ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

SIGNAL DETECTION AND PARAMETER ESTIMATION OF FREQUENCY HOPPING SIGNALS

M.Sc. THESIS

Batuhan KAPLAN

Department of Electronics and Communication Engineering

Telecommunication Engineering Programme

FEBRUARY 2022

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

SIGNAL DETECTION AND PARAMETER ESTIMATION OF FREQUENCY HOPPING SIGNALS

M.Sc. THESIS

Batuhan KAPLAN
(504181341)

Department of Electronics and Communication Engineering

Telecommunication Engineering Programme

Thesis Advisor: Prof. Dr. Hakan Ali ÇIRPAN

FEBRUARY 2022

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

FREKANS ATLAMALI SİNYALLERİN TESPİTİ VE PARAMETRE KESTİRİMİ

YüKSEK LİSANS TEZİ

Batuhan KAPLAN
(504181341)

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Telekomünikasyon Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Hakan Ali ÇIRPAN

ŞUBAT 2022

Batuhan KAPLAN, an M.Sc. student of ITU Graduate School student ID 504181341, successfully defended the thesis entitled "SIGNAL DETECTION AND PARAMETER ESTIMATION OF FREQUENCY HOPPING SIGNALS", which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Prof. Dr. Hakan Ali ÇIRPAN** Istanbul Technical University	.....
Jury Members :	**Prof. Dr. Ender Mete EKŞİOĞLU** Istanbul Technical University	.....
	Asst. Prof. Tunçer BAYKAŞ Kadir Has University	.....

Date of Submission : 14 January 2022
Date of Defense : 2 February 2022

To my family,

FOREWORD

First, I would like to express my gratitude to my advisor, Prof. Dr. Hakan Ali ÇIRPAN. It was a privilege to be his graduate student. I appreciate the freedom he gave me and his countless hours of guidance, encouragement, trust, and support throughout the entire process to emerge this work.

I would also like to thank my colleagues at TÜBİTAK BİLGEM HİSAR Laboratory for their continuous support and thought-provoking discussions.

Last but not least, I thank my parents, my sister, and my brother–in–law for sharing their love and support all these years. I owe all my success to their blessings and encouragement.

February 2022

Batuhan KAPLAN
(Electronics and Communication Engineer)

TABLE OF CONTENTS

Page

ABBREVIATIONS

V-2-X : Vehicle-to-Everything
FHSS : Frequency Hopping Spread Spectrum
RC : Radio Controller
ISM : Industrial, Scientific and Medical
DF : Direction Finding
AoA : Angle of Arrival
FH : Frequency Hopping
ISI : Inter symbol interference
RSS : Received Signal Strength
AWGN : Additive White Gaussian Noise
PSK : Phase-Shift Keying
SNR : Signal-to-Noise Ratio
OFDM : Orthogonal Frequency Division Multiplexing
CAF : Cyclic Autocorreletion Function
SCF : Spectral Correlation Function
STFT : Short-Time Fourier Transform
CS : Compressive Sampling
PSD : Power Spectral Density
RMSE : Root-Mean-Square-Error
TÜBİTAK : Scientific and Technological Research Council of Turkey
BİLGEM : Informatics and Information Security Research Center
SSA : Signal and Spectrum Analyzer
SBS : Switched Beam System
AAS : Adaptive Array System
ULA : Uniform Linear Array
MVDR : Minumum Variance Distortionless Response
NLOS : Non-Line-of-Sight
MUSIC : Multiple Signal Classification
LOS : Line-of-Sight
NI : National Instrument

SYMBOLS

t	**:** Time
$\mathbf{T_h}$	**:** Dwell time
W	**:** Bandwidth
$\mathbf{B_k}$	**:** Time gap between kth and $(k-1)$th hops
$\mathbf{C_k}$	**:** The tart time of the kth hop
N	**:** The period of the time gaps
τ	**:** Time lag
$\boldsymbol{M}$	**:** Window size
$\boldsymbol{L}$	**:** Overlap size
μ	**:** Threshold
c	**:** The speed of light
M	**:** The number of antenna

LIST OF TABLES

Page

LIST OF FIGURES

Page

SIGNAL DETECTION AND PARAMETER ESTIMATION OF FREQUENCY HOPPING SIGNALS

SUMMARY

Unmanned aerial vehicles (UAVs) have become a prevalent part of the daily life with their applications to many fields such as mapping and surveying, transportation, surveillance, law enforcement, aerial imaging and agriculture. Besides the aforementioned use of UAVs in many areas, one should keep in mind that UAVs can also be used dangerously to create unwanted incidents especially when they are diverted to the sensitive airspace near airports and their presence may cause accidents which can result in fatal crashes. Moreover, UAVs can be utilized for collecting information about people, organizations, and companies without their consent. Therefore, identification and direction of arrival estimation of UAV systems/remote controllers and their communication are great importance, especially to prevent unwanted situations. In this context, it is known that most of the communication between the UAVs and wireless radio controller (RC) utilize the spread spectrum technology of frequency hopping spread spectrum (FHSS) on ISM band at 2.4 GHz. Therefore a method to detect, classify and estimate the direction of arrival of these kinds of signals in this band would lead to the identification of the communication between the UAV and the controller. Thus, this thesis attempts to address solutions for identifying and direction of arrival estimation of FHSS signals.

In Chapter I, open issues and the state–of–the–art solutions to the open issues in FHSS signal detection, identification and direction of arrival estimation are given. Moreover, in Chapter II, mathematical preliminaries of FHSS signal characteristics are provided.

In Chapter III, signal detection and parameter estimation are discussed by focusing on cyclostationarity signal and time–frequency analyses. First, a method based on cyclostationarity analysis is applied to distinguish the FHSS signals. Furthermore, short–time Fourier transform (STFT) based blind signal detection and clustering are employed to reconstruct the correct hops of the FHSS signal. Therefore, if there is an interference signal, outliers are removed from the parameters table according to the spectral localization of the signals. Furthermore, the literature utilizes the simulated data instead of over–the–air signals in general and these simulations assume that there is no time guards between hops. This assumption makes differentiation of frequency–hopping (FH) signals easier, however, many hopping signals use time guards and also these time guards are different for different signal sources.

In Chapter IV, direction of arrival estimation for FHSS signals are studied by utilizing MUSIC algorithm which is a high–resolution subspace–based direction-finding algorithm. A variant of STFT is introduced to extract the parameters of detected FHSS signals. The correct hopping signals are then aggregated based on the clustered parameters to obtain their combined baseband equivalent signal. Furthermore, the resampling process is applied to reduce the unrelated samples in the spectrum

and represent the spectrum with the reconstructed signal, which has a much lower bandwidth than the spread bandwidth. Finally, two different multiple signal classification algorithms are utilized to estimate the direction of the drone controller relative to the receiving system. In order to validate the overall performance of the proposed method, the introduced framework is implemented on hardware platforms and tested under real–world conditions. A uniform linear antenna array is utilized to capture over–the–air signals in hilly terrain suburban environments by considering both line–of–sight and non–line–of–sight cases. Direction estimation performance is presented in a comparative manner and relevant discussions are provided.

