DOKUZ EYLÜL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

DIRECT SEQUENCE SPREAD-SPECTRUM BASED COVERT COMMUNICATION USING RANDOM PULSE WIDTH MODULATION

by

Gizem AKCAN

September, 2019

İZMİR

DIRECT SEQUENCE SPREAD-SPECTRUM BASED COVERT COMMUNICATION USING RANDOM PULSE WIDTH MODULATION

A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of Dokuz Eylül University
In Partial Fulfillment of the Requirements for the Degree of Master of Science of Electrical and Electronics Engineering

by
Gizem AKCAN

September, 2019
İZMİR

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"DIRECT SEQUENCE SPREAD-SPECTRUM BASED COVERT COMMUNICATION USING RANDOM PULSE WIDTH MODULATION"** completed by **GİZEM AKCAN** under supervision of **ASSIST.PROF.DR. MEHMET EMRE ÇEK** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Mehmet Emre ÇEK

Supervisor

Assoc. Prof. Dr. Olcay Akay

(Jury Member)

Assist. Prof. Dr. İlhan BAŞTÜRK

(Jury Member)

Prof.Dr. Kadriye ERTEKİN

Director

Graduate School of Natural and Applied Sciences

ACKNOWLEDGEMENT

Firstly, I would like to thank my supervisor Asst. Prof. Dr. Mehmet Emre Çek for accepting working with me and devoting me his precious time. I am grateful for his patience, interest and effort throughout my thesis. Also, I would like to express my appreciation to my jury members for significant feedback related to my thesis work.

I would like to acknowledge my superiors Hakan EVMEK and Levent Hakkı ŞENYÜREK for showing understanding and patience to me. I would like to offer my special thanks to my fellow Evren ÇATAK for expressive comments and her help. I want to thank my dear friends Burcu BARIŞ, Ayça KAYA, Halil İbrahim ALTUN and Taha Muhammed KAYAOĞLU. They provided moral support which gave me praise and courage.

Especially, I am grateful to my dear family, my father, İhsan AKCAN and my mother, Şaziye AKCAN due to their moral and material support. My little brother, Adem Görkem AKCAN always has been my source of joy and stamina.

Gizem AKCAN

DIRECT SEQUENCE SPREAD-SPECTRUM BASED COVERT COMMUNICATION USING RANDOM PULSE WIDTH MODULATION

ABSTRACT

In this thesis, a novel non-coherent spread-spectrum communication system which uses Random Pulse Width Modulation (RPWM) or equivalently Random Pulse Duration Modulation (RPDM) is proposed. Differing from the conventional spread-spectrum communication schemes where the receiver is assumed to generate the same pseudo-noise (PN) sequence with the transmitter, the receiver determines the transmitted binary message from the statistical properties of the residence times of the binary valued rectangular waveform whose positive and negative states have random lengths according to the prescribed probability density function. Since the residence times for both positive and negative states cannot be smaller than zero, the minimum value of the random variable must be controllable. Therefore, the uniform distribution having bounded interval is a reasonable choice and used to model the random length of the rectangular noise-like signal. At the receiver, there is a moving average process acting as low-pass filter in order to recover these random lengths without distortion under additive channel noise. This method provides to construct a noise sequence which does not exhibit repetitive behaviour for each message bit and instead of conventional PN sequence this proposed binary sequence exhibits more stochastic behaviour to increase security. The randomness of the proposed method is analysed in terms of autocorrelation and triple correlation characteristics according to the literature.

This method is observed to provide a certain error performance depending on the selection of noise parameters such as mean and variance at the transmitter and the detector performance can be improved by increasing the number of elements of the vectors achieved by positive and negative residence times of the noise-like signal.

Keywords: Direct Sequence Spread-Spectrum (DSSS), covert communication, Random Pulse Width Modulation (RPWM), Pseudo-Noise (PN) sequence

RASSAL DARBE KALINLIĞI KİPLENİMİ KULLANARAK DOĞRUDAN DİZİ YAYILI-SPEKTRUM TABANLI GİZLİ HABERLEŞME

ÖZ

Bu tezde, Rastgele Darbe Genişliği Modülasyonu (RPWM) veya aynı anlamlı Rastgele Darbe Süre Modülasyonu (RPDM) kullanan ve tutarlı olmayan yeni bir yayılı-spektrumlu iletişim sistemi önerilmiştir. Alıcının, vericiyle aynı sözde-gürültü (PN) dizisini oluşturduğu varsayıldığı geleneksel yayılı spektrum iletişim şemalarından farklı olarak; alıcı iletilen ikili mesajı, pozitif ve negatif durumları öngörülen olasılık yoğunluğu fonksiyonuna göre rastgele bir uzunluğa sahip olan ikili değerli dikdörtgen dalga biçiminin kalma zamanlarının istatistiksel özelliklerinden belirler. Hem pozitif hem de negatif durumlar için kalma süreleri sıfırdan küçük olamayacağı için, rastgele değişkenin minimum değeri kontrol edilebilir olmalıdır. Bu nedenle, sınırlı aralığa sahip olan düzgün dağılım makul bir seçimdir ve dikdörtgen şeklindeki gürültü benzeri sinyalin rastgele uzunluğunu modellemek için kullanılır. Alıcıda, ilave kanal gürültüsü altında bozulma olmadan bu rastgele uzunlukları geri kazanmak için düşük geçişli filtre görevi gören bir hareketli ortalama işlem vardır. Bu yöntem, her mesaj biti için tekrarlayıcı davranış sergilemeyen bir gürültü dizisi oluşturmayı sağlar ve geleneksel PN dizisi yerine bu önerilen ikili dizilim güvenliği arttırmak için daha stokastik davranış sergiler. Önerilen yöntemin rastgeleliği, literatüre göre otokorelasyon ve üçlü korelasyon özellikleri açısından analiz edilmiştir.

Bu yöntemin, vericideki ortalama ve varyans gibi gürültü parametrelerinin seçimine bağlı olarak belirli bir hata performansı sağladığı gözlenmektedir ve dedektör performansı, gürültü benzeri sinyalin pozitif ve negatif kalma süreleri ile elde edilen vektörlerin element sayısı arttırılarak iyileştirilebilir.

Anahtar kelimeler: Doğrudan Dizi Yayılı-Spektrum (DSSS), güvenli haberleşme, Rastgele Darbe Kalınlığı Modülasyonu (RPWM), Sözde-Gürültü (PN) dizisi

CONTENTS

Page

LIST OF FIGURES

Page

CHAPTER ONE
INTRODUCTION

The importance of the communication sector is increasing day by day. Depending on the data transmission rate, there exists an increased requirement on information capacity. In recent years, privacy and security have become challenging topics in wireless communication systems. With this motivation, the covertness has vital significance not only in military but also in commercial communication. Therefore, covertness of communication system is indispensable for security of data transmission. In the sequel, the literature survey is given related to studies concentrating on secure communication in physical layer.

1.1 Survey on Spread Spectrum (SS) Communication Techniques

In this thesis, the covertness of the digital communication in physical layer is characterized by camouflaging the message signal by spreading its narrow-band spectrum into wide-band in the channel by applying spectrum-spreading techniques. This procedure is also significant due to providing robustness against interference, and low probability of intercept in channel. The conventional attempt on spread-spectrum proposed by (Pickholtz, Schilling & Milstein, 1982) is to encode the message by a prescribed binary sequence and convert the narrow band message signal into wide band signal in the channel which is known as spectrum-spreading in order to reduce the jamming and/or interference from other sources in the channel. The spectrum-spreading operation is performed by utilizing specifically generated binary sequence which is called pseudo noise (PN) sequence. The term pseudo-noise comes from the spectral properties of PN binary sequence which is similar to white noise. Formally, a communication system can be described as spread-spectrum communication if the following requirements are satisfied:

- Transmitted signal bandwidth in the channel must be larger than the message signal bandwidth.
- The transmitted signal must be resolved by the receiver using the identical structure with the transmitter, which is uncorrelated with the message signal.

Among the several spectrum-spreading techniques the most studied ones are PN sequence based conventional spread-spectrum, chaotic and random communication techniques. The reason of conventional approach to be based on PN sequences is due to the statistical properties such as autocorrelation exhibiting the same characteristic with noise within a certain prescribed interval (Shiu, Chang, Wu, Huang, & Chen, 2011). Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) are known to be basic conventional methods (Haykin, 1994). There is also an interest on detection of transmitted message based on conventional spectrum-spreading. On the other hand, detection of wide band signals is another interest in covert communication research. An early attempt by (Hill, Comley & Adams, 1997) deals with detection of covert wide band digital communication signals which utilizes sideband structure of modulated signals and bi-spectral analysis arising from higher order correlation analysis. In a consequent study, fluctuation of autocorrelation estimators are proposed to detect DSSS signals (Burel, 2000). A remarkable other study is recommended for estimation of spreading sequences by appealing to the maximum-likelihood (ML) detector. On the contrary to eigenvalue decomposition (EVD) based algorithms, which have high computational complexity, ML estimator is reported to attain lower estimation error and exhibit superior performance (Mehboodi, Jamshidi & Farhang, 2018).

In practice, it is assumed to have no information about spreading code in order to detect PN sequence based communication signals. Therefore, the blind estimation methods to detect spread-spectrum sequences take prevalent part in the literature. Blind estimation techniques are consulted, when the receiver has no knowledge about transmitter parameters. A notable approach is the detection of DSSS sequence based on eigenanalysis techniques where the first and second eigenvectors of the covariance matrix obtained from observed signal is reported to give same clue about the transmitted sequence (Burel & Bouder, 2000; Bouder, Azou & Burel, 2004). Similarly, principal component analysis (PCA) is used to estimate weak spread-spectrum signals (Vlok & Olivier, 2012). By this method, the largest eigenvalue sequence of the intercepted signal is extracted and this value is used to perform detection in AWGN. Missing data model is used to detect long-code DSSS signals

by showing as a short-code DSSS signal (Zhang, Gan, Liao, Wei & Li, 2012). In this way, spread waveform estimation issue is replaced with a low-rank matrix approximation problem and with optimization methods which are expectation maximization (EM) algorithm and the Cramer–Rao lower bound (CRB), the estimation is performed successfully. Another study that aims blind source separation in direct-sequence code-division multiple-access (DS-CDMA) under multiple-input multiple-output (MIMO) channel model is described by (Yao & Poor, 2004). In a latter work (Qui, Huang, Jiang & Zhang, 2008), the SS signals and a novel segmentation algorithm is proposed for both the short-code and long-code DSSS signals. In addition, Qui and his colleagues combine their works with the multiple signal classification (MUSIC)-based algorithm (Haghighat & Soleymani, 2005) and robust blind multiuser spreading sequences estimation is accomplished (Qui et al., 2010).

Focusing on recent studies, detection is realized by taking triple correlation functions (TCF) (Zhao, Shen & Gu, 2016). An algorithm has been proposed for estimating PN sequences in multi-user long scrambling code direct sequence spread spectrum (LSC-DSSS) signals (Zhao, Gu & Qiang, 2017). In the study (Liang, Wang & Huang, 2017), an algorithm has been proposed about multi-user direct sequence code division estimation of PN sequences in a multiple access application. Additionally, detection of self-recurrence period of PN sequences is considered by (Shen & Wang, 2017). Information sequences of DSSS are tried to blind estimate by using Markov Chain Monte Carlo-Unscented Kalman Filter (MCMC-UKF) (Ma, Zhang & Liu, 2017). Alternatively, a new method is proposed including subspace algorithm and expansion of finite alphabet properties in Direct Sequence Code Division Multiple Access System (DS-CDMA) (Sarcheshmeh, Bizaki & Alizadeh, 2018).

Multiple access interference (MAI) is an important challenge for the multiuser communication system. To handle this difficulty, chirp modulation which is another conventional method (or other name linear frequency modulation) is suggested by (Winkler, 1962) firstly, is implemented for binary data transmission (Khan, Rao &

Wang, 2013). By using non-linear trigonometric and hyperbolic chirp waveforms, individual chip rate which decreases the interferences considerably, is gained for each user. To make more dependable, unpredictable and random DSSS system, logistic map is used to generate PN sequence which is formed by one-dimensional chirp signals (Swami & Sarma, 2014).

Chaotic communication techniques are suggested as an alternative to conventional approaches to improve security of spread-spectrum communication. The fundamental chaotic schemes are chaotic masking and chaotic modulation (Kocarev, Halle, Eckert, Chua & Parlitz, 1992) in analog communication whereas coherent system chaos shift keying (CSK) (Lau & Tse, 2003) and non-coherent systems differential chaos shift keying (DCSK) (Kolumban, Vizvki, Schwarz & Abel, 1996), frequency-modulated DCSK (FM-DCSK) (Kolumban, Kis, Jako & Kennedy, 1997) and correlation delay shift keying (CDSK) (Sushchik, Tsimring & Volkovskii, 2000) in digital communication (Stavroulakis, 2006). The beginning usage of chaotic signals in spectrum-spread communication is after the chaotic synchronization which is recognized by (Pecora & Caroll, 1990). Chaotic masking or modulation schemes are proposed by (Oppenheim, Wornell, Isabelle & Cuomo, 1992; Kolumban, Kennedy & Chua, 1998; Morgül, 2000; Parlitz et al., 2004). Observer based synchronization studies of chaotic masking are also mentioned by (Morgül, Solak & Akgül, 2003; Li, Wang, Zhou, Fang, & Ni, 2008; Chen & Min, 2008).

In contrast to analog chaotic communication, digital chaotic methods provide uncorrelated and non-periodic communication particularly. Uncorrelated spread spectrum techniques remove the requirement of pre-shared secrets and provide randomness in the frequency channels and spread code. Common synchronization is used in a reliable communication application (Min & Zhang, 2005). In (Guo-Hui, 2005), a complicated drive-response design is achieved to recover security. In another article (Li, Álvarez & Chen, 2005) chaotic encryption is claimed to improve safe communication. In addition, impulsive synchronization in digital chaotic schemes is described in (Yang & Chua, 1997; Xie, Wen & Li, 2000; Yang, 2001;

Sun, Zhang & Wu, 2002; Chen, Yang & Wang, 2004) and the necessary conditions are specified for stability of chaotic systems.

DCSK communication method reached high competence on the purpose of improving data security (Yang & Jiang, 2012). In spread spectrum (SS) communication, pre-shared secrets are shared among nodes first to install spread sequences. For long-term wireless communication, this causes circular dependency problem (CDP). Reliable secret sharing mechanism is achieved by combining two processes which are intractable forward decoding and efficient backward decoding (Cassola, Jin, Noubir & Thapa, 2013). Thus, faster solution is obtained against CDP. Moreover, a new spread spectrum communication system is presented with chaotic modulation (Kaddoum & Gagnon, 2013). Using the symbolic dynamics approach, robust sequence synchronization and a lower probability of detection are obtained. However, instead of direct transmission of chaotic signals, constant envelope signals which expose chaotic manner, can be used. Frequency modulated-differential chaos shift keying (FM-DCSK) is used for that aim (Kennedy et. al., 2000). The chaos based FM signals theory is studied by (Callegari, Rovatti & Setti, 2003a). Hardware application of FM-DCSK is mentioned in article (Callegari et al., 2003b) and another hardware implementation is demonstrated in (Leon, Balkir, Hoffman & Perez, 2005) in which a chaotic PN sequence is generated.

Random spread-spectrum communication developments are better alternatives for safe communication than previous techniques due to increased spectrum-spreading behaviour. The α-stable distribution is used as non-Gaussian noise-like carrier in random communication since it is characterized by its statistical properties. The first noteworthy article about α-stable distribution is publised by (Çek & Savacı, 2009), in which the symmetric α-stable noise (SαS) is modulated by binary message. The message signal is encoded by using a random signal rather than deterministic signals. Therefore, the signal can be called as random carrier. On the other hand, SαS sequences have considerable complexity unlike impulsive characteristic in time domain. To handle this problem, a new technique which is the symmetric alpha-

stable Differential Shift Keying (SαS-DSK) is offered by (Xu, Gong, Lu, Wang & Hua, 2014).

A further study is proposed in recent years based on random communication. In the article of (Çek, 2015a), a binary signal is encoded without basing on correlation method and skewed α-stable distribution (SkαS) is introduced. Unlike SαS noise parameter modulation method which is dependent on characteristic α parameter, SkαS is based on skewness parameter β. M-ary random communication system is tendered versus the binary SαS-DSK method (Çek, 2015b). M-ary random signal is recovered by using Hadamard matrix. In addition, the logarithmic moment estimator is offered by (Xu et al., 2016) to enhance bit error performance and acquire optimal decision in the receiver. An alternative approach is suggested by (Ahmed & Savacı, 2017a) in which β parameter of received signal is estimated by Modified Extreme Value Method (MEVM) and this estimator is fastest compared with sinc estimator and logarithmic estimator. (Xu et al., 2017) exhibited a new study which involves coefficient correlation estimation of two Gaussian successive sequences in terms of joint normal distribution. As the transmitted signal behaves as white Gaussian noise, an improved security performance is exposed versus eavesdroppers.

