IEEE*, 97, (2), pp. 205–230.

Xia, Y., Tse, C. K. and Lau, F. C. M. (2004), ‘Performance of differential chaosshift-keying digital communication systems over a multipath fading channel with delay spread’, *IEEE Trans. Circuits Syst. II, Exp. Briefs*, 51, (12), pp. 680-684.

Xu, Z.J., Yuan, J., Wang, K., LiMin, M. and Hua, J. (2014), ‘A Novel Structure for Covert Communication Based on Alpha Stable Distribution’, Information Technology Journal, 13, pp. 1673-1677.

Xu, Z.J., Wang, K., Gong, Y., Lu, W.D., Hua J.Y. (2016), ‘Structure and performance analysis of an SαS-based digital modulation system’, *IET Communications*, 10, (11), pp.1329–1339.

Xu, Z.J., Wang, K., Gong, Y Lu, W.D., Hua J.Y. (2017), ‘A Covert Digital Cmmunication System Based on Joint Normal Distribution’, *IET Communications*, 11, (8), pp. 1282-1290.

Yang, T., Yang, L.B. and Yang, C.M. (1998), ‘Breaking chaotic switching using generalized synchronization: Examples’, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 45, (10), pp. 1062-1067.

Yang, X. and Petropulu, A. (2003), ‘Co-channel interference modeling and analysis in a Poisson field of interferers in wireless communications’, IEEE Trans. Signal Process., 51, (1), pp. 64–76.

Yang, P., Tan, Z., Wiesel, A. and Nehorai, A. (2013), ‘Power system state estimation using PMUs with imperfect synchronization’, *IEEE Transactions on power Systems*, 28, 4, pp. 4162-4172.

Yu, J. and Yao, Y.-D. (2005), ‘Detection performance of chaotic spreading LPI waveforms’, *IEEE Transactions on Wireless Communications*, 4, (2), pp. 390-396.

Żak, G., Wyłomańska, A. and Zimroz, R. (2017), ‘Periodically impulsive behavior detection in noisy observation based on generalized fractional order dependency map’, *Applied Acoustics*.

Zhang, J. Qiu, T., Wang, P. and Luan, S. (2017) ‘A novel cauchy score function based DOA estimation method under alpha-stable noise environments’, *Signal Processing*, 138, pp. 98-105.

Zhou, T., Chen, L. and Aihara, K. (2005), ‘Molecular communication through stochastic synchronization induced by extracellular fluctuations’, *Physical Review Letters*, 95, (17), 178103.

Zolotarev, V. M. (1986), ‘One-dimensional Stable Distributions’, *Translations of mathematical monographs*, 65, American Mathematical Society.