FREKANS ATLAMALI SİNYALLERİN TESPİTİ VE PARAMETRE KESTİRİMİ

ÖZET

Akılı ev teknolojisi, kişisel cihazlar, endüstriyel otomasyon, araçla-herşey gibi alanlarının yaygınlaşması ile kablosuz haberleşme cihazlarının sayısı gün geçtikçe artmaktadır. Bundan dolayı, sınırlı kullanım alanına sahip spektrumun tüm kullanıcılar için yeterli kaynağı sağlaması mümkün gözükmemektedir. Dolayısıyla, bu kablosuz haberleşme cihazlarının her birinin mevcut kaynağı paylaşımlı bir şekilde kullanması önem arz etmektedir. Sinyal kaynakları spektrumda kesintisiz bir şekilde haberleşmeye devam edebilmek için çoklu erişim tekniklerini kullanmaktadır. Bunlar arasında frekans atlama yayılmalı spektrum (FAYS) teknolojisi ile kablosuz haberleşme sistemleri, hızlı bir şekilde merkez frekansını değiştirmesiyle spektrumda yayılarak herhangi bir frekans planı olmadan geniş bantta iletişim sağlamaktadır. Böylece, FAYS haberleşme sistemleri yoğun bir spektrumda girişime karşı dayanıklı ve karıştırmaya karşı koyma gibi yeteneklere sahip olmaktadır.

Frekans atlamalı haberleşme sistemlerinin kullanımı öncelikli olarak askeri amaçlı kullanılan radyolarda olmak üzere, Bluetooth haberleşmesi, drone radyo kontrolcü haberleşmesi, medikal cihazlar için kullanılan haberleşme sistemleri gibi birçok farklı sivil alan uygulamalarında da yaygın olarak kullanılmaktadır. Askeri uygulamalarda, birçok ülke iletişim güvenliği açısından taktik veri linklerinde frekans atlamalı sistemleri benimsemiştir. Frekans atlamalı haberleşme sistemleri, sivil uygulamalar için ise lisanssız spektrum bölgesinde frekans planlanmasına gerek duymadan spektrum paylaşımını girişim olmadan yapabilmektedir.

Günümüzde dronların ya da bir başka deyişle İnsansız Hava Araçları (İHA), hobi amaçlı olarak kullanılan bir alan olarak gözüksede haritalama ve ölçme, ulaşım, gözetleme, kolluk kuvvetleri, havadan görüntüleme, tarım gibi birçok alandaki uygulamaları ile günlük hayatın yaygın bir parçası haline gelmektedir. İHA'ların pek çok alanda kullanılmasının yanı sıra, güvenlik ve gizlilik açısından tehlike oluşturması da mümkündür. Örneğin, İHA'ların havaalanlarında istenmeyen olaylar yaratmak için tehlikeli bir şekilde kullanılabileceğini ve varlıklarının telafisi mümkün olmayan kazalara neden olabileceği unutulmamalıdır. Ayrıca İHA'lar, araçlar, altyapılar ve tesisler için doğrudan bir fiziksel tehdit olmanın yanı sıra, İHA'lar özellikle kritik operasyonlarda ve/veya hizmetlerde arızaya yol açan iletişim bağlantılarını karıştırmak, müdahale etmek veya tamamen engellemek için kullanıldıklarında da tehdit kaynağı olabilir. Her geçen gün küçülen boyutları ve artan yetenekleri göz önüne alındığında, güvenlik için çevredeki drone faaliyetlerinden haberdar olmak önemli bir gözetleme unsuru haline gelmektedir. Ek olarak, İHA'nın görünümünü uçurtma, kuş vb. gibi diğer uçan nesnelerden etkili bir şekilde ayırt edilemeyebilir. Bu nedenler göz önüne alındığında İHA sistemlerinin/uzaktan kumandaların tanımlanması ve varış yönü tahmini, özellikle istenmeyen durumların önlenmesi açısından büyük önem taşımaktadır. Bu noktada, birçok İHA ile kablosuz radyo denetleyicisi arasındaki

iletişimin 2.4 GHz ISM bandında ve FAYS teknolojisini kullandığı bilinmektedir. Bu bilgiler ışığında, daha önce ifade edilen bantta farklı sinyal kaynakları spektrumu meşgul edebileceği için FAYS türündeki drone radyo kontrolcüsünün tespit edilmesi ve farklı sinyal kaynakları arasından ayrıştırılması sağlanmalıdır. Bu tez çalışmasında FAYS türündeki drone radyo kontrolcüsünün tespit algoritması simülasyon verileri ile analiz edilmektedir. Ayrıca, test düzeneği kurularak gerçek dünya koşulları altında sinyal tespit ve parametre kestirimi yaklaşımı incelenmektedir. Ardından, çoklu alıcı sistem kullanılarak altuzay tabanlı yön bulma algoritması ile drone radyo kontrolcüsüne ait yön kestirimi yapılmaktadır. Sinyal ayrıştırma sırasındaki çözünürlük sorunu ele alınarak elde edilen başarım göz önüne alınıp gerçek dünya koşullarındaki performansına bakılmaktadır. Test için kurulan ölçüm düzeneği, Rohde & Schwarz spektrum analizörü, Rohde & Schwarz sinyal üreteci, Futaba T8J drone radyo kontrolcüsü, NI PXIe çok kanallı alıcı, özdeş 4 adet Quasi Yagi anten, kişisel bilgisayar ekipmanlarından oluşmaktadır. Tüm ölçümler Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Gebze, Kocaeli yerleşkesinde bulunan tepelik arazi banliyö tipi açık test sahasında yapılmıştır.

Bölüm I'de, dron kullanımı ve gerçekleşebilecek tehditler ele alınıp FAYS sinyal algılama, tanımlama ve varış yönü tahminindeki açık sorunlara yönelik literatürde yer alan çeşitli çözümlere yer verilmektedir. Ayrıca, Bölüm II'de FAYS sinyal karakteristiklerinin matematiksel ön bilgileri detaylı bir şekilde anlatılmaktadır.

Bölüm III'te, döngüsel durağanlık sinyali ve zaman-frekans analizlerine odaklanılarak sinyal tespiti ve parametre kestirimi tartışılmaktadır. İlk olarak, FAYS sinyallerini ayırt etmek için döngüsel durağanlık analizine dayalı bir yöntem uygulanmaktadır. İkince dereceden çevrimselözdurağan analizi ile alınan sinyal içinde gizli periyodiklik ortaya çıkabilmektedir. Böylece, bir FAYS sinyaline ait atlama oranı kestirilerek farklı sinyaller birbirinden ayrıştırılabilir. Örneğin, 2.4 GHz ISM bandında çokca bulunan Bluetooth sinyali (saniyede 1600 atlama) ile drone radyo kontrolcüsü sinyali (saniyede 100-200 atlama) kestirilen atlama oranı parametresine bakılarak gelen FAYS sinyalinin tanımlanması mümkün olmaktadır. Ayrıca, FAYS sinyalinin doğru atlamalarını yeniden oluşturmak için kısa süreli Fourier dönüşümü (STFT) tabanlı kör sinyal algılama ve kümeleme yöntemi kullanılır. Böylece, bir girişim sinyali varsa, sinyallerin spektral lokalizasyonuna göre parametreler tablosundan aykırı değerler çıkartılır. Bunun için, STFT değerlerinin gürültü seviyesinin hesaplanması ile elde edilen eşik seviyesi ile karşılaştırılmasıyla ikilileştirilmiş matris elde edilmektedir. Ardından kablosuz haberleşme bozukluklarından kaynaklı hatalı olarak ifade edilen değerler iki aşamada düzeltilmektedir. İlk önce, ikilileştirilmiş matris morfolojik işlemler kullanılarak sinyali ifade eden alanın iç bölgesi düzeltilmektedir. İkinci aşama olarak matris elemanlarının komşulukları kontrol edilerek sinyali ifade eden bölgenin sınırları düzeltilmektedir. Böylece matris üzerinden sinyalleri segmente edebilmek için süreklilik sağlanmış olup spektrumu meşgul eden sinyallerin zamansal ve frekans bilgileri elde edilmektedir. Ayrıca, literatür genel olarak kablosuz sinyaller yerine simüle edilmiş verileri kullanır ve bu simülasyonlar, atlamalar arasında zaman koruması olmadığını varsayar. Bu varsayım, frekans atlamalı sinyallerinin farklılaşmasını kolaylaştırır, ancak birçok frekans atlamalı sinyal zaman boşlukları kullanır ve ayrıca bu zaman boşlukları farklı sinyal kaynakları için farklıdır. Sinyal karakteristiklerine (başlangıç zamanı, bitiş zamanı, bandgenişliği, bulunma süresi) bakılarak merkez tabanlı kümeleme yaklaşımı ile FAYS sinyaline ait atlamalar sınıflandırılmaktadır. Buna bağlı olarakta, spektrumda FAYS sinyalinin

olup olmadığına bakılarak farklı sinyal–gürültü oranı (SNR) değerleri için doğru tespit olasılığı hesaplanmaktadır. Aynı zamanda, tespit performansı farklı yanlış alarm oranları içinde incelenmektedir. Ayrıca, çevrimselözdurağan sinyal analizi yöntemi ile kestirilen atlama oranı parametresi, gerçek atlama oranına ne kadar yaklaştığı analizi üzerinde de durulmuktadır.