In the studies given above, the synchronization is not separately analysed and any method about the synchronization does not exist. The significant study is demonstrated the synchronization in RCSs by (Ahmed & Savacı, 2018a). Noting that the correlation and covariance are second error moments of α-stable distribution and they cannot be applied in synchronization because the second-order and higher-order moments of α-stable random distribution do not occur, the fractional lower-order covariance-based correlator (FLOCC) is examined between two α-stable distributions in (Ahmed & Savacı, 2018a) to analyse the synchronization.

There are further studies which aim to improve spectrum-spreading in terms of deniability (Che, Bakshi & Jaggi, 2013; Che et al., 2014a; Che & Chan et al., 2014b), low-probability of detection (Bash, Goeckel & Towsley, 2013) and undetectable communication (Lee & Baxley, 2014; Lee, Weitnauer & Walkenhorst et al., 2015).

Performance of the secure wireless communication is limited due to some parameters such as average power and channel capacity, when the data is hidden in noise. Trying to solve these limitations, shadow network which consists of transmitters, receivers, and friendly jammers, are proposed (Bash & Guha et al., 2015) Moreover, secure communication is provided in the existence of uninformed jammer (Sobers et al., 2017).

In recent years, to achieve secure and reliable communication, different channel techniques are applied during transmission of information and the resolution of covert communication is examined over a discrete memoryless channel (Bloch, 2016; Yan, He, Cong & Zhou, 2017) investigated the impact of finite block length channels on receiver success rate and detection performance in AWGN. (Tahmasbi & Bloch, 2018) investigated the effect of the first and second-order asymptotics in covert communication that are characterized on binary-input Discrete Memoryless Channels (DMCs). Another article touches on difference between the covert communication and the spread-spectrum communication based on physical-layer security for a wiretap channel (Forouzesh, Azmi, Mokari & Wong, 2018). More recently, (Tan & Lee, 2019) establishes secure capacity region for discrete or Gaussian non-memory broadcast channel in time domain.

On the other hand, spreading methods of signal spectrum are used not only for telecommunication but also in power electronic applications to eliminate electromagnetic interference (EMI) (Pareschi, Rovatti & Setti, 2015). Among many spreading techniques, the randomized pulse width modulation (PWM) is remarkable. PWM waveform that has period or duty cycle, changes every time step randomly. Different approaches of pulse modulation can be viewed (Mihalic and Kos, 2006). PWM generally is applied in switching power converters for EMI reduction (Gosavi, 2008; Kobori, Arafune, Tsukiji, Takai & Kobayashi, 2015; Solankee, Bhatia & Khan, 2012; Wang, Lin, Du, Wu & He, 2017). In addition, alternate spread spectrum PWM techniques are examined also. Their analog and digital implementations are realized with robust converters against EMI in the switch-mode power supply (Gamoudi, Chariag & Sbita, 2018).

The security performance of the DSSS communication system is reported by (Narayanan, Chuang & DeMay, 2008) to be detectable for intruders using methods such as triple correlation, deviations in the auto-correlation function in the PN-based DSSS communication system. Additionally, it is reported that the noise-like statistical characteristic performance reflecting the non-periodic behaviour of the PN sequence is limited to the length of the generated sequence and that the message can be predicted by covariance analysis statistically due to the repetitive structure (Narayanan & Mohan et al., 2009). Therefore, more resistant methods are required against detection of DSSS signals. In light of previous studies, a novel direct sequence spread-spectrum method is proposed based on random pulse width modulation (RPWM) for covert communication in this thesis.

1.2 Scope of Thesis

This thesis mainly concentrates on the newly proposed covert communication method called random pulse width modulation (RPWM) for reliable communication where the signal parameters such as residence time for positive and negative states are obtained from the direct noise sequence instead of the pseudo noise (PN) sequence. In the DSSS technique, transmitters use partially periodic PN sequences to transmit the signal spectrum and transmit the signal below the noise level and main band signal is encoded. The PN sequence used in the transmitter is not known temporally or spectrally in the channel. The spectral information extraction of the PN sequence directly in the channel is practically impossible. The privacy performance of the DSSS communication system depends on the length of the PN sequence, which limits the security level and the need to produce the same PN sequence simultaneously in the receiver constitutes the disadvantages of this communication system.

The main approach in this thesis study for providing covertness in communication systems is the utilization of novel spectrum-spreading technique where the main concern is to create novel random sequence to encode the binary data. This method is called random pulse width modulation (RPWM) based DSSS communication in

which noise behaves autocorrelated function instead of the self-repeating and self-correlation structure of the PN sequence into signal observed in the channel. The first advantage of this method is that the receiver decides the binary message by doing statistical inference from time period of positive and negative values of sent signal. Another benefit is that the communication can be provided with non-coherent receiver in which synchronism is not needed between the receiver and the data.

1.3 Outline of Thesis

The thesis is organized as follows. Chapter 2 describes the spread spectrum methods from the literature which are conventional, chaotic and random communication techniques and their different modulation types are explained briefly. Chapter 3 includes the proposed method and describes the transmitter receiver structure. In addition, the autocorrelation and triple correlation analysis to represent the security and bit error rate (BER) performance are realised for the proposed study. The last chapter concludes the results, the receiver design is analysed to improve the error performance. The future projections are given.

CHAPTER TWO
SPREAD SPECTRUM METHODS

Spread-spectrum in digital communication is formally defined as:

Spread spectrum is a means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information; the band spread is accomplished by means of code which is independent of the data, and a synchronized reception with the code at the receiver is used for de-spreading and subsequent data recovery (Pickholtz et al., 1982, p. 855).

Starting in military communication from mid-1950s, spread spectrum has been an evolving technique for secure communication and preferred due to wide band-nature embedding narrow band message into wide-band (Sugi & Joe, 2015). Spectrum-spreading distributes the signal energy over a wider frequency band as shown in Figure 2.1 and then converts the wide-band signal into its original spectral form as shown in Figure 2.2.

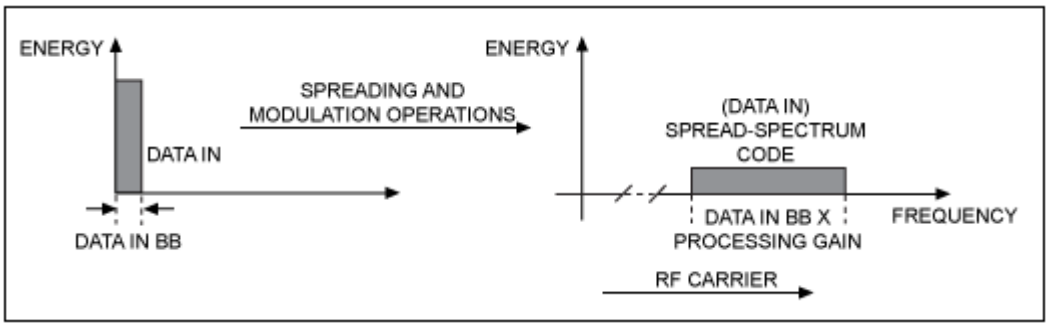

Figure 2.1 Spectrum-spreading of spread-spectrum transmitter (Singh, 2013)

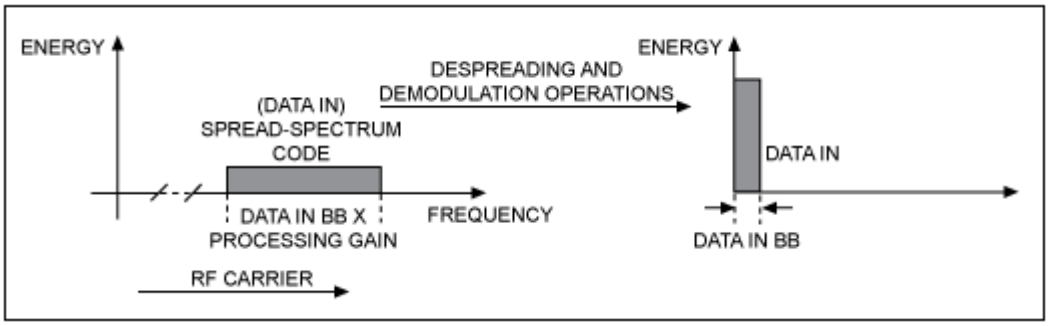

Figure 2.2 De-spreading operation of spread-spectrum receiver (Singh, 2013)

The advantages of spectrum-spreading is cross-talk elimination, decreased multipath fading, improved security, robustness against noise, co-existence with other systems, longer operative distances, hard to detect, not easy to decode by an intruder and resistant to jamming (Fazel & Kaiser, 2008).

2.1 Conventional Methods of Spread Spectrum

The basic conventional spectrum-spreading techniques are:

- Direct Sequence Spread Spectrum (DSSS)
- Frequency Hopped Spread Spectrum (FHSS)
- Chirp Spread Spectrum (CSS)
- Time Hopped Spread Spectrum (THSS)

In the first two methods, pseudo-random number sequences are employed which are called pseudo-noise (PN) sequences (Pickholtz et al., 1982). PN sequence is a coded binary series of 1s and 0s with exact autocorrelation properties of noise. It is generated by a feedback shift register. The block diagram of feedback shift register is shown in Figure 2.3. A feedback shift register consists of *m* flip-flops which are two-state memory and a logic circuit all connected to create a multi-loop feedback circuit. As a result, the PN sequence becomes periodic with a period of at most $2^m - 1$. The period of the PN sequence cannot exceed $2^m - 1$, it is called a maximal-length sequence or *m*-sequence simply (Haykin, 1994).

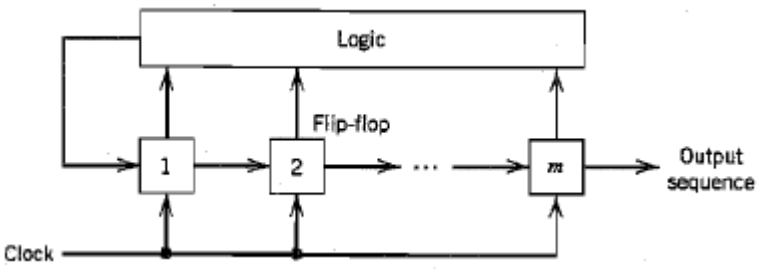

Figure 2.3 Feedback shift register (Haykin, 1994)

The fundamental properties of PN sequences are balance property, run property and auto-correlation property. In balance property, the number of 1s in the sequence is one greater than the number of 0s in every PN sequence. In run property, sub-sequence of 1s or 0s form a run. One half of the runs are of length 1, one quarter of the runs is of length 2 and this length continues increment sequentially along the power of 2. For maximal-length sequence, the total number run is $(G+1)/2$ in which $G = 2^m - 1$ and m is the length of shift register. The autocorrelation function of PN sequence is periodic and binary valued (Haykin, 1994).

The general formula of autocorrelation function of periodic signal *c(t)* is given as:

$$R_C(\tau) = \frac{1}{T_b}\int_{-T_b/2}^{T_b/2} c(t) * c(t-\tau)\, dt \tag{2.1}$$

In Equation (2.1), lag τ lies between $(-T_b/2, T_b/2)$ and T_b is period of maximal length PN sequence. It is expressed as:

$$T_b = G * T_c \tag{2.2}$$

T_c is duration of 1s and 0s which are appointed in PN code. The autocorrelation function is plotted in Figure 2.4 in which frequency of single bit f_c is used instead of T_c.

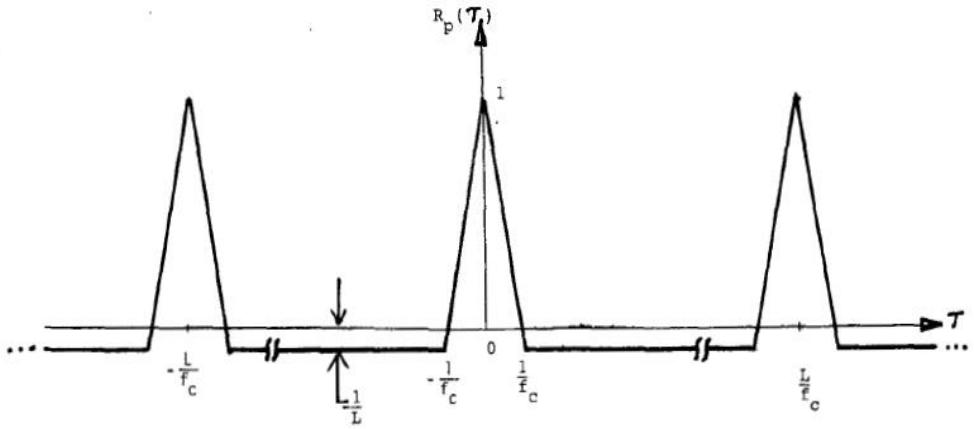

Figure 2.4 Autocorrelation function of PN sequence (Pickholtz et al., 1982)

2.1.1 Direct Sequence Spread Spectrum (DSSS)

Direct Sequence (DS) methods are the most frequently used spread spectrum technique. In DSSS technique, the spreading of narrow-band signal is provided by modulation in which pseudo-noise (PN) binary code is used to encode this information signal. The effect of PN sequence is transmission of the wideband noise like signal which carries the embedded data (Kopp, 2005). Spreading of data message with PN code is shown in Figure 2.5. In the PN code, chip is the time period of a single bit and the bit rate of the PN code is called the chip rate.

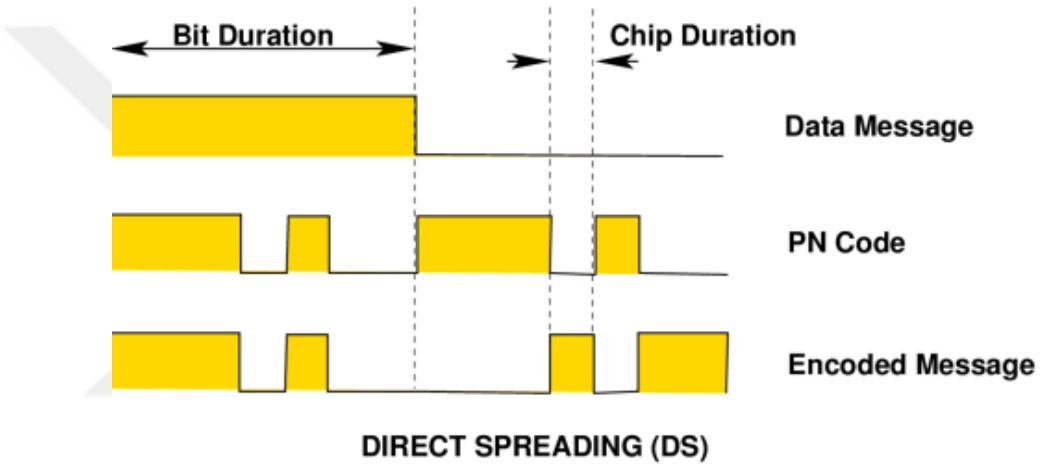

Figure 2.5 Direct-spreading of data signal (Kopp, 2005)

When the message is transmitted, several digital modulation methods can be employed although Phase Shift Keying (PSK) is the most common one in practice. Figure 2.6 demonstrates the block diagram for the direct sequence spread-spectrum system with binary phase shift keying (BPSK). By using Binary PSK, the carrier wave is phase shifted back and forth 180 degrees with each 1 or 0 in the PN code. As a result, resultant spectrum can be obtained which is nearly the same as the wideband PN sequence by multiplying the modulated signal with the PN code. The transmitted signal is called a direct sequence spread binary phase shift keyed signal (DS/ BPSK), (Sugi & Joe, 2015).

DSSS receiver is more complex than the transmitter. The main idea is the use of the correlation operation in all receivers of spread spectrum techniques. The

correlation operation is the integral of the product of two time varying functions mathematically. Similarly, the correlator is established by compounding a multiplier with a low pass filter in a DS receiver. First function is received PN modulated signal, the other is the PN sequence produced by a local PN code generator in the receiver. The receiver's local PN generator is identical with PN generator in the transmitter. The time varying measure of the similarity between the two codes is taken from multiplier output and the estimated data is extracted by coherent detector. The series of processes is often named de-spreading (Kopp, 2005).