Bölüm IV'te, FAYS sinyalleri için varış yönü tahmini, yüksek çözünürlüklü altuzay tabanlı yön bulma algoritmaları kullanılarak incelenmiştir. Frekans atlama sinyalleri daha sonra birleştirilmiş temel bant eşdeğer sinyalini elde etmek için Bölüm III'te bahsedildiği üzere kümelenmiş parametrelere dayalı olarak arka arkaya eklenir. Böylece FAYS sinyali için kısa zamanda bulunan sinyal örnekleri yerine temel bantta sinyal örnekleri arttırılmıştır. Ayrıca, temel bantta yeniden elde edilen sinyali spektrumda yayılmış bant genişliğinden çok daha düşük bir bant genişliğine sahip olacak şekilde yeniden örnekleme işlemi uygunabilmektedir. Böylece, spektrumdaki ilgisiz örnekleri azaltmak ve altuzay tabanlı yön kestirimi uygulaması için gerekli olan kovaryans matrisinin hesaplanmasını kolaylaşmaktadır. Bu önişlemlerin ardından, alıcı sisteme göre drone kontrolörünün yönünü tahmin etmek için iki farklı çoklu sinyal sınıflandırma algoritması kullanılır. Önerilen yöntemin genel performansını doğrulamak için tanıtılan çerçeve, donanım platformları ile uygulanmaktadır ve gerçek dünya koşulları altında test edilmektedir. Dronlar kısa sürede bir noktadan başka bir noktaya hareket ettirilebilmektedir. Dronun hızlı hareket etmesinin yanı sıra, drone pilotu o kadar hızlı hareket edememektedir. Bu durum göz önüne alınarak, farklı mesafeler için yavaş açı değişiklikleri için oluşturulan senaryo ile hem görüş hattı hem de görüş hattı olmayan durumlar ele alınmaktadır. Düzgün doğrusal dizilime sahip anten dizisi ile havadan alınan sinyaller için farklı anten sayısı, önişlem etkisi, farklı yön kestirimi algoritması parametrelerine göre sonuçlar karşılaştırmalı olarak sunulmaktadır ve ilgili tartışmalara yer verilmektedir.

Gelecek çalışmalarda, son zamanlarda farklı alanlarda giderek kullanımı artan derin öğrenme tabanlı sistemleri ile FAYS sinyallerinin tespiti için kullanılması araştırılmalıdır. Böylece, spektral lokalizasyon açısından önişlem adımının yerine geçmesi öngörülebilir. Bunun yanında, çoklu FAYS sinyallerinin spektrumda mevcut olması durumunda, farklı SNR değerleri için farklı koşullar altında doğru kümelenme olasılığı incelenebilir. FAYS sinyalleri geniş bantta farklı frekanslarda bulunduğundan dolayı, yön kestirimi için Fourier domaninde altuzay tabanlı algoritmalar araştırılmalıdır.

1. INTRODUCTION

Nowadays, wireless communication is an indispensable point for communities. There is a growing demand for the number of physical devices that used wireless communications, such areas as personal devices, smart homes, vehicle-to-everything (V2X), industrial automation, etc [1]. Since the demand for mobile data traffic extremely grows day by day, scarcity emerges in the finite spectrum resources. Utilization of the spectrum becomes inaccessible and in this regard, allocation is controlled by national and international regulations. While the frequency spectrum is a natural resource, it can not be expanded or increased and the demand of the spectrum activity can be overcome with the development of communication systems. Many of the communication devices rely on multiple access techniques to operate, especially in the unlicensed spectrum [2]. In the context of the cooperative environment which is consists of V2X or smart systems, the spectrum can be used over the network. However, not all devices transmit signals over a network and hence, communicate using the shared spectrum. This leads to uses the FHSS technology to avoid interference or jamming and can share the frequency channels without frequency planning.

FHSS communication is provided by changing carrier frequency rapidly while transmitting information and occupies a large spectral region over time. Although it was first developed for military areas, civilian applications also benefit from this technology as a process of time. In the aspect of military usage, tactical data link (Link–16) adopted the FHSS, since it has the ability of transmission security [3]. On the other hand, to manage the interference problem commercial communication devices are using the FHSS [4]. Common commercial devices are operating with FHSS such as Bluetooth, radio controller (RC), cordless phones, microphone signals, and unstructured signal sources such as microwave ovens or several medical devices. Among these applications, increased demand for the higher capacity of the V2X leads to the usage of drones. As drones become more popular, they have pivoted various

applications. Since the drones are controlled by a RC, the transmission between the drone and its pilot is provided by FHSS.

Drones pervade the modern civilian life almost in every aspect. Mapping and surveying, transportation, surveillance, law enforcement, aerial imaging, and agriculture are just to name a few [5]. Apparent penetration of drones into the aforementioned fields swiftly stems mainly from their multi–dimensional capabilities such as payload transportation, telecommunications, and task accomplishment. On the other hand, these capabilities pose several concerns regarding safety, security, and privacy etc. Beyond these concerns, presence of drones is considered to be a threat, especially in the vicinity or surrounding airspace of critical zones [6, 7]. For instance, a drone appeared at the Gatwick airport and it causes the shut down of the airport due to the risk of a crash with any aircraft. Hence, hundreds of flights were canceled and $140,000$ passengers were affected [8]. Moreover, drones can be utilized for collecting information about people, organizations, and companies without their consent. In addition to being a direct physical threat to vehicles, infrastructures, and facilities, drones could be an auxiliary source of threat especially when they are employed to jam, interfere, or totally block communication links leading to malfunction in critical operations and/or services. It is evident that detection of any potential or actual intrusion by cooperative and non–cooperative drones and their pilots is required to protect critical zones, vehicles, and operations. In this context, it is known that most of the communication between the drone and wireless RC utilize the spread spectrum technology of FHSS on industrial, scientific, and medical (ISM) band at 2.4 GHz, which provide resilience to interference, enhance security, and networking operations, as well as covert transmission [9].

Once a potential drone–RC/pilot link is detected, the next step is to determine the direction of the incoming signals. This immediately implies the employment of radio–direction finding (DF) techniques. It is important to estimate the angle of arrival (AoA) of the signal while protecting the critical zones or unknown usage of spectrum. Also, it can be expanded to localize the user, hence intercepting the harmful usage of the spectrum and events is provided. Moreover, tracking is another crucial parameter while identifying the sources. While the user occupies the spectrum, the estimation of the angle of arrival should be provided constantly, especially for mobile

users. In order not spotted by target users, passive systems are considered instead of active systems. These are lead to considering the smart antenna systems [10, 11].

This thesis is composed of 5 chapters which are Introduction, FHSS Signals, Signal Detection and Parameter Estimation, Direction of Arrival of Estimation of for FHSS Signals, and Concluding Remarks and Future Directions. Chapter 2 presents the background for FHSS signals. The Chapter 3 focuses on cyclostationarity and time–frequency analysis for FHSS signals. Additionally, gives the real–world measurements for signal detection and parameter estimation for FHSS signals. In Chapter 4, the reconstruction is discussed for direction–finding estimation of FHSS signals. Also, the estimation results of direction–finding are given under the real–world conditions. Chapter 5 concludes the ideas that has been presented in the thesis and presents the possible future studies about the signal detection and direction–finding for FHSS signals.

2. FHSS SIGNALS

In the digital communication system, the modulated signals are multiplied with the carrier signal on a certain frequency. In the aspect of systems that uses FHSS, carrier frequencies are changed over time. Considering the number of users that use the limited spectrum, hops can allow avoiding interference. Also, if the avoidance is not provided, the interference occurs only temporarily and the communication still is available when the changing frequency [12].

The information is transmitted by a sequence of carrier frequencies which called as a FH pattern. In order to consistency of the communication, each frequency channel of an FHSS signal has a same width of a spectral region for all hops, depending on input signal. Furthermore, the speed of the switching between hops occurs at a constant rate. Therefore, the hopping duration or dwell time, which means the time that spends on a certain frequency channel, is standard per user. Fig. 2.1 illustrates the communication of an FHSS signal according to FH pattern between the interfere signals. The hopping characteristics can be listed as: the time interval between the hops can be denoted as T_h and W represents the bandwidth of the each hop. Additionally, the difference between the maximum frequency channel and minimum frequency channel means that the spreading spectrum.

In a typical communication system, information bits are mapped to symbols according to amplitude, phase, etc. After that, pulse shaping is utilized to prevent inter symbol interference (ISI) and generating a band-limited signal which results of achieve more suitable spectrum usage. Furthermore, a frequency synthesizer allows for up-conversion of the baseband signal. In the FHSS communication system, the frequency synthesizer produces a distinct tone determined by a set of channel numbers. To provide the secrecy and unpredictably of the FH pattern, these channel numbers are generated from the pseudo-noise sequence generator. Thus, mixing the output of the frequency synthesizer and modulated signal produce the FHSS signal. The generation of the FHSS signal can shown in Fig. 2.2. Additionally, when the communication

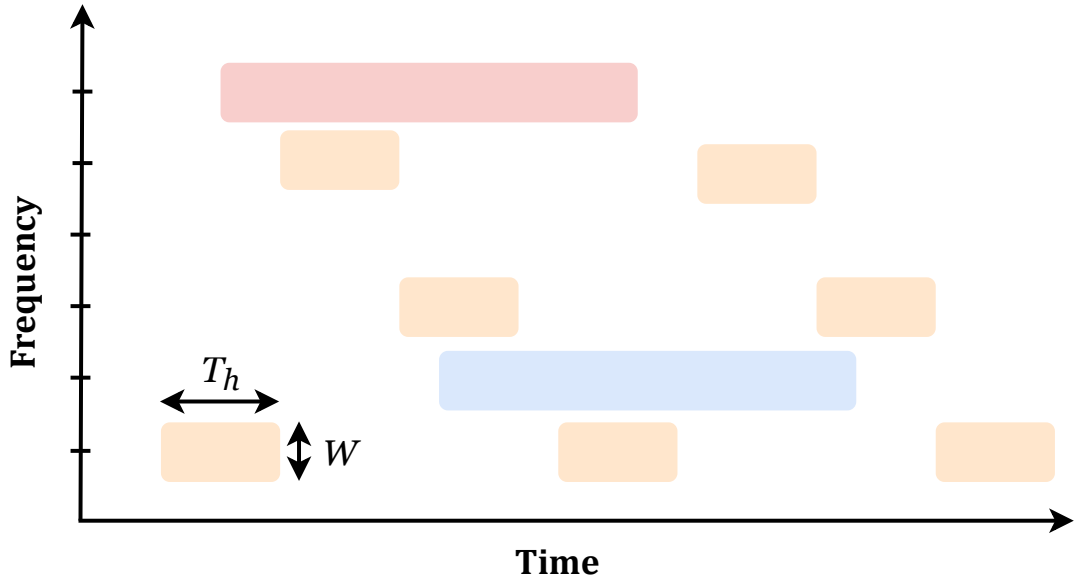


Figure 2.1 : FHSS signal pattern.

begins, the signal power is maximal at each frequency channel according to the hopping pattern. However, due to the limitation of the RF components, signal energy can not be infinitesimal. Therefore, the rise time and fall time transitions are occurred. Another factor that determines the consistency between each hop is the transmit power. Since there are various users in a shared spectrum, at the receiver side, channel conditions affect the signal that sent by the same user in a similar way, when considering the received signal strength (RSS).

The variants of the FHSS signal can be classified as fast hopping rate and slow hopping rate. The difference between the fast and slow is number of transmitted symbols at each hop [13]. Considering the symbol rate, when there are multiple data symbols per hop the system is called slow hopping, on the contrary, there are multiple hops per data symbol for fast hopping. For spectral efficiency, the slow FH is more preferable.

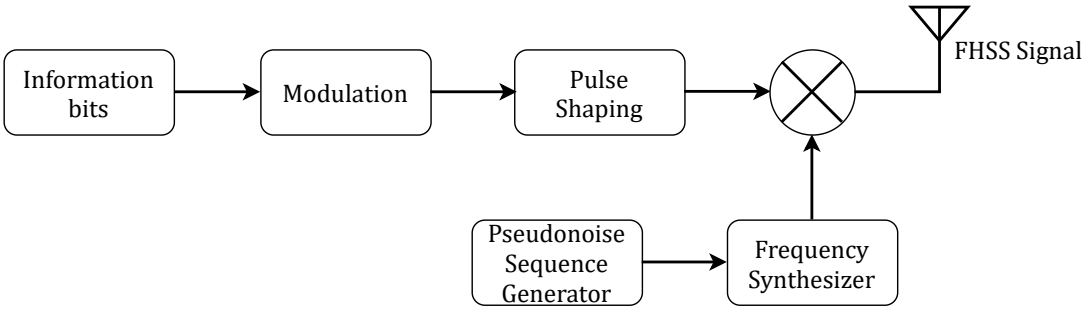


Figure 2.2 : FHSS signal modulator.

The advantage of the fast FH, the communication systems are more robust against the fading and noisy channels and also, possible jammers [14].

2.1 Signal Model

In the transmitter side, modulated signal is mixed with the frequency synthesizer output. A single FHSS signal can be written as,

$$x(t) = s(t) \times \sum_{k=1}^{K} e^{j(2\pi f_k t + \varphi_k)} w_k(t - B_k) \tag{2.1}$$

where $s(t)$ denotes the complex baseband equivalent of the information bearer that has a periodic burst type transmission for $t \in [0, T]$, K stands for the total number of hops during the duration of T, f_k and φ_k represent the carrier frequency and initial phase of the kth hopping, respectively. Rectangular window function, $w_k(t)$, can be expressed as,

$$w_k(t) = \begin{cases} 1, & t \in [(k-1)T_h, kT_h) \\ 0, & \text{others} \end{cases} \tag{2.2}$$

where T_h is the dwell time.