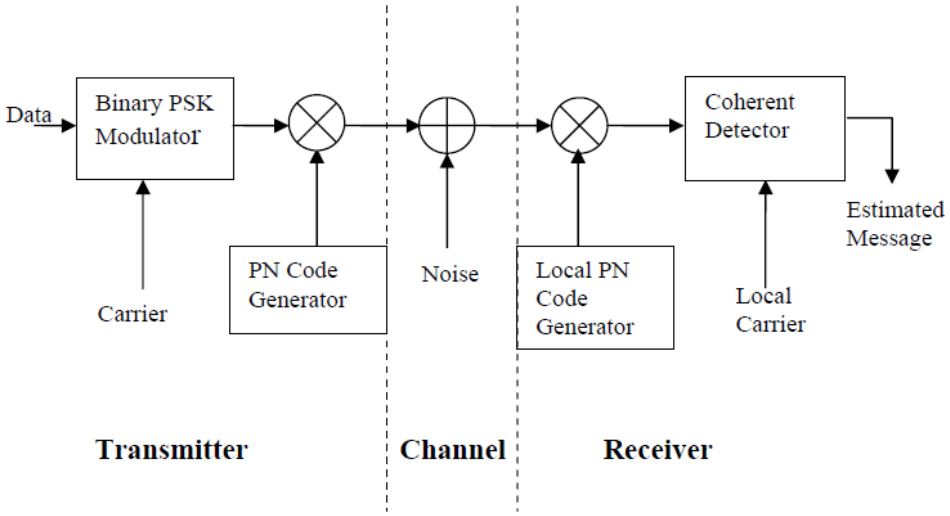

Figure 2.6 Block diagram of the direct sequence spread-binary PSK system (Haykin, 1994)

2.1.2 Frequency Hopped Spread Spectrum (FHSS)

In FHSS system, the name of frequency hopping comes from the carrier which hops from one frequency to another over a wide band via a PN sequence. The speed of hops changes according to the data rate of the original information. Therefore, there are two basic characterizations of frequency hopping which are fast frequency hopping (Fast FHSS) and low frequency hopping (Low FHSS). Low FHSS is the most common and allows sequential data bits to modulate the same frequency. Fast FHSS is characterized by several hops within each data bit (Singh, 2013). In FHSS, M-ary frequency shift keying (MFSK) is the mostly employed modulation method.

The combination of both methods FH/MFSK is described in Figure 2.7. In the transmitter, binary data is passed through M-ary FSK modulator first. After product of modulated signal, the frequency synthesizer is applied to the band pass filter. PN code generator creates *m*-bit segments which drive the frequency synthesizer. In this way, carrier frequency hops over 2^m exact values and frequency hopping is succeeded (Haykin, 1994).

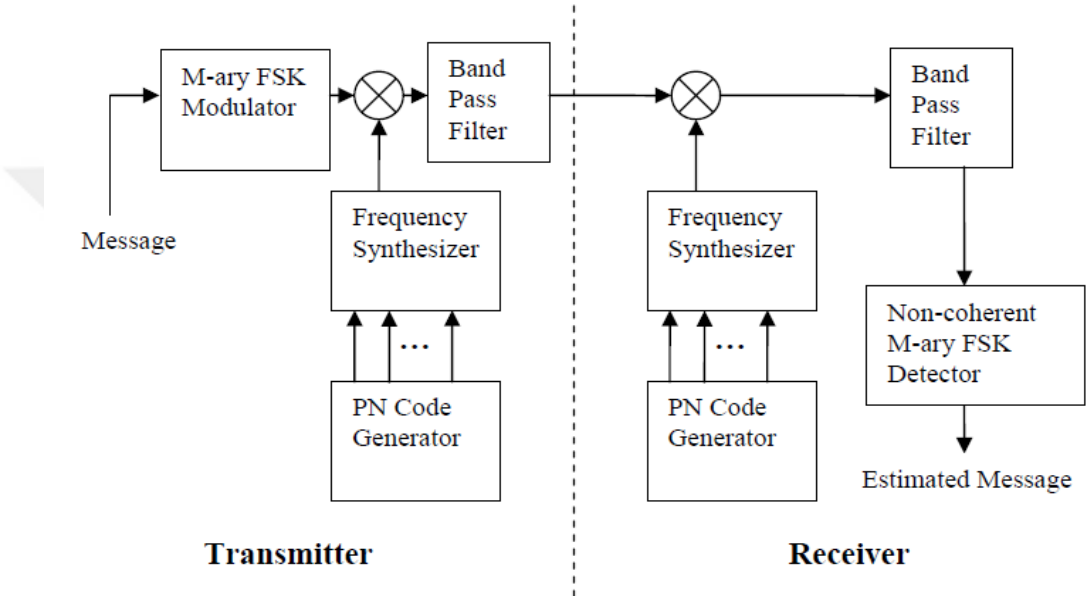

Figure 2.7 Block diagram of the frequency hop M-ary frequency-shift keying (Haykin, 1994)

In the receiver part in Figure 2.7, the frequency hopping provides correlation of the received data by mixing with the frequency synthesizer which behaves in the same manner as in the transmitter. After the received signal is passed through from the band pass filter, it is applied to the non-coherent M-ary FSK detector. Non-coherent match filter is used to implement the detector and original symbol of transmitted signal is achieved by choosing the largest filter output (Haykin, 1994).

2.1.3 Chirp Spread Spectrum (CSS)

A chirp is a sinusoidal signal whose frequency varies over a defined time. Chirp modulation or linear frequency modulation is presented in (Winkler, 1962). Chirp

spread spectrum technique is applied in order to provide multiple access (Billa, Sharma & Ashraf, 2012).

Unlike DSSS and FHSS, pseudo-random elements are not used for encoding in CSS instead wide-band deterministic signal is distinguished from noise using the characteristics of the chirp pulse such as chirp parameter and auto-correlation behaviour. The whole allocated bandwidth of the chirp spread spectrum is used to transmit the signal. Therefore, this technique is robust to channel noise and resistant to multi-path fading even at very low power because of wide band of the spectrum (Kowatsch & Lafferl, 1983).

In Figure 2.8, the multi-user chirp spread-spectrum system is described. As an earlier study, multi-access CSS is defined by (Cook, 1974). Linear chirps with different chirp rates are used as spread spectrum signals by assigning them to several users. Thus, multiple access is provided within a common frequency band. The orthogonal frequency-division multiplexing (OFDM) method can be used for chirp modulation, where all user channels are parallel slices of bandwidth in the time-frequency domain. As a result, parallel slices are orthogonal to time and frequency axis. Demodulation and estimation are realized by correlation receivers. Each received signal is multiplied by its coherent. The replica of spreading signal of unit energy is generated and integrated over one symbol interval to access the decision variable. Eventually, the transmitted message is estimated by a threshold detector by detecting the sign of the decision device (Billa et al., 2012).

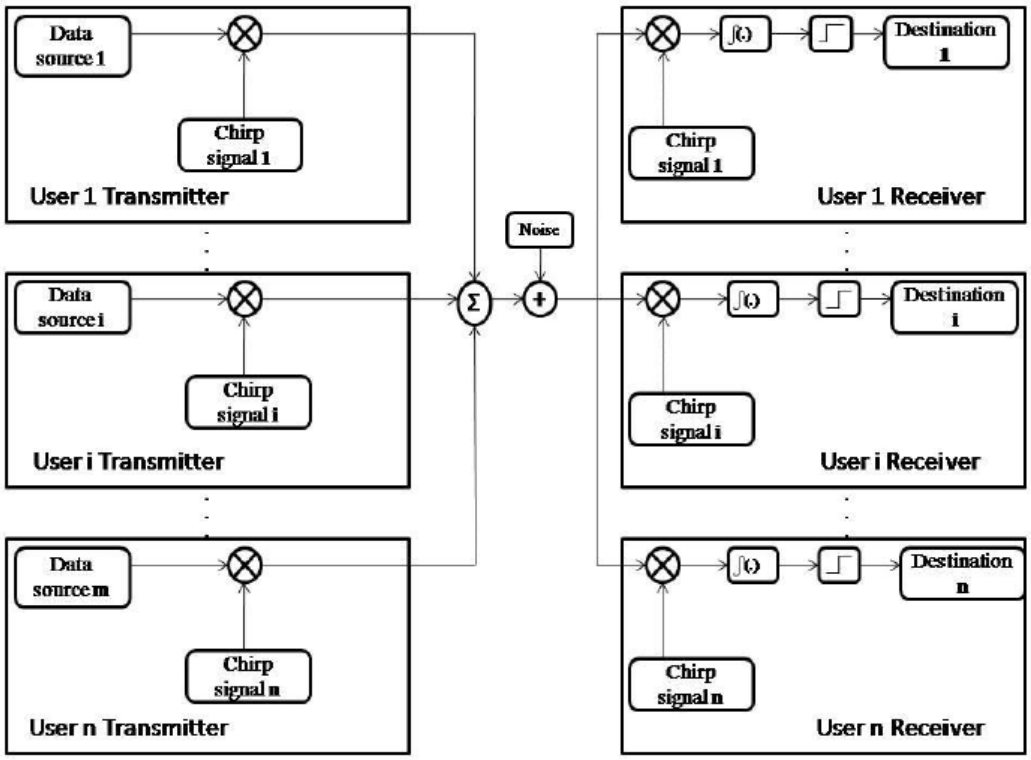

Figure 2.8 Block diagram of chirp spread spectrum system (Billa et al., 2012)

The time-division duplex also can be applied for the multi-user chirp spread spectrum system to separate the downlink and uplink communication in RF design. The pulse-position for multiple access is applied on the downlink and feedback channel equalization is used on the uplink to improve the CSS (Knapp & Pap, 2018).

2.1.4 Time Hopped Spread Spectrum (THSS)

Time-hopping (TH) is a communication technique of spread spectrum signal which provides anti-jamming (AJ) or low probability of intercept (LPI). The pulse period and duty cycle is changed in terms of pseudo number sequence to achieve LPI in TH. In this way, the transmission time in terms of varies and transmitted signal has intermittent start and stop times. TH resembles the digital modulation scheme called pulse position modulation (PPM) so time hopping method is not considered apart from PPM. The main difference between PPM and TH is that data information is characterized by using pulse position model in PPM whereas special code sequences

are defined firstly which behave as secret keys, then hidden information is decoded (Win & Scholtz, 2000).

2.2 Chaotic Communication

Unlike conventional communication system in which the information signal is transmitted by high frequency sinusoidal carrier, chaotic communication system is based on an aperiodic signal acquired by chaotic dynamical system. Even if identical symbol is sent continuously, transmitted signal is never repetitive due to one of the main properties of chaotic dynamical systems to be sensitively dependent on initial conditions. The reason for employing chaotic signals in spread-spectrum communication is due to the properties of chaotic signals such as noise-like behaviour, easy to generate, broadband spectrum yielding low probability detection, increased data security and relatively simple hardware implementation (Ren, Bai, Liu, Baptista & Grebogi, 2016). Chaos-based communication is desirable in spread spectrum system with these features.

Chaotic communication system is applied both in analog and digital communication. Chaotic masking and chaotic modulation are two basic techniques for analog communication. Both techniques are separated from each other by synchronization in demodulation process (Stavroulakis, 2006). Since chaos-based system depends on parameter values and is sensitive to initial condition values, the synchronization is needed in transmitter and receiver part of chaotic masking (Çiçek, Kocamaz & Uyaroğlu, 2018) where synchronization of chaotic systems is introduced for the first time by (Pecora & Carroll, 1990). The digital chaotic techniques apply shift keying modulation which are chaos shift keying (CSK) based on coherent detection at the receiver, differential chaos shift keying (DCSK), correlation delay shift keying (CDSK) and frequency-modulated DCSK (FM-DCSK) based on non-coherent detection at the receiver (Stavroulakis, 2006). Due to the synchronization problems between transmitter and receiver in practice, non-coherent receiver based techniques are most commonly employed in recent years. In the sequel, analog and digital chaotic communication systems are explained briefly.

2.2.1 Chaotic Masking

Chaotic masking process is described such that the analog message signal is added to the noise-like chaotic signal in the transmitter unit. At the receiver, chaotic signal is obtained during synchronization process and the original information signal is estimated by subtracting the regenerated chaotic signal from arriving signal. The achievement of chaotic masking depends on the selected synchronization technique (Sun, 2016).

After the synchronization invention of (Pecora & Carroll, 1990), the chaotic masking and modulation is reported by (Oppenheim et al., 1992, Cuomo & Oppenheim, 1993). In that article, it is shown how the synchronization is integrated with the masking concept. In addition, the chaotic signal is generated by Chua's circuit along synchronization in masking method. A similar result was obtained in another study (Kocarev et al., 1992).

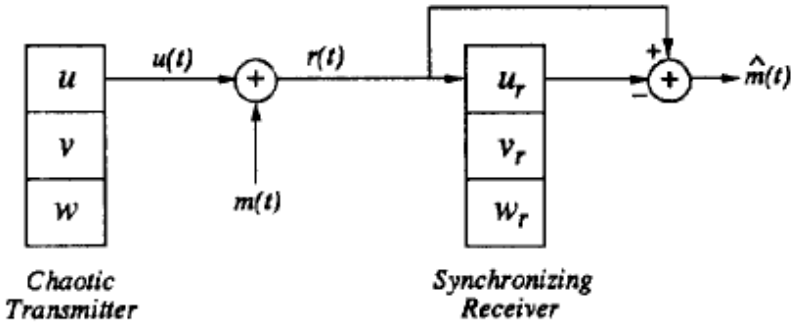

Figure 2.9 Chaotic signal masking system (Cuomo & Oppenheim, 1993)

Chaotic masking block diagram is described in Figure 2.9. Masking is provided by noise-like signal $u(t)$ which is added to information-bearing message $m(t)$ at the transmitter. This masking is eliminated at the receiver by extracting the chaotic signal from received signal $r(t)$. To benefit from synchronization at the receiver, the power of $m(t)$ should be importantly lower than the power of chaotic signal $u(t)$.

2.2.2 Chaos Shift Keying (CSK)

Chaos shift keying communication system is described by (Kocarev et al., 1992) and (Dedieu, Kennedy & Hasler, 1993). In CSK scheme, each symbol is matched with the dissimilar chaotic attractor signal and the chaotic attractor is generated by identical dynamic system in terms of distinct bifurcation values or other parameters of dynamic system. The purpose of CSK demodulation is to determine which attractor provides less synchronization error.

The block diagram of basic CSK digital communication is viewed in Figure 2.10. In the transmitter, two chaotic signals f and g generate $c(\widehat{t})$ and $c(\widetilde{t})$ sequentially. The bit duration is defined by T_b. When the binary signal is +1, $c(\widehat{t})$ is sent or the binary signal is -1, $c(\widetilde{t})$ is transmitted during the bit duration. Demodulation of CSK scheme can be provided by coherent correlation receiver or non-coherent receiver (Kolumban et al., 1998). Their difference is that the coherent correlation receiver realizes demodulation process by synchronization. On the other hand, the non-coherent receiver method evaluates the variance of received signal or uses the chaotic on-off keying (COOK).

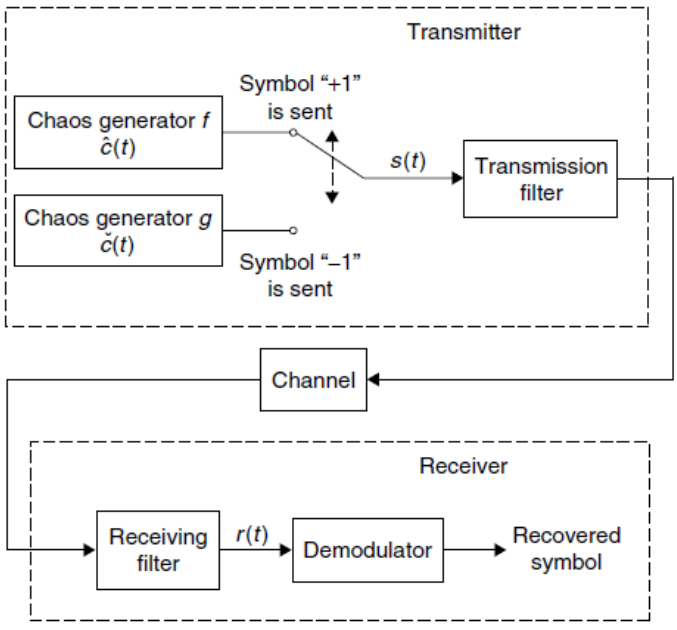

Figure 2.10 CSK digital communication (Stavroulakis, 2006)

COOK technique is a straightforward type of CSK communication as can be seen in Figure 2.11. According to its basic structure, if binary information b_i is +1, the system switches on. If the value of b_i is -1 there will be no apparent signal to switch on. At the receiver, the binary information is estimated according to the level of bit energy E_b obtained by correlation output. When the energy is above a certain threshold, the message bit is estimated as +1. The only need for simple system is the chaotic oscillator but resultant system offers poor security. The main disadvantage is that the threshold always can vary according to the signal to noise ratio.

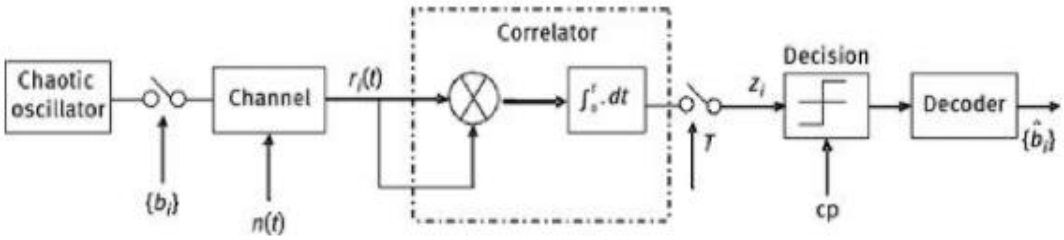

Figure 2.11 Block diagram of non-coherent COOK modulation and demodulation (Sun, 2016)

2.2.3 Differential Chaos Shift Keying (DCSK)

Due to the strong synchronization requirement of coherent CSK receiver, and non-constant threshold to estimate message bit under various intensity of noise for non-coherent CSK detector, differential chaos shift keying (DCSK) is proposed as non-coherent communication method by (Kolumban et al., 1996). DCSK has superior advantages compared to CSK. Chaotic carrier is not regenerated in demodulation process and DCSK needs only an auto-coherent demodulator (Fang et al., 2016). Each symbol to be sent is described in two sample functions in DCSK communication. The first one is reference function and the other one is information bearing function that keeps information. The reference signal is created twice by chaos generator and sends the bit “1” in the event of binary transmission. The chaotic reference message is transmitted followed by reversed version of the same message for the bit “-1”. At the receiver unit, both functions are correlated and the threshold comparator decides the transmitted message bit (Kolumban et al., 1998).

Figure 2.12 illustrates DCSK communication scheme. A chaotic signal x_i at time instant i is obtained at the end of the transmit process whose sequence of length M is continued by identical sequence which is multiplied by information message of lth bit $b_l = \pm 1$. The transmitted signal s_i is defined by:

$$s_i = \begin{cases} x_i, & 0 < i \leq M \\ b_l x_{i-M}, & M < i \leq 2M \end{cases} \tag{2.3}$$

The received signal M delayed r_{i+M} is multiplied by itself r_i to retrieve the information signal. The average of result is calculated over spreading length M and the correlator output is obtained as:

$$S = \sum_{i=1}^{M} r_i r_{i+M} \tag{2.4}$$

Consequently, the desirable information signal is reached.

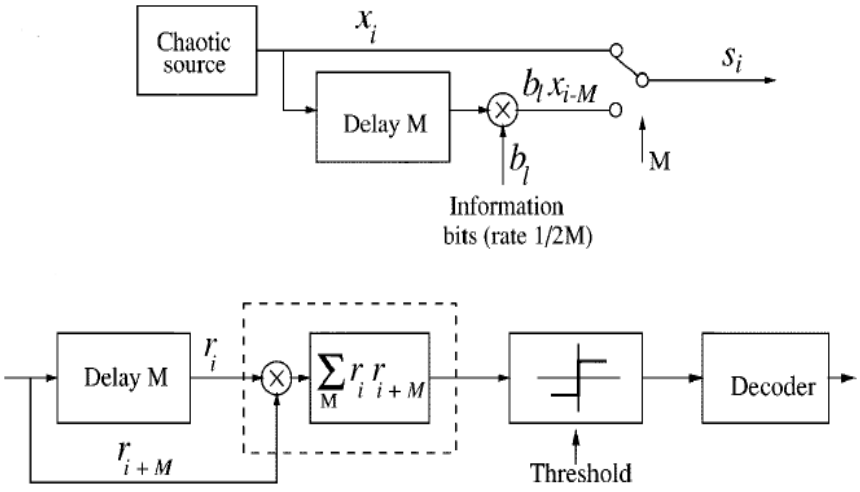

Figure 2.12 Block diagram of DCSK transmitter and receiver (Sushchik et al., 2000)

2.2.4 Correlation Delay Shift Keying (CDSK)

A recent study reports that the main shortcomings of DCSK are inclination to interception because of twice transmission of similar chaotic signal and switching

problem of transmission signal between information and reference signal by which DCSK bandwidth efficiency reduces to half (Duan & Yang, 2018). An alternative method exists in non-coherent chaotic communication systems, correlation delay shift keying (CDSK) is offered by (Sushchik et al., 2000). Figure 2.13 represents CDSK operation. Transmitted signal $s_i = x_i + b_l x_{i-L}$ is summation of chaotic signal x_i and its delayed signal x_{i-L} that is multiplied with data signal lth message bit $b_l = \pm 1$. Since the adder is used instead of switching, the transmit signal is not replicated which ensures better tolerance to interception than DCSK. Receiver part of CDSK communication is almost identical to DCSK apart from the delay L. The correlation of chaotic signals is nonzero and the signum of the correlator output determines the transmitted message bit (Stavroulakis, 2006).

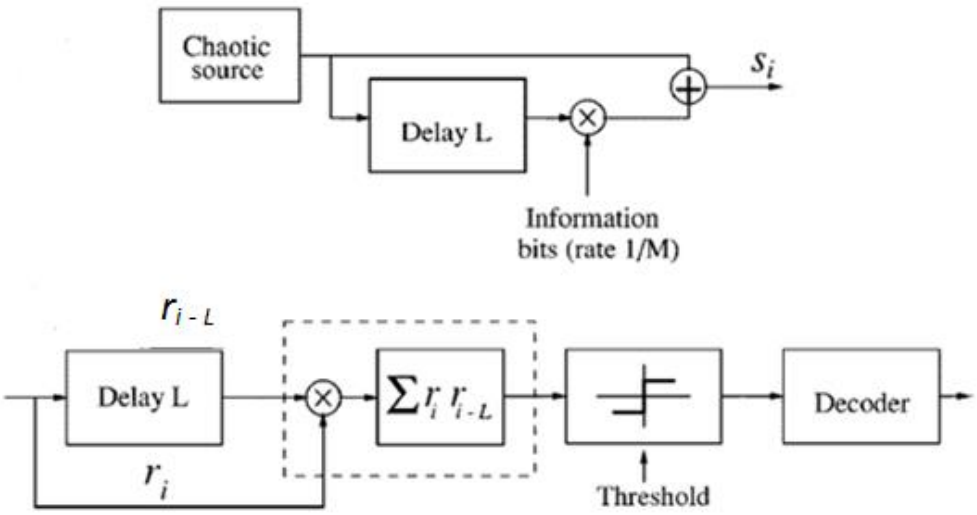

Figure 2.13 Block diagram of CDSK transmitter and receiver

2.2.5 Frequency-Modulated DCSK (FM-DCSK)

Since the necessity on transmission of binary information over a high frequency carrier within a certain bandwidth, there exists an improvement on chaotic communication systems by modifying transmitter and receiver structure considering constant envelop sinusoidal carrier. As a result, frequency-modulated differential

chaos shift keying (FM-DCSK) is proposed by (Kolumban et al., 1997). FM-DCSK is constant power version of DCSK and has other promising characteristics like superior performance and easy implementation. FM-DCSK uses Walsh functions providing orthogonality which can also be used for multiple access. Moreover, chaotic signal is combined with conventional sinusoidal carrier signal in this technique which ensures persistent bit energy to be constant (Ye, Chen & Wang, 2005).

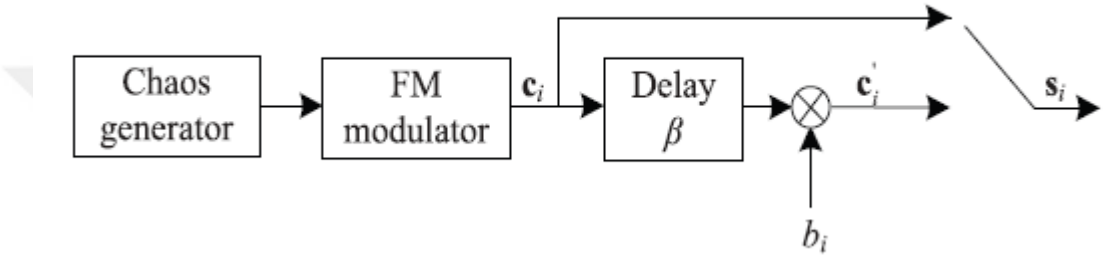

Figure 2.14 Block diagram of FM-DCSK transmitter (Fang et al., 2016)

FM-DCSK transmitter is different from DCSK and that is illustrated in Figure 2.14. In this scheme, the chaotic FM signal generator is required which is fed by chaos generator. The output of transmitter s_i is bandlimited and controlled by chaotic FM modulator. The receiver scheme of FM-DCSK is identical with DCSK demodulator.

2.3 Random Communication

The conventional communication techniques mentioned above used encoding and decoding processes which need synchronization for coherent detection and to achieve the information signal. PN codes also are reported to be uncovered even though they exhibit noise-like behaviour. Since the autocorrelation of PN creates self-repetitive sequences due to periodic nature of PN sequence, the system is vulnerable to intruders (Narayanan et al., 2009). This shortcoming degrades the security of conventional communication. Moreover, chaotic communication methods described in the previous section, apply mostly the self-synchronization procedure

before passing to demodulation process to provide rigid synchronism. On the other hand, chaotic carrier is sensitive to additive noise and channel distortions. Therefore synchronization constitutes the most critical drawback of chaotic system because of high SNR requirement.

These drawbacks of conventional PN based direct sequence spread-spectrum and chaotic communication systems lead to be development of alternative spread-spectrum communication techniques. In this manner, random communication system (RCS) is proposed to enhance security of SS communication considering conventional CSs and chaotic CSs (Çek & Savacı, 2009). The main principle of random communication is to demonstrate the waveform to be sent as noise instead of noise-like carrier. RCS employs stochastic carrier signal to transmit binary message. Random shift keying based modulation techniques are used for this secure communication scheme. An early attempt having the similar concept called as stochastic process shift keying (SPSK) method is reported by (Salberg & Hanssen, 1999) where different noise sequences are generated to carry binary information and the receiver determines the estimated symbol by utilizing statistical properties of the transmitted message. SPSK system is then reported to be evolved by constructing subspace detector against inter symbol interference effects (Salberg & Hanssen, 2001).

2.3.1 Noise Parameter Modulation

Another utilization of noise in secure communication is to employ a noise signal generated from a prescribed probability density function which is necessarily to be non-Gaussian. As the non-Gaussian noise, the α-stable distributed random signal is used to encode the binary message as stochastic modulation technique. The binary information is encoded by the noise parameters that is why it is called noise parameter modulation. It is proposed by (Çek & Savacı, 2009) where symmetric α-stable (SαS) distributed noise signal is used to carry binary information. This type of communication method is called as random communication technique. Since there is no closed form expression for the α-stable distribution except for Gaussian, Cauchy

and Levy distributions, this non-Gaussian distribution is expressed in terms of its characteristic function as given below:

$$\emptyset(\theta) = \begin{cases} \exp\left\{j\mu\theta - \gamma^{\alpha}|\theta|^{\alpha}\left(1 - j\beta sign(\theta) tan\left(\frac{\alpha\pi}{2}\right)\right)\right\} & if\ \alpha \neq 1 \\ \exp\left\{j\mu\theta - \gamma|\theta|(1 + j\beta\frac{2}{\pi}sign(\theta)\ln|\theta|)\right\} & if\ \alpha = 1 \end{cases} \quad (2.5)$$

where $\alpha \in (0,2]$, $\beta \in [-1,1]$, $\gamma \geq 0$, and $\mu \in (-\infty, \infty)$, tune the impulsiveness, symmetry, intensity and location, respectively. If β is equal to zero, the function becomes symmetric around μ (Samorodnitsky & Taqqu, 1994).

The noise parameter modulation scheme is illustrated in Figure 2.15. The binary message modulates the stable non-Gaussian noise sequences. During this process, the binary information is carried by characteristic exponent α of the symmetric α-stable distribution. When the message bit to be sent is 0, α_0 stable signal is transmitted along bit duration. When the message bit 1 is sent, α_1 stable signal is transmitted. In the receiver, characteristic exponent is estimated and the binary signal is decided by using parameter estimation described by (Kuruoğlu, 2001).

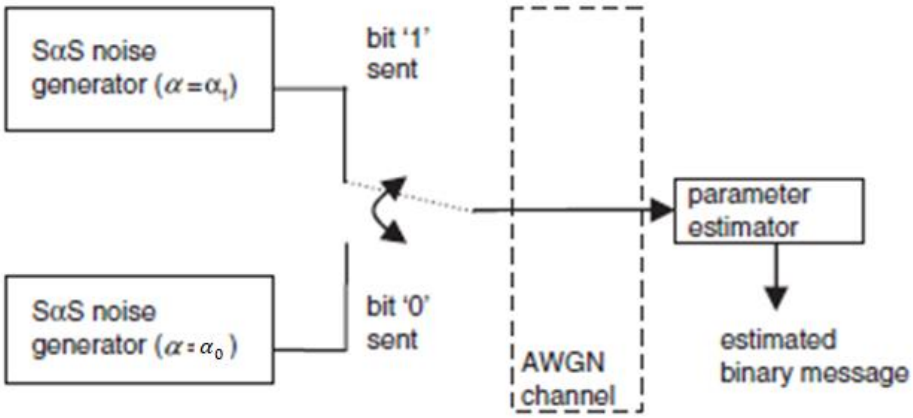

Figure 2.15 Block diagram of noise parameter modulation (Çek & Savacı, 2009)

2.3.2 Differential Symmetric α Stable Shift Keying (SαS-DSK)

Transmitter part of the noise parameter modulation, given in the previous section needs two separate SαS noise generators which increases the system complexity. In addition, if two α parameters are far away from each other, they can be estimated easily but if both parameters are too close, separating them from each other is difficult and this causes a trade-off between bit error performance and security of the system. Therefore, a new method which is named Differential Symmetric α Stable Shift Keying (SαS-DSK) is proposed by (Xu et al., 2014). In the SαS-DSK technique, the reference signal having SαS distribution and its replica modulated by binary message is augmented. Correlator receiver determines the sign of correlation result in order to estimate the message. The transmitter and receiver parts of aforementioned communication system are illustrated in Figure 2.16 and Figure 2.17, respectively.

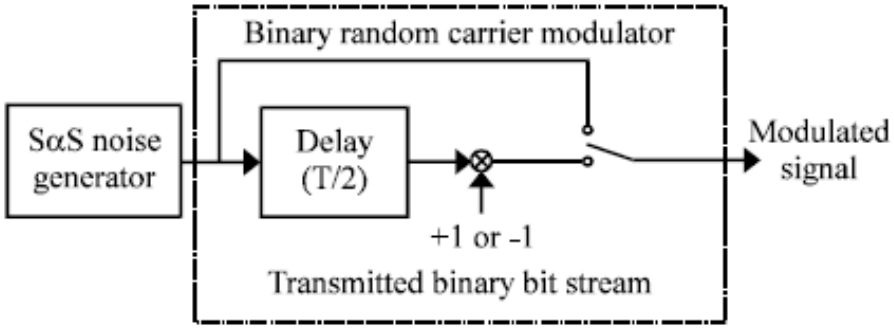

Figure 2.16 Block diagram of SαS-DSK transmitter (Xu et al., 2014)

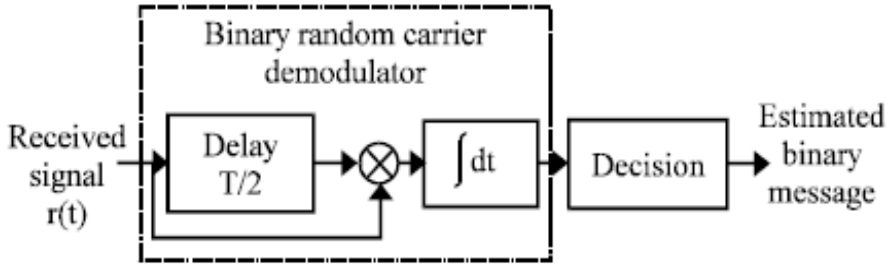

Figure 2.17 Block diagram of SαS-DSK receiver (Xu et al., 2014)

Instead of transmitting single message bit, SαS-DSK method is extended to carry more than one message bit and the enhanced communication scheme is called M-ary SαS-DSK as seen in Figure 2.18 and Figure 2.19. The receiver structure is identical to the SαS-DSK for single bit. At the receiver, the received signal is divided into two parts and the sign of the covariation evaluated. This procedure is repeated iteratively for a number of bits for each symbol. The bit error rate performance of the system improves if the impulsiveness of the information carrying signal increases; i.e., the characteristic exponent decreases. The performance also depends on the number of bits per symbol or bit duration, if the symbol carries increased number of bits, the error performance decreases, as expected.