The start time of the kth hop is represented as B_k. Then, we define a sequence $\{C_k\}$, which is the time difference between kth and $(k+1)$th hop, are given as,

$$C_k = B_{k+1} - B_k, \quad k \in [1, K-1] \tag{2.3}$$

where B_{k+1} and B_k are the sum of all time gaps corresponding to $(k+1)$th and kth hops, respectively. By assuming that the sequence of time gaps is periodic with N, C_l can then described in terms of the estimated time gaps as,

$$C_l = T_h + \Delta t_i,\ l \equiv i \mod N,\ 0 < i \leq N. \tag{2.4}$$

The complex baseband equivalent of the received passband signal can be described by,

$$r(t) = \underbrace{h(t) * x(t)}_{y(t)} + n(t) + i(t) \tag{2.5}$$

where $*$ is the convolution operator, $h(t)$ is the channel impulse response between the transmitter and receiver, which has frequency flat fading, $x(t)$ denotes the desired FHSS signal and $n(t)$ stands for the complex additive white Gaussian noise (AWGN) in which I and Q components are i.i.d $\sim \mathcal{N}(0, \sigma^2/2)$. Also, $i(t)$ represents the possible interference signal that disturbs the desired signal, and assumed as $i(t)$ and $x(t)$ are uncorrelated signals. Considering the drastic increase in the number of wireless communication devices, the impact of the interference might occur as co-channel interference. The applications that use unlicensed spectrum consist of Wi-Fi technology, ZigBee signals, and unstructured signal sources such as microwave ovens or several medical devices. Hence, to define the signal model can comprise an interference signal.

3. SIGNAL DETECTION AND PARAMETER ESTIMATION

3.1 Cyclostationarity Signal Analysis

Communication signals are interpreted as a random process. Herein, encountered in statistical signal processing and communication signals are often assumed stationary processes. For example, a binary phase–shift keying (PSK) modulation scheme mapped bits to -1 and $+1$ with equal probability is considered a stationary process. However, the cyclostationarity process depends on varying cyclically statistical properties with time. The stationary process can be affected due to the varying environmental conditions (e.g. random fluctuations) and human-made external additions such as upsampling, repetitive pulsing/on–off keying, sine-wave carriers [15, 16]. Therefore, communication signals can be thought as a cyclostationarity process under these effects.

For many years, research on the cyclostationarity process developed various algorithms on different application areas. Considering the presence of periodicities in every aspect of real life, cyclostationarity signals can occur in communication, radar, sonar, telemetry, geophysical and atmospheric sciences, rotating machinery, econometrics, and biological systems [17]. In regard to the communication signals, the cyclostationarity signal analysis is preferred mostly in the problems of statistical function estimation, signal detection, and cycle frequency estimation. In the problems of spectrum sensing, cyclostationarity becomes prominent a robust technique under the fading and low signal–to–noise ratio (SNR) [18]. Furthermore, cyclostationarity can be used for identification between the different types of signals because of the extracting cyclic features. For instance, in [19, 20], the authors preferred the cyclostationarity based feature detection for modulation recognition with using higher–order cumulants, in [21], orthogonal frequency division multiplexing (OFDM) based wireless standards are distinguished with second–order cyclostationarity feature. Also, blind channel estimation and equalization are achievable by using cyclostationarity signal analysis [22]. The recent interest in cyclostationarity based solutions is adopted for periodically

varying communication systems and signal processing applications tremendously, with emphasis on second-order statistical characterization.

3.1.1 First–order cyclostationarity

If the signal behaves first–order periodicity as [23],

$$m_r^{\alpha} = \lim_{T\to\infty} \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} r(t) e^{-j2\pi\alpha t} dt \tag{3.1}$$

where α and m_r^{α} are the first-order cycle frequency and cyclic moment, respectively.

3.1.2 Second–order cyclostationarity

Cyclostationarity analysis can be utilized to discover hidden periodicity within a received signal [24, 25]. The second-order cyclostationarity of the received signal reveals the hopping rate of the FHSS signal. Cyclostationarity analysis begins by taking the autocorrelation function which is denoted as,

$$R_{r,r}(t,\tau) = \mathbb{E}\left\{r(t+\tau)r^*(t)\right\}, \tag{3.2}$$

where $(\cdot)^*$ is the complex conjugate operator, and τ represents the time lag. If the autocorrelation function has a periodicity in t, it can be written by Fourier series expansion,

$$\begin{aligned} R_r(t,\tau) &= \sum_{k=-\infty}^{\infty} A_k(\tau) e^{j\frac{2\pi}{T_0}kt} \\ A_k(\tau) &= \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} R_r(t,\tau) e^{-j\frac{2\pi}{T_0}kt}\, dt \end{aligned} \tag{3.3}$$

where $A_k(\tau)$ represents the kth coefficient at τ time lag which is also known as a cyclic autocorrelation function (CAF), and T_0 is the fundamental period. Furthermore, the frequency domain representation of the signals can extract unique features. In this regard, the Fourier transform of the CAF can be calculated by using the cyclic Wiener relationship,

$$S_k(f) = \int_{-\infty}^{\infty} A_k(\tau) e^{-j2\pi f\tau} d\tau \tag{3.4}$$

where $S_k(f)$ is known as spectral correlation function (SCF) for a fixed k value.

3.1.2.1 On the investigation of second–order cyclostationarity for FHSS signals

Many FHSS signals follow a pattern in time and this leads cyclic behavior in time domain. The received signal can be reformed by combining the $x(t)$ into the $r(t)$ by,

$$r(t) = h \times \underbrace{s(t) \sum_{k=1}^{K} e^{j(2\pi f_k t + \varphi_k)} w_k(t - B_k)}_{x(t)} + n(t) + i(t). \tag{3.5}$$

The periodicity is provided by $s(t)$ whereas $x(t)$ and $r(t)$ are not periodic due to the frequency hopping pattern. To analyze hidden periodicity inside $r(t)$, frequency hopping pattern is suppressed on $\widetilde{r}(t)$ which is defined as,

$$\widetilde{r}(t) = |r(t)|^2 \tag{3.6}$$

where $r(t)$ represents the received signal. Considering the **(3.5)**, $\widetilde{r}(t)$ equals to,

$$\widetilde{r}(t) = \left|h\right|^2 \left|s(t)\right|^2 + hx(t)n^*(t) + hx(t)i^*(t) + h^*x^*(t)n(t) + n(t)n^*(t) + n(t)i^*(t) \tag{3.7}$$

Autocorrelation function is considered for cyclostationarity analysis as,

$$\begin{aligned} R_{\widetilde{r},\widetilde{r}}(t,\tau) = &\left|h\right|^4 \left|R_{s,s}(t,\tau)\right|^2 + \left|R_{i,i}(t,\tau)\right|^2 + 2\left|h\right|^2 R_{x,x}(t,\tau)R_{i,i}(t,\tau) + \left(h^2 + (h^*)^2\right) \\ &R_{x,x^*}(t,\tau)R_{i,i^*}(t,\tau) + 2\delta(\tau)\sigma^2\left(\left|h\right|^2 P_s + P_i\right) + 2\left|h\right|^2 P_s\left(P_i + \sigma^2\right) \\ &+ 2\sigma^2 P_i + \sigma^4 \end{aligned} \tag{3.8}$$

where $R_{\widetilde{r},\widetilde{r}}(t,\tau)$ represents autocorrelation of $\widetilde{r}(t)$. $R_{\widetilde{r},\widetilde{r}}(t,\tau)$ has 81 summation terms and 64 of them are 0 due to properties of noise. σ^2 stands for the noise variance, and P_s and P_i are the average power of $s(t)$ and $i(t)$, respectively. In addition, if there is no interference signal, then **(3.8)** is simplified as,

$$R_{\widetilde{r},\widetilde{r}}(t,\tau) = \left|h\right|^4 \left|R_{s,s}(t,\tau)\right|^2 + 2\left|h\right|^2 \sigma^2 P_s + \sigma^4 + 2\sigma^2 \left|h\right|^2 P_s \delta(\tau) \tag{3.9}$$

Recall that $s(t)$ is periodic that depends on hopping duration, which indicates that $R_{s,s}(t,\tau)$ is also periodic. Thus, $R_{\widetilde{r},\widetilde{r}}(t,\tau)$ can be expanded via Fourier Series

coefficients. Finally, SCF for FHSS signals can be obtained by calculating the Fourier Transform of the CAF which defined in **(3.4)**. SCF should have peaks at cyclic frequencies for which the fundamental frequency is defined as a hopping rate.