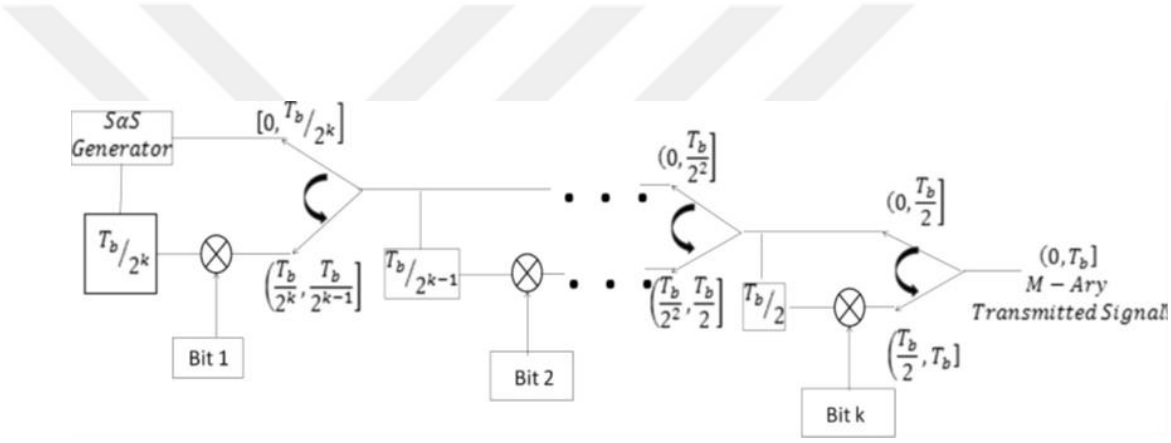

Figure 2.18 Block diagram of M-ary SαS-DSK transmitter (Çek, 2015b)

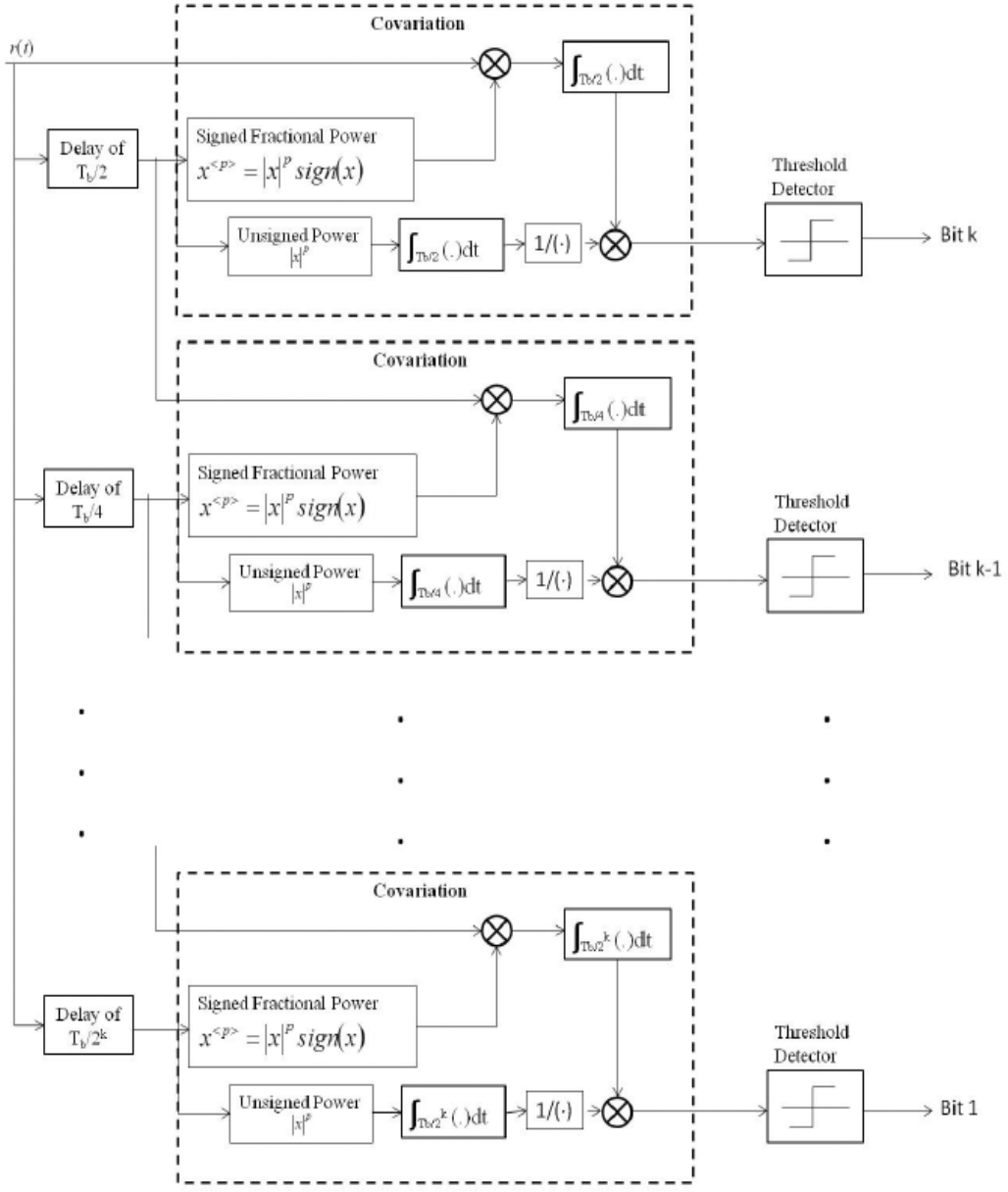

Figure 2.19 Block diagram of M-ary SαS-DSK receiver (Çek, 2015b)

2.3.3 Other Random Communication Studies

In all RCS methods mentioned so far, perfect synchronization is assumed. It is shown that imperfect synchronization causes severe declines in performance of RCSs (Ahmed & Savacı, 2017b). Therefore, Fractional Lower Order Covariance based Correlators (FLOCCs) method is suggested for the RCSs synchronization in the article of (Ahmed & Savacı, 2017a). In addition, α-stable distributions do not involve

the second-order and higher order moments. So that, time delay estimation methods such as correlation and covariance, cannot be utilised for the synchronization of RCS. As a result, FLOCC method is applied as a new measure for correlation between α-stable noise signals firstly (Ma & Nikias, 1996). Moreover, FLOCC technique is applied in the receiver part of α-stable noise based communication system (Çek, 2015a). Ultimately, the effect of fractional powers are analysed in calculation of Fractional Lower-Order Auto-Covariance (FLOAC) of SαS noise signals (Ahmed, Savacı, Wahdan & Othman, 2019).

CHAPTER THREE
PROPOSED COVERT COMMUNICATION USING RANDOM PULSE WIDTH MODULATION

In this novel proposed RPWM based secure communication system, the positive and negative durations of the baseband rectangular waveform vary randomly according to the prescribed probability density. The binary information is determined from the statistics obtained by the positive and negative residence times. The baseband waveform is expressed by antipodal rectangular signal. Since the duration of rectangular waveform cannot be lower than zero, the probability distribution is chosen from family where the minimum and maximum value of the random numbers can be adjusted by the transmitter. The receiver determines first or second moments such as mean value and variance to estimate the transmitted message bit even the exact information of the probability distribution is not known by the receiver. A proper selection of the probability distribution is the uniform distribution.

The proposed random communication system applies two approaches in order to construct the transmitter. In the first approach, the transmitted message is determined by the sign of the difference of the mean values obtained from positive and negative pulse durations where the variance is kept fixed. This method is called “Fixed-Variance RPWM”. In the second approach the transmitted message is determined by the same way using variance while the mean value is kept to be fixed. It is called “Fixed-Mean RPWM”. In the next subsections, the mathematical models of Fixed-Variance and Fixed-Mean RPWM methods are described.

3.1 Fixed-Variance RPWM

3.1.1 Transmitter Structure

The transmitter is formed by two vectors $\mathbf{s}_\mu^+$ and $\mathbf{s}_\mu^-$ holding the sequences of residence times for positive and negative states, respectively. The baseband binary information representing one-bit data is sent from the transmitter determined by positive and negative durations given by Equations (3.1) and (3.2), respectively, (Akcan & Çek, 2019).

$$\mathbf{s}_\mu^+ = \begin{bmatrix} s_{\mu_1}^+ & \cdots & s_{\mu_i}^+ & \cdots & s_{\mu_C}^+ \end{bmatrix} \tag{3.1}$$

$$\mathbf{s}_\mu^- = \begin{bmatrix} s_{\mu_1}^- & \cdots & s_{\mu_i}^- & \cdots & s_{\mu_C}^- \end{bmatrix} \tag{3.2}$$

Each of the vectors given above has length C where each element of these random vectors are derived from the uniform distribution denoted by $\mathcal{U}(\cdot)$. Each ith element is statistically defined by $s_{\mu_i}^+ \sim \mathcal{U}(\mu^+, \sigma^2)$ and $s_{\mu_i}^- \sim \mathcal{U}(\mu^-, \sigma^2)$ distributions, respectively, in terms of mean values of positive states μ^+ and negative states $\mu^-$and a fixed variance σ^2. When binary message sign is "$g = +1$", the distributions are tuned to yield $\mu^+ > \mu^-$, and if "$g = -1$", the mean values become $\mu^+ < \mu^-$. In order to assess the number of samples in a particular rectangular pulse, each $s_{\mu_i}^+$ and $s_{\mu_i}^-$ components are rounded to their nearest integer values and new variables are expressed as $\lfloor s_{\mu_i}^+ \rfloor$ and $\lfloor s_{\mu_i}^- \rfloor$, respectively. Thus, the total length of the rectangular wave becomes $K_\mu = \sum_i^C \lfloor s_{\mu_i}^+ \rfloor + \sum_i^C \lfloor s_{\mu_i}^- \rfloor$. The number of required samples in terms of the sampling period T_s and the message bit length T_b is $N = \frac{T_b}{T_s}$. Since K_μ is random and takes different values for each realization, there should be an additional residual vector $\mathbf{1}_{N-K_\mu}$ having a length of $N - K_\mu$ samples to maintain the number of samples for each message bit to be fixed which acts as buffer state (Akcan & Çek, 2019). The resultant vector to be transmitted is expressed as in Equation (3.3).

$$\mathbf{s} = \begin{bmatrix} 1_{\lfloor s_{\mu_1}^+ \rfloor} & -1_{\lfloor s_{\mu_1}^- \rfloor} & \cdots & 1_{\lfloor s_{\mu_N}^+ \rfloor} & -1_{s_{\mu_N}^-} & 1_{N-K_\mu} \end{bmatrix} \tag{3.3}$$

An illustrative example of the random pulse width modulated waveform for the message bits "+1" and "-1" are shown in Figure 3.1 (a) and Figure 3.1 (b), respectively.

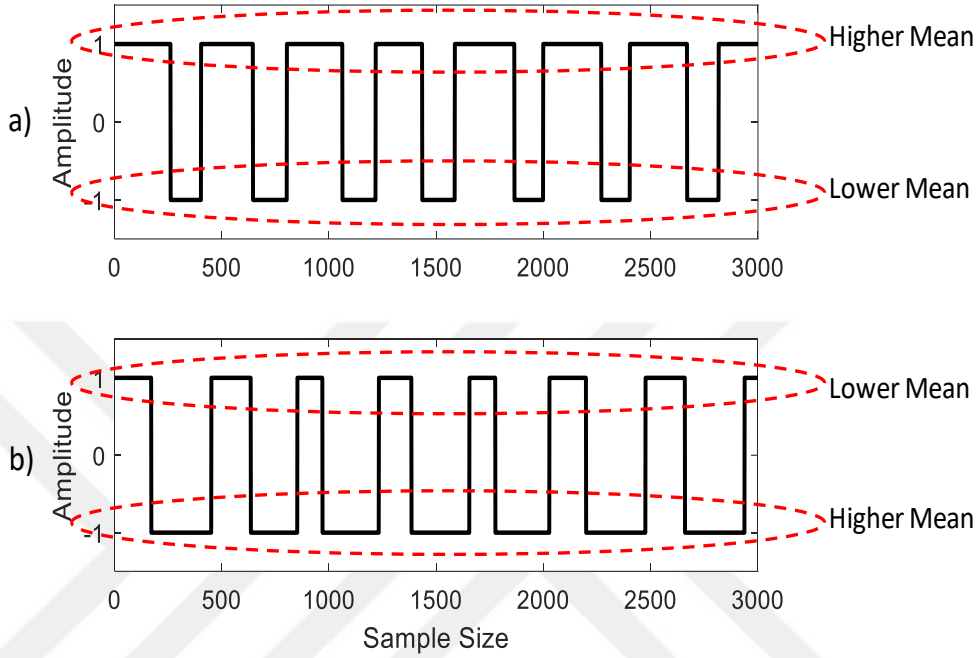

Figure 3.1 Random pulse width modulated waveform with N = 3000 samples: a) Message "+1" for $\mu^{+} = 250$, $\mu^{-} = 150$, $\sigma^{2} = 20$ b) Message "-1" for $\mu^{+} = 150$, $\mu^{-} = 250$, $\sigma^{2} = 20$

3.1.2 Receiver Structure

The receiver holds the lengths of the positive and negative values of the incoming signal and then detects the message signal g sent from the encoded signal by the statistical analysis (Akcan & Çek, 2019). Theoretically, the process performed at the receiver is expressed by Equation (3.4).

$$g = sgn\,(\mu^{+} - \mu^{-}) \tag{3.4}$$

The function $sgn(\cdot)$ is expressed as in Equation (3.5).

$$sgn(x) = \begin{cases} +1, & x \geq 0 \\ -1, & x < 0 \end{cases} \tag{3.5}$$

The predicted message bit, indicated as $\hat{g}$ from the transmitted proposed spread-spectrum waveform, can be found as in Equation (3.6).

$$\hat{g} = sgn\left(\sum_{i}^{C} \lfloor s_{\mu_i}^{+} \rfloor - \sum_{i}^{C} \lfloor s_{\mu_i}^{-} \rfloor\right) \tag{3.6}$$

3.2 Fixed-Mean RPWM

3.2.1 Transmitter Structure

The transmitter is formed by two vectors $\mathbf{s}_{\sigma}^{+}$ and $\mathbf{s}_{\sigma}^{-}$ holding the sequence of residence times for positive and negative states, respectively. The baseband binary information representing one-bit data is sent from the transmitter determined by positive and negative durations given by Equations (3.7) and (3.8), respectively.

$$\mathbf{s}_{\sigma}^{+} = \begin{bmatrix} s_{\sigma_1}^{+} & \cdots & s_{\sigma_i}^{+} & \cdots & s_{\sigma_C}^{+} \end{bmatrix} \tag{3.7}$$

$$\mathbf{s}_{\sigma}^{-} = \begin{bmatrix} s_{\sigma_1}^{-} & \cdots & s_{\sigma_i}^{-} & \cdots & s_{\sigma_C}^{-} \end{bmatrix} \tag{3.8}$$

As in the previous method, both of the vectors given above have a length C where each element of these random vectors are derived from the uniform distribution denoted by $\mathcal{U}(\cdot)$. Each ith element is statistically defined by $s_{\sigma_i}^{+} \sim \mathcal{U}(\mu, \sigma_{+}^{2})$ and $s_{\sigma_i}^{-} \sim \mathcal{U}(\mu, \sigma_{-}^{2})$ distributions, respectively, in terms of fixed-mean value μ and variances of positive states σ_{+}^{2} and negative states σ_{-}^{2}. When binary message sign is "$g = +1$", the distributions are tuned to yield $\sigma_{+}^{2} > \sigma_{-}^{2}$, and if "$g = -1$", the average values become $\sigma_{+}^{2} < \sigma_{-}^{2}$. In order to assess the number of samples in a particular rectangular pulse, each $s_{\sigma_i}^{+}$ and $s_{\sigma_i}^{-}$ components are rounded to their nearest integer values and new variables are expressed as $\lfloor s_{\sigma_i}^{+} \rfloor$ and $\lfloor s_{\sigma_i}^{-} \rfloor$, respectively. The total length of the rectangular wave becomes $K_{\sigma} = \sum_{i}^{C} \lfloor s_{\sigma_i}^{+} \rfloor + \sum_{i}^{C} \lfloor s_{\sigma_i}^{-} \rfloor$. The number of

required samples in terms of the sampling period T_s and the message bit length T_b is $N = \frac{T_b}{T_s}$. Since K_σ is random and takes different values for each realization, there should be an additional vector $\mathbf{1}_{N-K_\sigma}$ having a length of $N - K_\sigma$ samples to maintain the number of samples for each message bit to be fixed which acts as buffer state. The resultant vector to be transmitted is expressed as in Equation (3.9).

$$\boldsymbol{s} = \left[1_{\lfloor s_{\sigma_1}^{+} \rfloor} \quad -1_{\lfloor s_{\sigma_1}^{-} \rfloor} \quad \cdots \quad 1_{\lfloor s_{\sigma_N}^{+} \rfloor} \quad -1_{s_{\sigma_N}^{-}} \quad 1_{N-K_\sigma}\right] \tag{3.9}$$

An illustrative example of the random pulse width modulated waveform for the message bits "+1" and "-1" are shown in Figure 3.2 (a) and Figure 3.2 (b) respectively.