Since the cyclostationarity based methods generally focus on periodicities such as chip rate, pilot signals, etc., non-periodic signals such as double side band–single carrier amplitude modulation do not indicate cyclic features. Any signal that behaves periodically is detected by cyclostationarity feature detection. Moreover, if the ISM spectrum is occupied with various signal sources, the cyclostationarity analysis estimates the periodicity feature for signals that are periodic and reveal peaks for them. However, the search area of cyclic frequencies is limited in the range specified in the standards. Hence, the existence of other peak values would not be a concern to consider.

3.2 Time–Frequency Analysis

Traditional time or frequency analysis can not be suitable for FHSS signals. Rather than generating a 1-dimensional signal after taking a transform, the time-frequency analysis provides a 2–dimensional representation [26, 27]. For instance, musical sounds are time-varying signals which starts with a high level and gradually decay, can not analysis with 1–dimensional transforms. Hence, time-frequency analysis is needed for time-varying signals. Furthermore, time-frequency analysis is a great opportunity to analyze when the model of signals is not known. Since FHSS signals that changing carrier frequency in a short interval with an unknown sequence, time-frequency analysis can provide in which carrier frequency where the signal starts in time and where the ends in time.

Over years, there are different approaches are developed for represents signals in 2–dimensional. The time-frequency analysis can be categorized into two classes [28]. First class is based on translating, modulating, and scaling a basis function to derive time–frequency representation. This category can consist of short–time Fourier transform (STFT), wavelets, and matching pursuit algorithms, as an example [29–31]. In the aspect of the second class, the time–frequency representation can be characterized by a kernel function. Wigner distribution, and Choi-Williams distribution can be seen as some of the kernel based algorithms. Moreover,

compressive sampling (CS) is developed with the advances in the digital signal processing algorithms [32–35]. CS is utilize the sparsity of the signals to reduce the number of measurements needed, which achieved that with a fewer samples than Nyquist-Shannon sampling theorem. However, CS brings with such problems at the receiver as increased noise figure related to subsampling rate [36].

3.2.1 Short–time Fourier transform

The STFT approach is utilized to analyze the FHSS signals as a method to observe the frequency content of this type of non–stationary signals over time. Mathematical expression of STFT of the time-domain signal can be written as,

$$STFT\Big\{r(t)\Big\} = \int_{-\infty}^{\infty} [r(t)w(t-\tau)]e^{-j2\pi f\tau}d\tau \tag{3.10}$$

where $w(t)$ is the window function. The STFT matrix $S = [s_1[f], s_2[f], \cdots, s_K[f]]$ such that i_{th} element of this matrix is a column vector determined by discrete Fourier transform of windowed signal as,

$$s_i[f] = \sum_{n=0}^{N-1} r[n]w[n-iR]e^{-j2\pi fn} \tag{3.11}$$

where $r[n]$ is sampled version of $r(t)$ by considering the anti–aliasing property and R denotes the shifting length.

One should keep in mind that adjusting the time and frequency resolution is crucial point for STFT analysis [37] due to the trade off between them. The length of the time point can be calculated as [38]

$$m = \left\lfloor \frac{N_r - L}{M - L} \right\rfloor \tag{3.12}$$

where N_r is length of the signal, L denotes the number of overlap in the Fourier transform, M represents the window size, $\lfloor \cdot \rfloor$ stands for the floor operator.

As depicted in Fig. 3.1, the flow graph explains how the system works in brief. After the signal is received in the first stage, optimal window time length is decided to get the optimum resolution at **(3.12)** based on maximizing the number of elements on

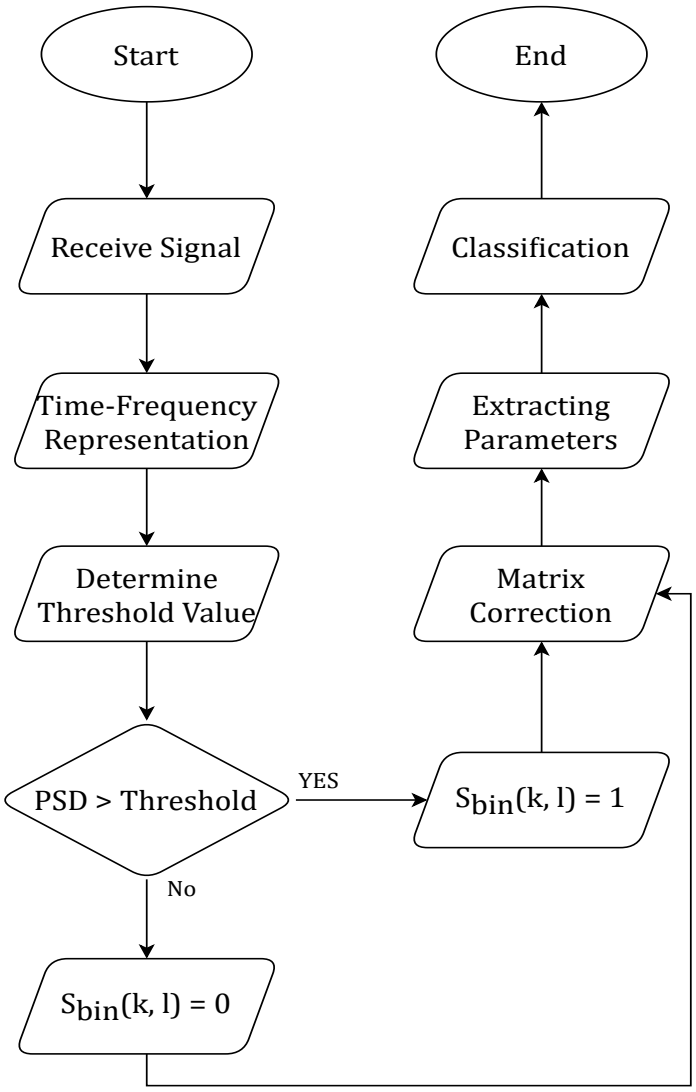


Figure 3.1 : The flowchart of the detection method.

the matrix S in the second stage of the flowchart. STFT is calculated in a dBm unit according to power spectral density (PSD) in the same step and shown in Fig. 3.3a.

As the next step of the flowchart, a binarization operation is conducted. The STFT matrix is converted to $S_{bin}(k,l)$, which will be defined as a binary matrix, using the threshold μ. Also, in the flowchart PSD refers to each point in the STFT matrix. Based on the dynamically calculated threshold value, whether the signal presents or not for each element of the STFT matrix is decided as shown in Fig. 3.3b. When the signal is present, $S_{bin}(k,l)$ is evaluated as 1 and the new binarized matrix, $S_{bin}(k,l)$, is given as,

$$S_{bin}(k,l) = \begin{cases} 1, & S(k,l) \geq \mu \\ 0, & S(k,l) < \mu \end{cases} \tag{3.13}$$

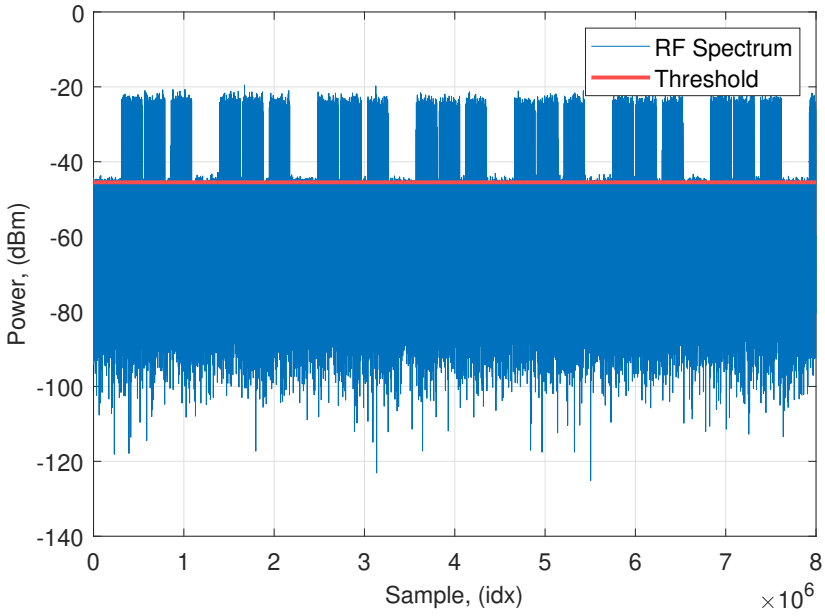


Figure 3.2 : Estimated threshold representation.

where k and l represent the frequency and time index in the sampled domain, respectively. To determine the threshold value, each element of STFT matrix are concatenated and a sorting algorithm implemented to list the power levels of each point of the STFT matrix in a ascending order. Considering the wideband spectrum and the fact that the hops of the FHSS signal occur in a short time interval, the majority of the received signal is comprised of noise samples. Therefore, taking the mean value of the top 20% of the sorted values of STFT matrix provides the to determine a lower bound for the computation of the threshold. Fig. 3.2 shows PSD values of the received signal, and the threshold value. Since the threshold value estimates the noise level, even for the very low SNR regimes, the simulation results indicate the feasibility of this threshold selection process.

Due to the wireless impairments on the received signal, the spectral region of the signal on $\mathbf{S_{bin}}$ is corrupted. This corruption is made it difficult to estimate the parameters of the spectral region and leads to miss the signal or increases the error of estimation of the spectral region. Moreover, as a result of the binarize the S matrix with an adaptive threshold, salt–and–pepper noise is seen which occurs from fluctuations of Gaussian noise. In order to represent the signal in a more plausible way, widely used morphological dilation and erosion aspects from the domain of image processing [39,40] are considered to recover the received signal properly. This problem is handled

in two parts as the inner region and edges of the signal. First, a 2–D convolution operator is used to filling the inner region of the signal calculated as,

$$S_{in}(k,l) = \begin{cases} 1, & S_{\text{bin}}(k,l) * J_{n,m} > \frac{n\times(m-1)}{2} \\ 0, & S_{\text{bin}}(k,l) * J_{n,m} < \frac{n\times(m-1)}{2} \end{cases} \tag{3.14}$$

where J is the all–ones matrix with a size of $n \times m$. According to the size of the kernel matrix which determines the threshold, the sum of the overlapping elements in each shifting in convolution are compared with the threshold value. Since the salt–and–pepper noise is impulse noise which is seen to random points in the matrix, the convolution operation is suppressing these points. Additionally, the region of the signal is dilated while inner elements are filled up after the convolution operation. The results of convolution with binarized matrix can be shown in Fig. 3.3c. Second part of the correction of the $\mathbf{S}_{\text{bin}}$ considers the edges of the spectral region that represents the presence of a signal. In order to preserve the continuity of the signal, the edge elements are controlled by considering the similarity of the values of the neighboring elements. For instance, when a signal region in the $\mathbf{S_{in}}$ is illustrates as,

$$\begin{bmatrix} \ddots & & \cdots & & \cdots & & \iddots \\ & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\ & 0 & 1 & 1 & 1 & 1 & 1 & 0 & \\ \cdots & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots \\ & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \\ & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \\ & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\ & & & & \vdots & & & & \end{bmatrix} \tag{3.15}$$

where 0 values marked in red are the values that remain incorrect. To change the incorrect 0 values, the left, right, up and down corners of each 0 value are controlled. Hence, if the conditions of neighbors elements are provided, the value is changed with 1. This process is continued until the region is shaped as rectangular, and the result is exhibited in Fig. 3.3d.

After the recovery process, it becomes possible to extract the signal parameters such as start time, stop time, center frequency and difference between start time and stop time (dwell time) accurately. The parameter extraction process relied on the binary search that detects the position of 1–valued elements of the $\mathbf{S_{in}}$. Since the rows and columns of

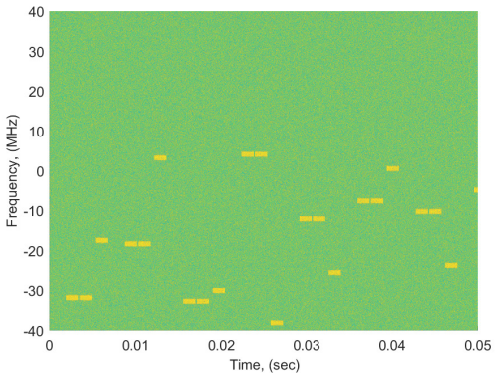


Figure 3.3a : The spectrogram of the received signal.

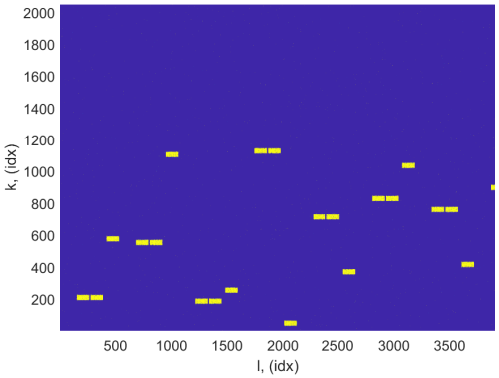


Figure 3.3b : The binarized version of the spectrum.

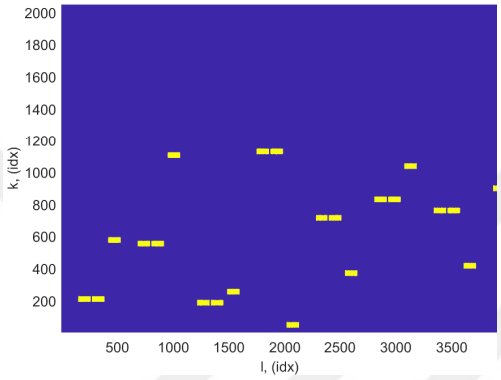


Figure 3.3c : Matrix correction process: Inner side of the signal.

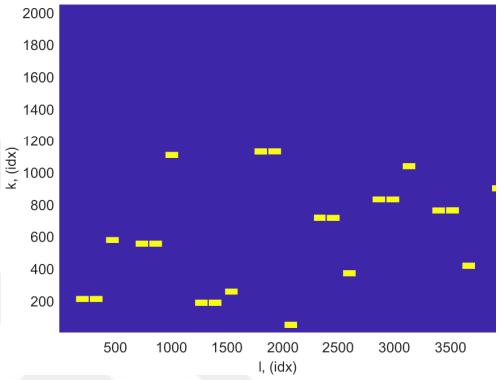


Figure 3.3d : Matrix correction process: Edge correction of the signal.

Figure 3.3 : Time–frequency calculation of the received signal. After the calculation binarization and correction results of the **S**.

the $\mathbf{S_{in}}$ indicate the time and frequency, respectively, when the first 1–valued element is detected, the counting on the rows is started until the detecting the next 0–valued element on the same row. Also, if the counter is reached the dimension of the $\mathbf{S_{in}}$, the counting process is terminated. Thus, at the end of the counting of the rows, the duration of the signal has been estimated as the value of the counter. In addition to these, the position of the row of the $\mathbf{S_{in}}$ that has been detected as 1–valued is defined as the lower frequency band of the signal. After the counter is stopped by detecting the 0–valued element or reaching the dimension of the row of the matrix, the search position is updated as the position of the previous element in the row. This time, the counter is established in the direction of the columns of the matrix. Hence, the bandwidth of the signal can be defined as the difference between where the counter

stops and its initial starting position. In the end a list is generated signal duration, center frequency, start time, end time, and bandwidth.