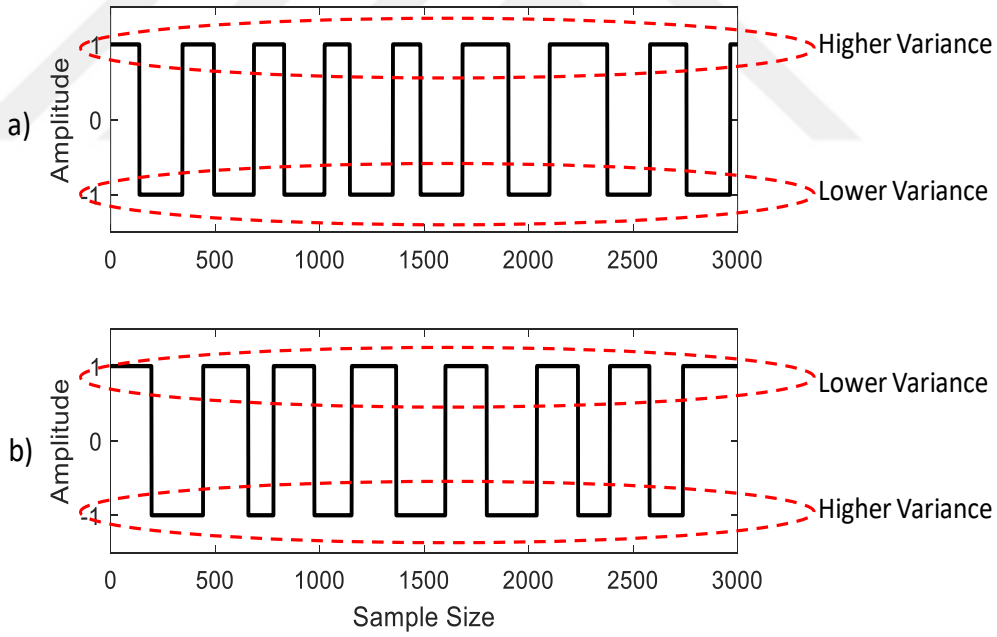

Figure 3.2 Random pulse width modulated waveform with N = 3000 samples: a) Message "+1" for $\sigma_+^2 = 50,\ \sigma_-^2 = 10, \mu = 200$, b) Message "-1" for $\sigma_+^2 = 10,\ \sigma_-^2 = 50, \mu = 200$

3.2.2 Receiver Structure

The receiver holds the lengths of the positive and negative values of the incoming signal and then detects the message signal g sent from the encoded signal by the second order statistical analysis to obtain variance. Theoretically, the process performed at the receiver is expressed by Equation (3.10).

$$g = sgn\left(\sigma_{+}^{2} - \sigma_{-}^{2}\right) \tag{3.10}$$

The predicted message bit, indicated by $\hat{g}$ from the transmitted proposed spread-spectrum waveform, can be found as in Equation (3.11).

$$\hat{g} = sgn\left(\sum_{i}^{C} \lfloor s_{\sigma_i}^{+} \rfloor - \sum_{i}^{C} \lfloor s_{\sigma_i}^{-} \rfloor\right) \tag{3.11}$$

3.3 Correlation Analysis

Since the major aim is to provide secure communication in physical layer, one question is about the degree of predictability of the RPWM based communication system. In order to observe the noise-like behaviour of the proposed method, autocorrelation and triple correlation function (TCF) are used in the literature. As the worst case scenario, it may be assumed that the same message bit is transmitted for several times and the correlation analysis gives same clue about the existence of potential periodic behaviour of the proposed method (Akcan & Çek, 2019).

3.3.1 Fixed-Variance RPWM Correlation Analysis

Correspondingly, a vector $\boldsymbol{y}$ obtained by augmentation of RPWM data stream $\boldsymbol{s}$ generated from independently identically distributed uniform random variables for each realization is expressed by (3.12).

$$\boldsymbol{y} = [\boldsymbol{s} \quad \cdots \quad \boldsymbol{s}] \tag{3.12}$$

Figure 3.3 illustrates a particular realization of the RPWM signal corresponding to vector $\boldsymbol{y}$ in time domain generated from independent $\boldsymbol{s}$ vectors corresponding to binary message sequence $\mathrm{g} = [1 \quad 1 \quad 1 \quad 1]$.

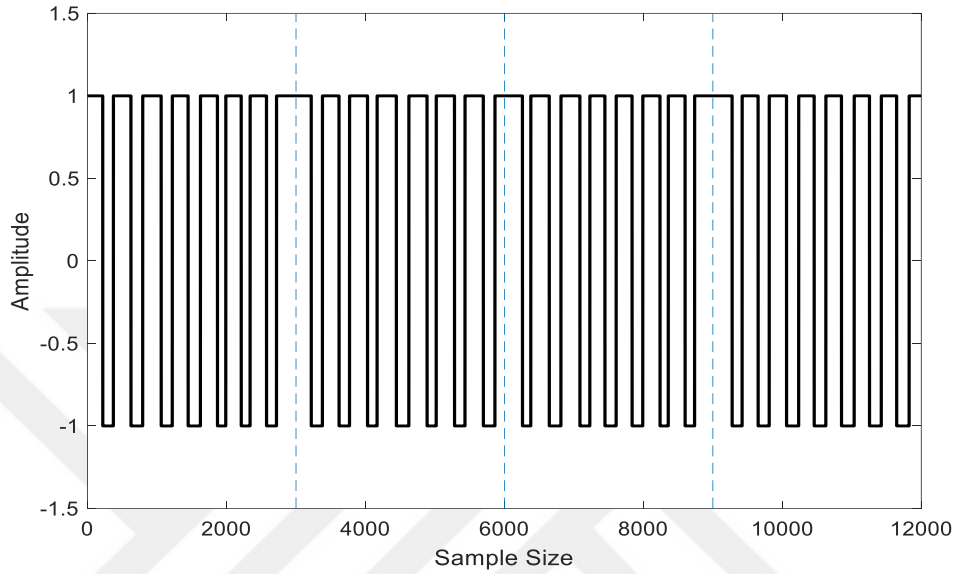

Figure 3.3 Fixed-variance RPWM signal on the transmitter for repetitive message "+1" ($\mu^{+} = 250$, $\mu^{-} = 150, \sigma^{2} = 20$)

The autocorrelation function $R_{yy}(\cdot)$ obtained from the vector $\mathbf{y}$ is described within a certain time delay in Equation (3.13) by (Stoica & Moses, 2005).

$$R_{yy}(k) = \frac{1}{P - |k|} \sum_{i=0}^{P-k-1} y[i+k]y[i] \tag{3.13}$$

It is apparent that $R_{yy}(k)$ is determined with respect to P and time delay k. Figure 3.4 illustrates the auto-correlation function as the ensemble average of 100 realizations.

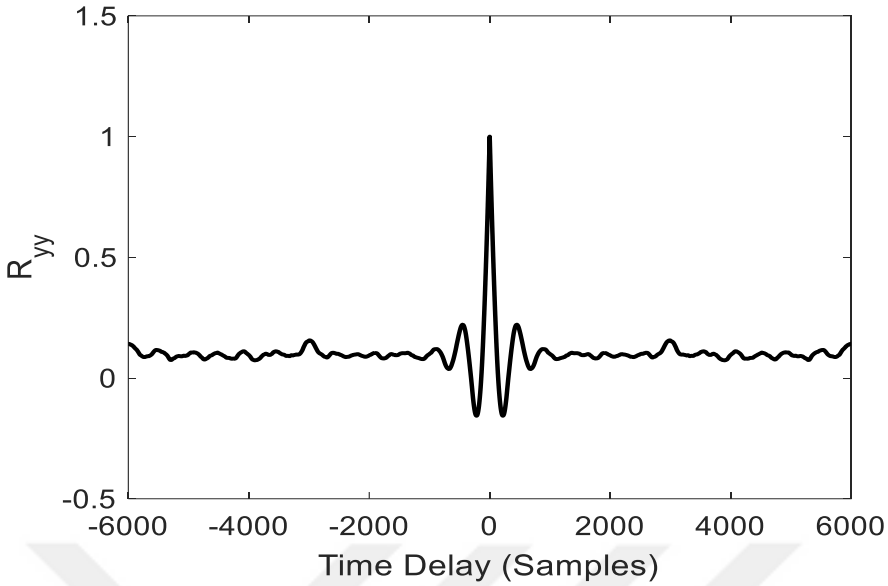

Figure 3.4 Autocorrelation function of fixed-variance RPWM signal ($\mu^+ = 250$, $\mu^- = 150$, $\sigma^2 = 80$)

Accordingly, it is seen that the received RPWM signal exhibits autocorrelation behaviour almost identical with pure noise even if the binary data stream having same message bits and corresponding signal is transmitted repetitively. Another approach is based on higher order correlation TCF and is expressed in Equation (3.14) for the vector **y**.

$$R_{yyy}(k,r) = \frac{1}{P}\sum_{i=0}^{P} y[i]y[i+k]y[i+r] \tag{3.14}$$

TCF can be considered as the measure of correlation in terms of two different time delay variables. The existence of potential periodic correlation variation arises as positive and negative peak values and corresponding periodic patterns in two dimensions. Figure 3.5 and Figure 3.6 illustrate the TCF obtained from RPWM signals of the vector **y** for lower variance ($\sigma^2 = 10$) and higher variance ($\sigma^2 = 60$), respectively. It is indicated that, selection of lower variance results in more periodic rectangular waveform which offers less security. TCF plot shown in Figure 3.5 gives rough information about mean value of the period of the rectangular signal. An increase on the variance of the RPWM signal, as shown in Figure 3.6, causes a TCF result with a periodic pattern that is hard to be detect. Therefore, one can consider

designing a RPWM system by taking into account the fact that the security aspect strongly depends on the selection of the variance to be sufficiently large.

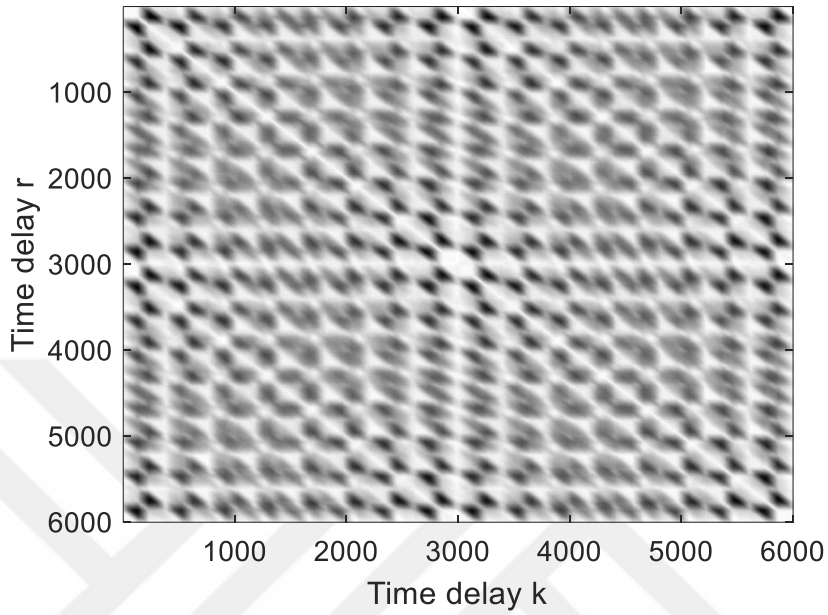

Figure 3.5 Triple correlation function of the fixed-variance RPWM signal for $\mu^+ = 250$, $\mu^- = 150$, $\sigma^2 = 10$

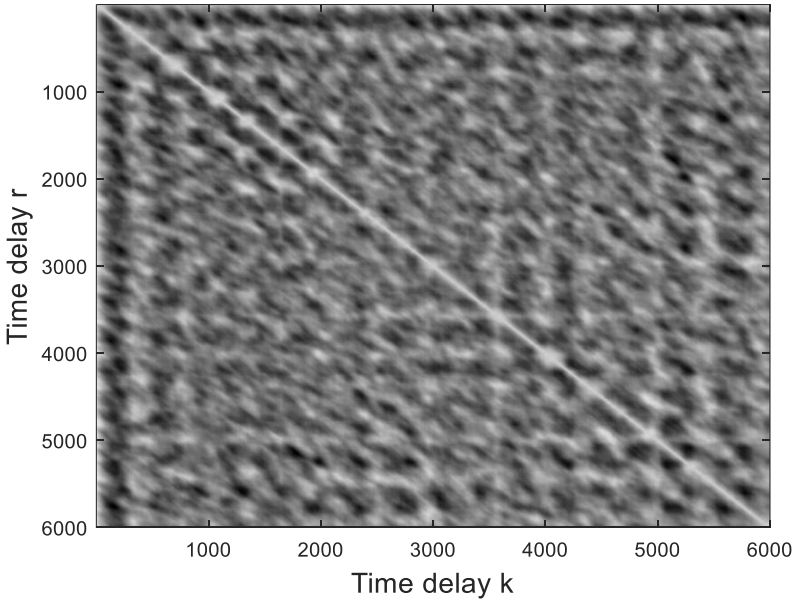

Figure 3.6 Triple correlation function of the fixed-variance RPWM signal for $\mu^+ = 250$, $\mu^- = 150$, $\sigma^2 = 60$

3.3.2 Fixed-Mean RPWM Correlation Analysis

In this approach, the correlation analysis is performed for the RPWM signal where the mean value is kept fixed while the binary data is encoded by the variances of the positive and negative residence times. In order to construct repetitive data as in Section 3.3.1, a vector $\boldsymbol{y}$ is obtained by augmentation of RPWM data stream $\boldsymbol{s}$ generated from independently and identically distributed uniform random variables for each realization as given in Equation (3.15).

$$\boldsymbol{y} = [\boldsymbol{s} \quad \cdots \quad \boldsymbol{s}] \tag{3.15}$$

Figure 3.7 illustrates the $\boldsymbol{y}$ vector that is generated from $\boldsymbol{s}$ vectors representing binary message sequence $\mathrm{g} = [1 \quad 1 \quad 1 \quad 1]$ as the resultant RPWM signal is constructed.

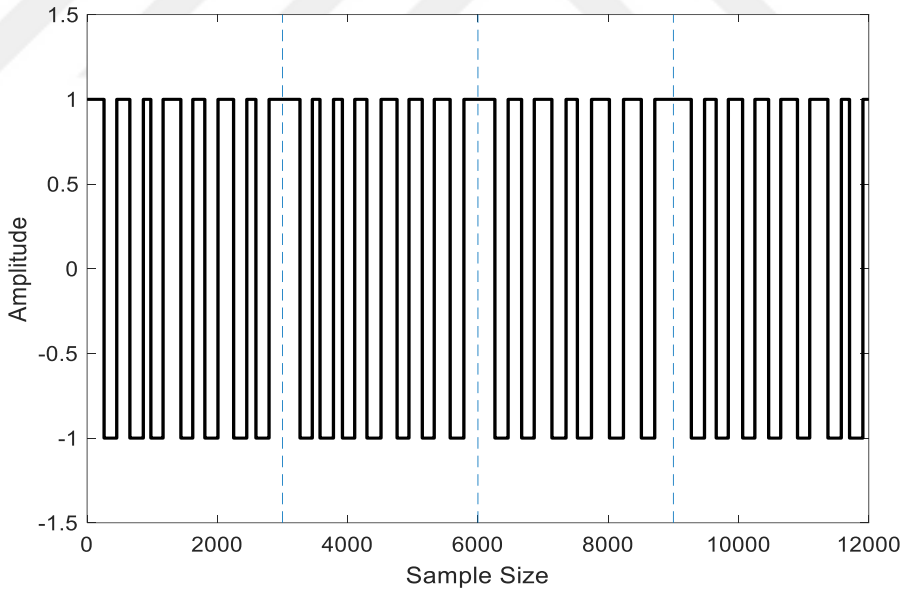

Figure 3.7 Fixed-mean RPWM signal on the transmitter for repetitive message "+1" ($\sigma_+^2 = 50$, $\sigma_-^2 = 10$, $\mu = 200$)

The autocorrelation function $R_{yy}(\cdot)$ is described again with respect to the transmitted signal for the vector $\mathbf{y}$ for the second approach. Figure 3.8 illustrates the average autocorrelation function as the ensemble average of 100 realizations.

Accordingly, it is seen that the received RPWM signal shows autocorrelation behaviour similar to noise even if the same message bit stream and corresponding signal is transmitted repetitively. An increase on the variances to model positive and negative residence times would yield more random behaviour.

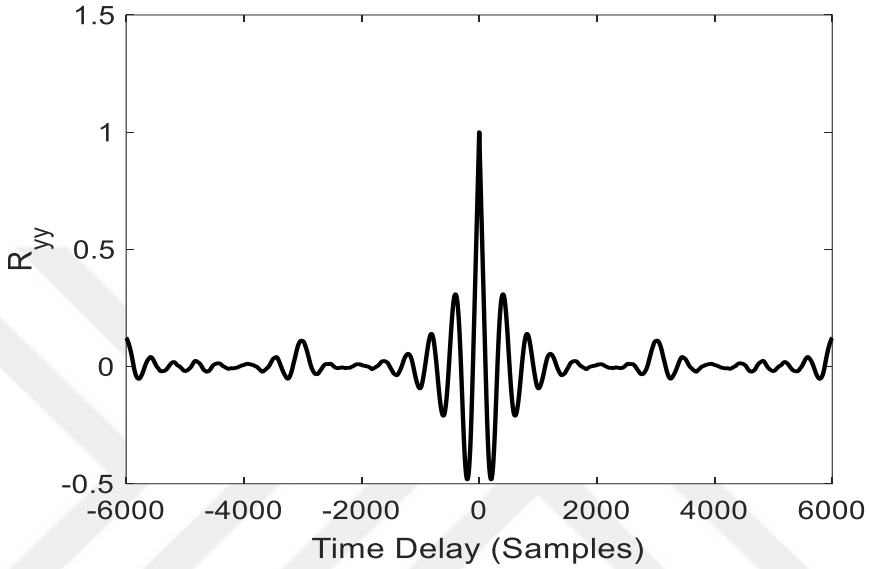

Figure 3.8 Autocorrelation function of fixed-mean RPWM signal ($\sigma_+^2 = 60$, $\sigma_-^2 = 40$, $\mu = 200$)

Another approach is to evaluate the TCF again for the vector $\mathbf{y}$. Figure 3.9 and Figure 3.10 show the TCF obtained from RPWM signals for different selections of variances when the mean value is kept fixed ($\mu = 200$). It is indicated that, selection of low variance results in more periodic rectangular waveform which offers less security. TCF plot shown in Figure 3.9 gives rough information about mean value of the period of the rectangular signal. An increase on the variance of the RPWM signal shown in Figure 3.10, causes a TCF result where it is more difficult to detect a periodic pattern. Therefore, one can consider designing a RPWM system by taking into account that the security aspect strongly depends on the selection of the variance to be sufficiently large.

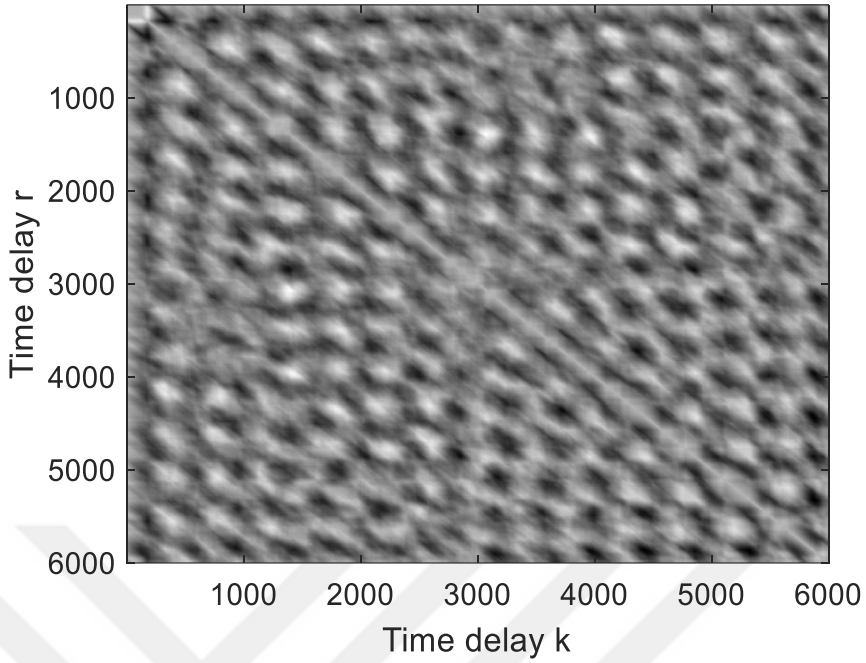

Figure 3.9 Triple correlation function of the fixed-mean RPWM signal for $\sigma_+^2 = 50$, $\sigma_-^2 = 10$, $\mu = 200$

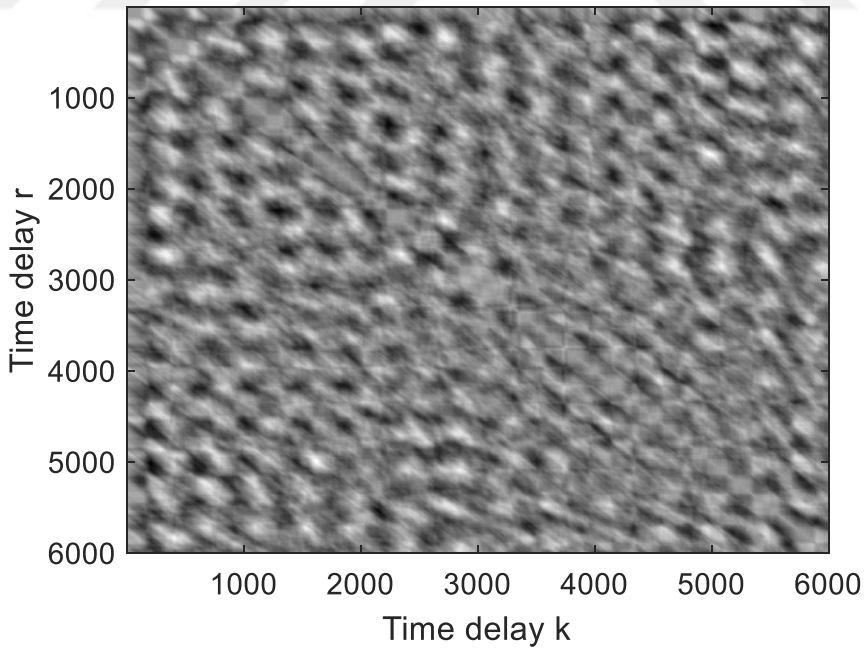

Figure 3.10 Triple correlation function of the fixed-mean RPWM signal for $\sigma_+^2 = 40$, $\sigma_-^2 = 20$, $\mu = 200$

3.4 Bit Error Rate (BER) Analysis

The error performance of the proposed communication system is determined under additive white Gaussian noise (AWGN) channel assumption. Signal to noise ratio (SNR) is expressed as in Equation (3.16):

$$SNR\ (dB) = 10\log\frac{\sum_{n=1}^{N} s^2[n]}{2{\sigma_G}^2} \tag{3.16}$$

where $\boldsymbol{\sigma_G}^{\boldsymbol{2}}$ is the variance of the additive white Gaussian noise. Since the channel noise can cause unwanted zero crossings and occurring spurious state transitions, the residence times can be determined incorrectly under the noise without any post-processing at the receiver. In order to eliminate the noise effect to maintain the residence times to keep unchanged a moving average filtering is a proper way to smooth the received signal before sending to decision device. Depending on the length of filter W, the received signal is modified as given in Equation (3.17). As an illustration, the filtered signal at the receiver is plotted in Figure 3.11.

$$\hat{r}[n] = \frac{1}{W}\sum_{i=-W/2}^{W/2} r[n+i] \tag{3.17}$$

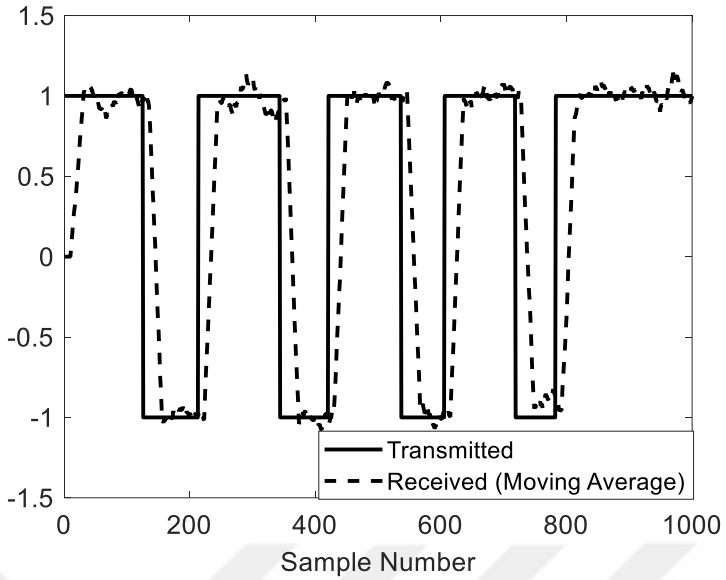

Figure 3.11 Received signal after moving average filter is applied to fixed-variance RPWM signal for $\mu^{+} = 120,\ \mu^{-} = 80,\ T_b = 1000, W = 20,\ SNR = 10dB$

A Monte Carlo computer simulation is performed on Matlab environment. The number of random message bits is $\mathbf{10^3}$ and the results are determined by ensemble averaging of 5 realizations. The results depending on the selection of different variance values for fixed variance RPWM method are shown in Figure 3.12. It is observed that the selection of lower variance provides two distributions not to overlap with each other and the message bits are determined without a distortion. However, choosing increased variance provides enhanced security with respect to the triple correlation results. Hence, one can say that there is a tradeoff between security and error performance.

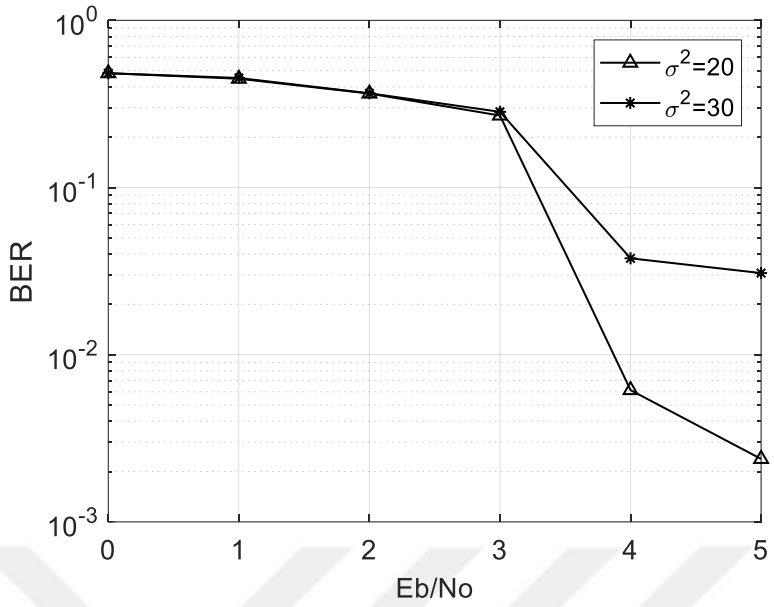

Figure 3.12 BER performance of fixed-variance RPWM signal for $\mu^+ = 120,\ \mu^- = 80,\ T_b = 1000$

As the second the method, variance is used to encode the message bit and BER analysis is performed for two fixed-mean value to show the effect of selection of mean value. The BER results are shown in Figure 3.13

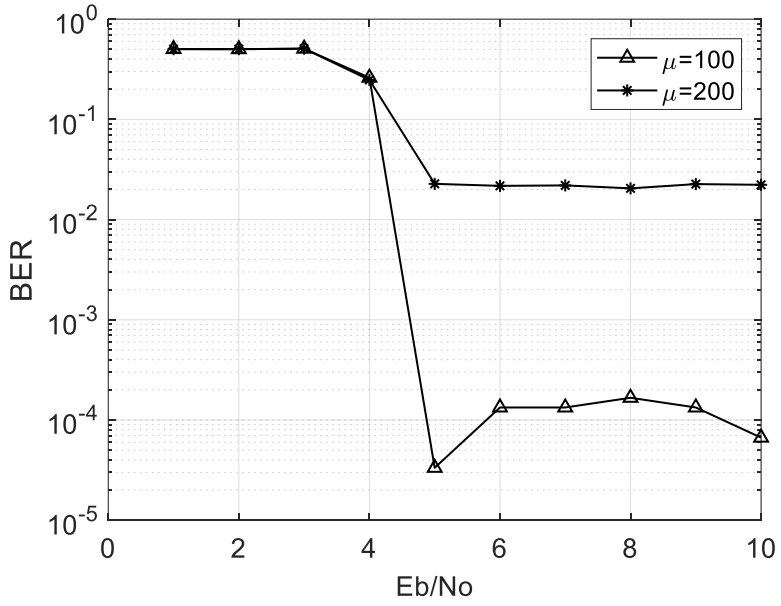

Figure 3.13 BER performance of fixed-mean RPWM signal for $\sigma_+^2 = 40, \sigma_-^2 = 10, T_b = 2000$

It can be seen that increased mean within a constant bit duration yields reduced random residence time vector and the receiver is able to utilize less data to determine the message bit from the statistics obtained from estimated positive and residence time variances. Although the SNR is increased, the receiver can mistakenly determine the message bit and a saturation structure is observed. Therefore the amount of information obtained from residence times should be sufficiently provided and the statistical values and threshold should be improved as the future study.

CHAPTER FOUR
CONCLUSION

In this thesis study, a novel direct sequence spread-spectrum communication is proposed by using “Random Pulse Width Modulation” or equivalently “Random Pulse Duration Modulation” method. The reason of constructing such a spread-spectrum communication system arises from the limited covertness ability of conventional DSSS communication systems due to periodic behaviour of PN sequences for each message bit.

Instead of generating PN sequence, the proposed method builds a rectangular pulse train whose pulse durations vary randomly according to a prescribed probability density function. The security aspect of the proposed method relies on the random behaviour of residence time of the positive and negative states of binary a non-return-to-zero (NRZ) signal. Since the pulse duration cannot be negative inherently, uniform distribution whose minimum and maximum values can be tuned by the transmitter in a finite interval, is considered to be an appropriate selection for pdf to encode the binary message. Noting that the pulse durations in discrete time correspond to certain integer values, the generated random values from uniform distribution are rounded to their nearest integer values. The non-coherent receiver determines the message by formulating the extracted information obtained. This may be achieved by comparing the mean values of the residence times of the positive and negative state durations having a fixed variance. Alternatively, variance variations are utilized to determine the message bit for fixed mean value.

There are critical points which affect the design of this communication system. Firstly, it is observed that higher variance selection for fixed-variance RPWM yields improved security performance. Likewise, it is observed that selection of higher values of varying variances for each positive and negative states enhance the security performance of the communication system independent from the value of fixed mean. The second point is the error probability of the proposed system. Since the channel noise directly causes the unwanted state changes, a moving average filter

based integrator acts as error corrector on received signal and improves the bit error rate performance so that the RPWM based system can be practically implementable. It should be taken into account that an increase on the variance of the residence times for positive and negative states yields increased security. However, it also causes an increase on potential overlap between the probability density functions for each state and causes decreased error performance. The development of optimal parameter selection to provide satisfactory error performance and the security constitute future challenges of this newly proposed random spread-spectrum communication method.

REFERENCES

Ahmed, A., & Savacı, F. A. (2017a). Random communication system based on skewed alpha-stable levy noise shift keying. *Fluctuation and Noise Letters, 16* (03), 1-10.

Ahmed, A., & Savacı, F. A. (2017b). Measure of covertness based on the imperfect synchronization of an eavesdropper in random communication systems. *10th International Conference on Electrical and Electronics Engineering (ELECO),* Bursa Turkey, Nov, 638 – 641.

Ahmed, A., & Savacı, F. A. (2018a). Synchronization of alpha-stable levy noise-based random communication system. *IET Communications, 12* (3), 276–282.

Ahmed, A., & Savacı, F. A. (2018b). On optimizing fractional lower order covariance based synchronization method for random communication systems. *26th Signal Processing and Communications Applications Conference (SIU),* 1-4.

Ahmed A., Savacı F. A., Wahdan M., & Othman H. (2019). Role of fractional powers in maneuvering the fractional lower-order auto-covariance of skewed alpha-stable signals in Gaussian noise environment. *Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT),* Istanbul, Turkey, 1- 4.

Akcan G., & Çek M. E. (2019). Direct sequence spread-spectrum based covert communication using random pulse width modulation. *27th Signal Processing and Communications Applications Conference (SIU),* Sivas, Turkey, 1-4.

Bash, B. A., Goeckel, D., & Towsley, D. (2013). Limits of reliable communication with low probability of detection on AWGN channels. *IEEE Journal on Selected Areas in Communications, 31* (9), 1921–1930.

Bash, B. A., Goeckel, D., Towsley, D., & Guha, S. (2015). Hiding information in noise: Fundamental limits of covert wireless communication. *IEEE Communications Magazine.* Retrieved April 25, 2019, from https://doi.org/10.1109/MCOM.2015.7355562

Billa, R., Sharma, P., & Ashraf, J. (2012). Analysis of chirp spread spectrum system for multiple access. *International Journal of Engineering Research & Technology (IJERT), 1* (3), 1–9.

Bloch, M. R. (2016). Covert communication over noisy channels: A resolvability perspective. *IEEE Transactions on Information Theory*, *62* (5), 2334–2354.

Bouder, C., Azou, S., & Burel, G. (2004). Performance analysis of a spreading sequence estimator for spread spectrum transmissions. *Journal of the Franklin Institute*, *341* (7), 595–614.

Burel, G. (2000). Detection of spread spectrum transmissions using fluctuations of correlation estimators. *IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS'2000), 11*(4), Honolulu, Hawaii, USA.

Burel, G., & Bouder, C. (2000). Blind estimation of the pseudo-random sequence of a direct sequence spread spectrum signal. *MILCOM 2000 Proceedings 21st Century Military Communications. Architectures and Technologies for Information Superiority*, *2*, 967–970.

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

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

Cassola, A., Jin, T., Noubir, G., & Thapa, B. (2013). Efficient spread spectrum communication without preshared secrets. *IEEE Transactions on Mobile Computing*, *12* (8), 1669–1680.

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

Çek, M. E. (2010). *Chaotic modulation and alpha-stable noise parameter modulation methods in spread spectrum communication*. PhD Thesis, Dokuz Eylül University, İzmir.

Çek, M. E. (2015a). Covert communication using skewed α-stable distributions. *Electronics Letters, 51* (1), 116–118.

Çek, M. E. (2015b). M-ary alpha-stable noise modulation in spread-spectrum communication. *Fluctuation and Noise Letters*, *14* (03), 1-10.

Che, P. H., Bakshi, M., & Jaggi, S. (2013). Reliable deniable communication: Hiding messages in noise. *IEEE International Symposium on Information Theory - Proceedings*, 2945–2949.

Che, P. H., Kadhe, S., Bakshi, M., Chan, C., Jaggi, S., & Sprintson, A. (2014a). Reliable, deniable and hidable communication: A quick survey. *2014 IEEE Information Theory Workshop (ITW)*, 227–231.

Che, P. H., Bakshi, M., Chan, C., & Jaggi, S. (2014b). Reliable deniable communication with channel uncertainty. *2014 IEEE Information Theory Workshop (ITW)*, 30–34.

Chen, S., Yang, Q., & Wang, C. (2004). Impulsive control and synchronization of unified chaotic system. *Chaos, Solitons and Fractals, 20* (4), 751–758.

Chen, M., & Min, W. (2008). Unknown input observer based chaotic secure communication. *Physics Letters, Section A: General, Atomic and Solid State Physics, 372* (10), 1595–1600.

Çiçek, S., Kocamaz, U. E., & Uyaroğlu, Y. (2018). Secure communication with a chaotic system owning logic element. *AEU - International Journal of Electronics and Communications, 88*, 52–62.

Cook C. E., (1974). Linear FM signal formats for beacon and communication systems. *IEEE Transactions on Aerospace and Electronic Systems, 10* (4), 471-478.

Cuomo, K. M. & Oppenheim, A. V., (1993). Circuit implementation of synchronized chaos with applications to communications. *Physical Review Letters, 71* (1), 65–68.

Dedieu H., Kennedy M. P., & Hasler M. (1993). Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit. *IEEE Trans. Circuits Systems Part II, 40* (10), 634–642.

Duan, J.-Y., & Yang, H. (2018). Phase-orthogonality CDSK: A reliable and effective chaotic communication scheme. *IET Communications, 12* (9), 1116–1122.

Fang, Y., Han, G., Chen, P., Lau, F. C. M., Chen, G., & Wang, L. (2016). A survey on DCSK-based communication systems and their application to UWB scenarios. *IEEE Communications Surveys and Tutorials, 18* (3), 1804–1837.

Fazel, K., & Kaiser, S. (2008). *Multi-carrier and spread spectrum systems* (2th ed.). Singapore: John Wiley & Sons, Inc.

Forouzesh, M., Azmi, P., Mokari, N., & Wong, K. K. (2018). Covert communications versus physical layer security. *1*, 1–4. Retrieved April 30, 2019 from http://arxiv.org/abs/1803.06608v1.

Gamoudi, R., Chariag, D. E., & Sbita, L. (2018). A review of spread-spectrum based PWM techniques - a novel fast digital implementation. *IEEE Transactions on Power Electronics*, *33* (12), 10292–10307.

Gosavi, A. (2008). Application of spread-spectrum technique for EMI reduction in boost converter - a case study. *10th International Conference on Electromagnetic Interference & Compatibility*, 145-148.

Guo-Hui, L. (2005). An active control synchronization for two modified Chua circuits. *Chinese Physics*, *14* (3), 472–475.

Haghighat, A., & Soleymani, M. R. (2005). A MUSIC-based algorithm for blind user identification in multiuser DS-CDMA. *EURASIP Journal on Applied Signal Processing*, 649–657.

Haykin, S. (1994). *Communication Systems* (4th ed.). U.S. of America: John Wiley & Sons, Inc.

Hill, P. C. J., Comley, V. E., & Adams, E. R. (1997). Techniques for detecting and characterizing covert communication signals. *European Conference on Security and Detection, ECOS '97, London, UK, 1* (437), 1361–1365.

Kaddoum, G., Gagnon G., & Gagnon F. (2013). Spread spectrum communication system with sequence synchronization unit using chaotic symbolic dynamics modulation. *International Journal of Bifurcation and Chaos*, *23* (02), 1-14.

Kennedy, M. P., Kolumban, G., Kis, G., & Jakoa, Z. (2000). Performance evaluation of FM-DCSK modulation in multipath environments. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 47* (12), 1702–1711.

Khan, M. A., Rao, R. K., & Wang, X. (2013). Non-linear trigonometric and hyperbolic chirps in multiuser spread spectrum communication systems. *2013 IEEE 9th International Conference on Emerging Technologies (ICET),* 1–6.

Knapp, A., & Pap, L. (2018). A novel mobile communication system using pulse position based chirp spread-spectrum modulation. *Journal of Communications Software and Systems, 14* (3), 228–238.

Kobori, Y., Arafune, T., Tsukiji, N., Takai, N., & Kobayashi, H. (2015). Selectable notch frequencies of EMI spread spectrum using pulse modulation in switching converter. *2015 IEEE 11th International Conference on ASIC,* 1–4.

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

Kolumban, G., Vizvki, B., Schwarz, W., & Abel, A. (1996) Differential chaos shift keying: A robust coding for chaotic communication. *In Proc. 4th Int. Workshop on Nonlinear Dynamics of Electronic Systems,* Sevilla, Spain, June 27–28, 87–92.

Kolumban, G., Kis, G., Jako, Z., & Kennedy, M. P. (1997). FM-DCSK: A new and robust solution to chaos communications. *In Proc. International Symposium on Nonlinear Theory and its Applications*, Honolulu, HI, USA, Nov. 29–Dec. 2, 117–120.

Kolumban, G., Kennedy, M. P., & Chua, L. O. (1998). The role of synchronization in digital communications using chaos-Part II: Chaotic modulation and chaotic synchronization. *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, 45* (11), 1129–1140.

Kopp, C. (2005). *An introduction to spread-spectrum techniques*. Retrieved April 20, 2019 from http://www.ausairpower.net/OSR-0597.html

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

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

Lau, F. C. M., & Tse, C. K. (2003). *Chaos-based digital communication systems*. Berlin – Germany: Springer-Verlag.

Lee, S., & Baxley, R. J. (2014). Achieving positive rate with undetectable communication over AWGN and Rayleigh channels. *2014 IEEE International Conference on Communications (ICC)*, 780–785.

Lee, S., Baxley, R. J., Weitnauer, M. A., & Walkenhorst, B. (2015). Achieving undetectable communication. *IEEE Journal on Selected Topics in Signal Processing*, *9* (7), 1195–1205.

Leon, D., Balkir, S., Hoffman, M. W., & Perez, L. C. (2004). Pseudo-chaotic PN-sequence generator circuits for spread spectrum communications. *IEE Proceedings - Circuits, Devices and Systems, 151* (6), 543–550.

Li, S., Álvarez, G., & Chen, G. (2005). Breaking a chaos-based secure communication scheme designed by an improved modulation method. *Chaos, Solitons and Fractals, 25* (1), 109–120.

Li, D., Wang, Z., Zhou, J., Fang, J., & Ni, J. (2008). A note on chaotic synchronization of time-delay secure communication systems. *Chaos, Solitons and Fractals*, *38* (4), 1217–1224.

Liang, J.-H., Wang, X., Wang, F.-H., & Huang, Z.-T. (2017). Blind spreading sequence estimation algorithm for long-code DS-CDMA signals in asynchronous multi-user systems. *IET Signal Processing*, *11* (6), 704–710.

Ma, X., & Nikias, C. L. (1996). Joint estimation of time delay and frequency delay in impulsive noise using fractional lower order statistics. *IEEE Transactions on Signal Processing*, *44* (11), 2669–2687.

Ma, C., Zhang, L., & Liu, J. (2017). Blind estimation of spread spectrum code and information sequence of DSSS signals based on MCMC-UKF. *2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 228–234.

Mehboodi, S., Jamshidi, A., & Farhang, M. (2018). Spreading sequence estimation algorithms based on ML detector in DSSS communication systems. *IET Signal Processing*, *12* (6), 802–809.

Mihalič, F., & Kos, D. (2006). Reduced conductive EMI in switched-mode DC-DC power converters without EMI filters: PWM versus randomized PWM. *IEEE Transactions on Power Electronics, 21* (6), 1783-1794.

Min, L., Zhang, X., & Chen, G. (2005). A generalized synchronization theorem for array differential equations with application to secure communication. *International Journal of Bifurcation and Chaos, 15* (1), 119–135.

Morgül, O. (2000). An RC realization of Chua's circuit family. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 47* (9), 1424–1430.

Morgül, O., Solak, E., & Akgül M. (2003). Observer based chaotic message transmission. *International Journal of Bifurcation and Chaos, 13* (4), 1003–1017.

Narayanan, R. M. Chuang, J., & DeMay, M. W. (2008). Design, analysis, and performance of a noise modulated covert communications system. *EURASIP Journal on Wireless Communications and Networking*, 1–12.

Narayanan, R., Chuang, J., & Mohan, K. (2009). Propagation effects on noise-modulated randomly polarized ultra-wideband communication system. *IETE Technical Review, 26* (4), 303.

Oppenheim, A. V., Wornell, G. W., Isabelle, S. H., & Cuomo, K. M. (1992). Signal processing in the context of chaotic signals. 1992 *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP-92), 4*, 117-120.

Pareschi, F., Rovatti, R., & Setti, G. (2015). EMI reduction via spread spectrum in DC/DC converters: State of the art, optimization, and tradeoffs. *IEEE Access*, *3*, 2857–2874.

Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. S. & Shang, A. (2004). Transmission of digital signals by chaotic synchronization. *International Journal of Bifurcation and Chaos, 2* (3), 973–977.

Pecora, L. M., & Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical Review Letters, 64* (8), 821–824.

Pickholtz, R. L., Schilling, D. L., & Milstein, L. B. (1982). Theory of spread-spectrum communications—A tutorial. *IEEE Transactions on Communications, 30* (5), 855–884.

Qui, P.-Y., Huang, Z.-T., Jiang, W.-L., & Zhang, C. (2008). Improved blind-spreading sequence estimation algorithm for direct sequence spread spectrum signals. *IET Signal Processing, 2* (2), 139– 146.

Qui, P. Y., Huang, Z. T., Jiang, W. L., & Zhang, C. (2010). Blind multiuser spreading sequences estimation algorithm for the direct-sequence code division multiple access signals. *IET Signal Processing, 4* (5), 465.

Ren, H. P., Bai, C., Liu, J., Baptista, M. S., & Grebogi, C. (2016). Experimental validation of wireless communication with chaos. *Chaos: An Interdisciplinary Journal of Nonlinear Science, 26*(8), 1-10.

Salberg, A. B., & Hanssen, A. (1999). Secure digital communications by means of stochastic process shift keying. *Conference Record of the 33rd Asilomar Conference on Signals, Systems, and Computers, 2* (February), 1523–1527.

Salberg, A. B., & Hansen, A. (2001). Subspace detectors for stochastic process shift keying. *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, 4* (February), 2549–2552.

Samorodnitsky, G., & Taqqu, M. S., (1994). *Stable non-Gaussian random processes,* NewYork: Chapman Hall / CRC Press.

Sarcheshmeh, H. M., Bizaki, H. K. & Alizadeh, S. (2018). PN sequence blind estimation in multiuser DS-CDMA systems with multipath channels based on successive subspace scheme. *International Journal of Communication Systems, 31* (12), e3591.

Shen, B., & Wang, J. X. (2017). Chip rate and pseudo-noise sequence estimation for direct sequence spread spectrum signals", *IET Signal Processing, 11* (6), 727-733.

Shiu, Y. S., Chang, S. Y., Wu, H. C., Huang, S. C. H., & Chen, H. H. (2011). Physical layer security in wireless networks: A tutorial. *IEEE Wireless Communications, 18* (2), 66–74.

Singh, A. (2013). Performance analysis of spread-spectrum techniques. *Proceedings of Conference on Advances in Communication and Control Systems,* 683-687.

Sobers, T. V., Bash, B. A., Guha, S., Towsley, D., & Goeckel, D. (2017). Covert communication in the presence of an uninformed jammer. *IEEE Transactions on Wireless Communications, 16* (9), 6193–6206.

Solankee, L., Bhatia, K., & Khan, A. (2012). EMI reduction in switching power converter by using chaotic frequency modulation technique. *Contemporary Engineering Sciences, 5* (1), 33–47.

Stavroulakis, P. (2006). *Chaos applications in telecommunications*, Newyork: CRC Press.

Stoica, P., & Moses, R. (2005). *Spectral analysis of signals*, Upper Saddle River - New Jersey: Prentice Hall.

Sun, J., Zhang, Y., & Wu, Q. (2002). Impulsive control for the stabilization and synchronization of Lorenz systems. *Physics Letters, Section A: General, Atomic and Solid State Physics, 298* (2-3), 153–160.

Sun, K. (2016). *Chaotic secure communication: Principles and technologies*, Berlin, Germany; Boston, MA, USA: Walter de Gruyter.

Sugi, S.S.S., & Joe, V. (2015). Spread-spectrum modulation techniques using MATLAB, *International Journal of Innovative Research in Technology*, *2* (3), 47-52.

Sushchik, M., Tsimring, L. S., & Volkovskii, A. R. (2000). Performance analysis of correlation-based communication schemes utilizing chaos. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *47* (12), 1684–1691.

Swami, D. S., & Sarma, K. K. (2014). A chaos based PN sequence generator for direct-sequence spread spectrum communication system. *International Journal of Circuits, Systems and Signal Processing, 8,* 351–360.

Tahmasbi, M., & Bloch, M. R. (2018). First and second order asymptotics in covert communication. *IEEE Transactions on Information Theory, 65* (4), 2190-2212.

Tan, V. Y. F., & Lee, S. H. (2019). Time-division is optimal for covert communication over some broadcast channels. *IEEE Transactions on Information Forensics and Security, 14* (5), 1377–1389.

Vlok, J. D., & Olivier, J. C. (2012). Non-cooperative detection of weak spread-spectrum signals in additive white Gaussian noise. *IET Communications, 6* (16), 2513–2524.

Wang, R., Lin, Z., Du, J., Wu, J., & He, X. (2017). Direct sequence spread-spectrum-based PWM strategy for harmonic reduction and communication. *IEEE Transactions on Power Electronics, 32* (6), 4455–4465.

Win, M. Z., & Scholtz, R. A. (2000). Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications. *IEEE Transactions on Communications, 48* (4), 679–691.

Winkler, M. R. (1962). Chirp signals for communications. *IEEE WESCON Convention Record, 14* (2).

Xie, W., Wen, C., & Li, Z. (2000). Impulsive control for the stabilization and synchronization of Lorenz systems. *Physics Letters, Section A: General, Atomic and Solid State Physics, 275*, 67-72.

Xu, Z.-J., Gong, Y., Lu, W.-D., Wang, K., & Hua, J.-Y. (2014). A novel structure for covert communication based on alpha stable distribution. *Information Technology Journal, 13* (9), 1673–1677.

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

Xu, Z.-J., Gong, Y., Wang, K., Lu, W.-D., & Hua, J.-Y. (2017). Covert digital communication systems based on joint normal distribution. *IET Communications, 11* (8), 1282–1290.

Yan, S., He, B., Cong, Y., & Zhou, X. (2017). Covert communication with finite blocklength in AWGN channels. *IEEE International Conference on Communications*, 1–6.

Yang, T., & Chua, L. O. (1997). Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 44* (10), 976–988.

Yang T. (2001). *Impulsive control theory*. Lecture Notes in Control and Information Sciences, *272*, Berlin, Germany: Spinger-Verlag.

Yang, H., & Jiang, G. P. (2012). High-efficiency differential-chaos-shift-keying scheme for chaos-based non-coherent communication. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *59* (5), 312–316.

Yao, Y., & Poor, V. (2004). Blind detection of synchronous CDMA in non-Gaussian channels. *IEEE Transactions on Signal Processing*, *52* (1), 271–279.

Ye, L., Chen, G., & Wang, L. (2005). Essence and advantages of FM-DCSK versus conventional spread-spectrum communication methods. *Circuits, Systems, and Signal Processing*, *24* (5), 657–673.

Zhang, H. G., Gan, L., Liao, H. S., Wei, P., & Li, L. P. (2012). Estimating spreading waveform of long-code direct sequence spread spectrum signals at a low signal-to-noise ratio. *IET Signal Processing*, *6* (4), 358–363.

Zhao, Z., Shen, L., & Gu, X. (2016). Blind estimation of pseudo-random codes in periodic long code direct sequence spread spectrum signals. *IET Communications*, *10* (11), 1273–1281.

Zhao, Z., Gu, X., Qiang, F., & Shen, L. (2017). Blind estimation of PN codes in multi-user LSC-DSSS signals. *Journal of Communications*, *12* (1), 55-61.