In the last step of the flowchart, controlling for each hop is done to decide whether it belongs to the FHSS signal or not. Based on the similarities of the features, the signals can be separated correctly. Clustering analysis utilizes the unsupervised learning process which points each data points to a group without prior knowledge. To achieve the clustering process, there exist different approaches under unsupervised learning such as centroid–based, density-based, distribution-based, and hierarchical-based algorithms [41]. Considering the problems, these algorithms can give solutions in different aspects. Considering the highly dynamic structure of the unlicensed spectrum, it is hard to label each scenario. Hence, unsupervised clustering is most beneficial to the signal separation process. In this regard, a set is formed according to the estimated parameters which include several temporal parameters (*e.g.*, dwell time, start/stop time) and bandwidth of each hop. If there is a signal that is not satisfying to the statistic of the set, this hop is excluded because of a possible interference signal. In the aspect of FHSS signals, separating the signals while employing the clustering analysis has unique conditions. The hops of FHSS signals must start after the previous-hop ends and also, the hopping duration and bandwidth of the hops are the same as each other. Moreover, in the case of multiple FHSS signals randomly occupying the spectrum band, the hops of the interested FHSS signal can be clustered. Therefore, regarding the number of input data features, the number of output labels can be varied when defining the user that occupies the spectrum.

To obtain the separated signal sources, a centroid–based algorithm is utilized with modifications. To initialize the clustering process, one of the input data is selected and is set as a first centroid. Following that, selected input data is compared with other parameters found in the parameter list concerning to hopping duration and bandwidth. Also, as stated earlier, the hops must follow the consecutive start and end time, therefore the difference between the end time of the selected input data and the start time of the compared data must be a positive value. When these conditions are provided, the hops are kept as a cluster, however, if the conditions are not matched, the data, which is compared feature, is defined as an outlier for this cluster. After that, the initial point of the bandwidth and hopping duration is updated according to clustered

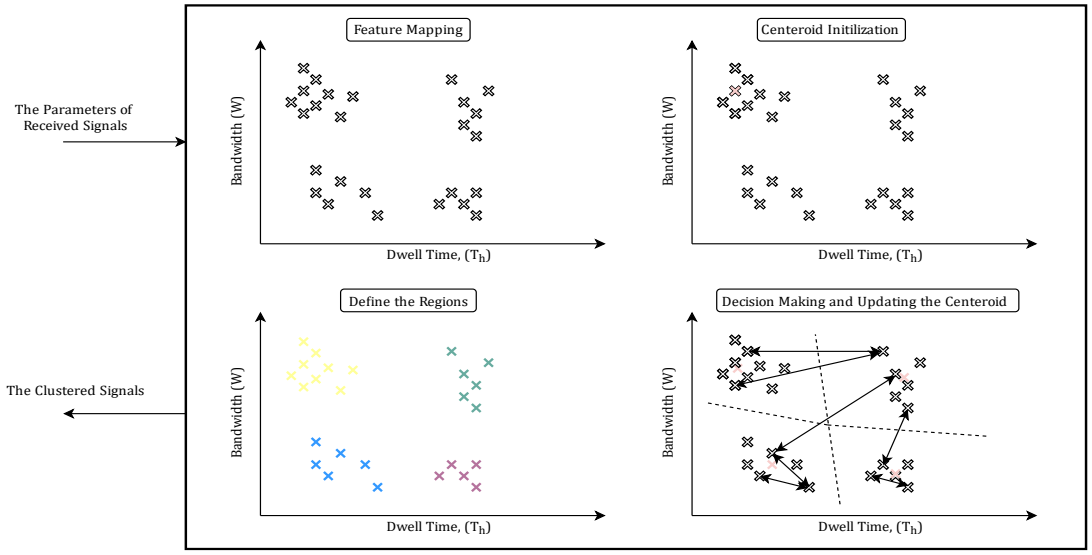


Figure 3.4 : An illustration of the clustering algorithm, which is taken parameters of the signals as inputs and compared with each other. The outputs are the clustered parameters and cluster labels.

parameters. Moreover, non–clustered signals are proceeded to compare with other features. If the conditions between the compared ones are achieved, a new centroid is determined. This process proceeds until all input features are compared with each other. An illustration of this algorithm is shown in Fig. 3.4. Regarding unrelated signals in spectral localization behavior, the clustering process is not converging any centroid for these signals, and hence different clusters are designated for these kinds of signals.

3.3 Simulation Results for Signal Detection and Parameter Estimation

To demonstrate the performance analysis of the signal detection, parameter estimation, and clustering performance, the occupied spectrum is simulated for the random users, which have varied signal characteristics. Since the spectrum contains a mixture of signals, the signal characteristics for each signal source are selected randomly as defined in Table 3.1. Considering the 80 MHz spectrum bandwidth, which is the available spectrum range for the unlicensed 2.4 GHz ISM band, in the simulation environment the frequency range is used as 80 MHz. Additionally, observation duration is one of the crucial specifications when capturing the signals. Considering the hop rates that are used in the simulations and computation limit, observation duration is selected as 0.01 seconds. Figure 3.5 exhibits that the simulation process that modulates

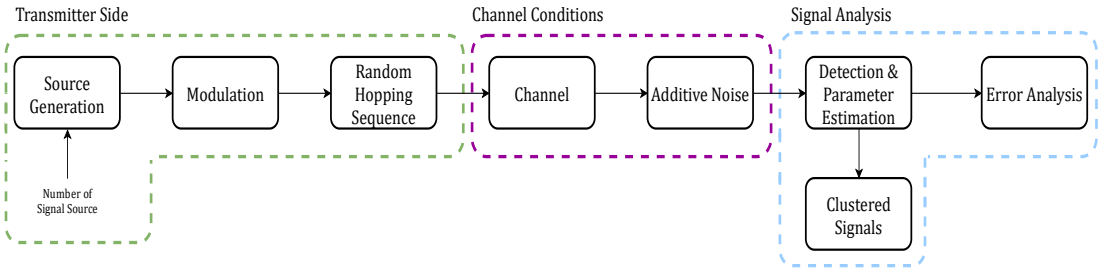


Figure 3.5 : Block diagram of emulation of FHSS signal generation and signal analysis.

the input bits of each signal sources, determines the hopping sequence, and adds the channel conditions.

Considering, Table 3.1 specifies the range of the transmitted FHSS signals characteristics, different scenarios can be examined. The hopping parameters are selected within the scope of Bluetooth specification and drone RC signal [42, 43]. In this regard, the lower and upper bounds of parameters, which are used for signal generation, have been set. Moreover, the radio frequency (RF) channel list, the dwell time and bandwidth of each hop, the time gap between the consecutive hops are selected uniformly within the bounds. Also, the initial start time of each signal source is determined as Poisson distributed. When the spectrum is occupied by the different signal sources, interference may occur. However, since the interference is observed within the dwell time duration of the FHSS signal, the consecutive hops can be analyzed, which will proceed on another carrier frequency.

When the simulated signal is generated, first, cyclostationarity analysis is applied as discussed in Section 3.1.2.1, second, time–frequency analysis is employed to determine where the signal is located in the spectrum and which signals are related

Table 3.1 : Frequency hopping spread spectrum (FHSS) parameters used for generating simulated signal.

	Lower-bound	Upper-bound
Start Time (s)	0	-
Stop Time (s)	-	0.01
Dwell Time (s)	0.00005	0.01
Bandwidth (MHz)	0.5	2
Spreaded Bandwidth (MHz)	30	70
SNR (dB)	-18	4

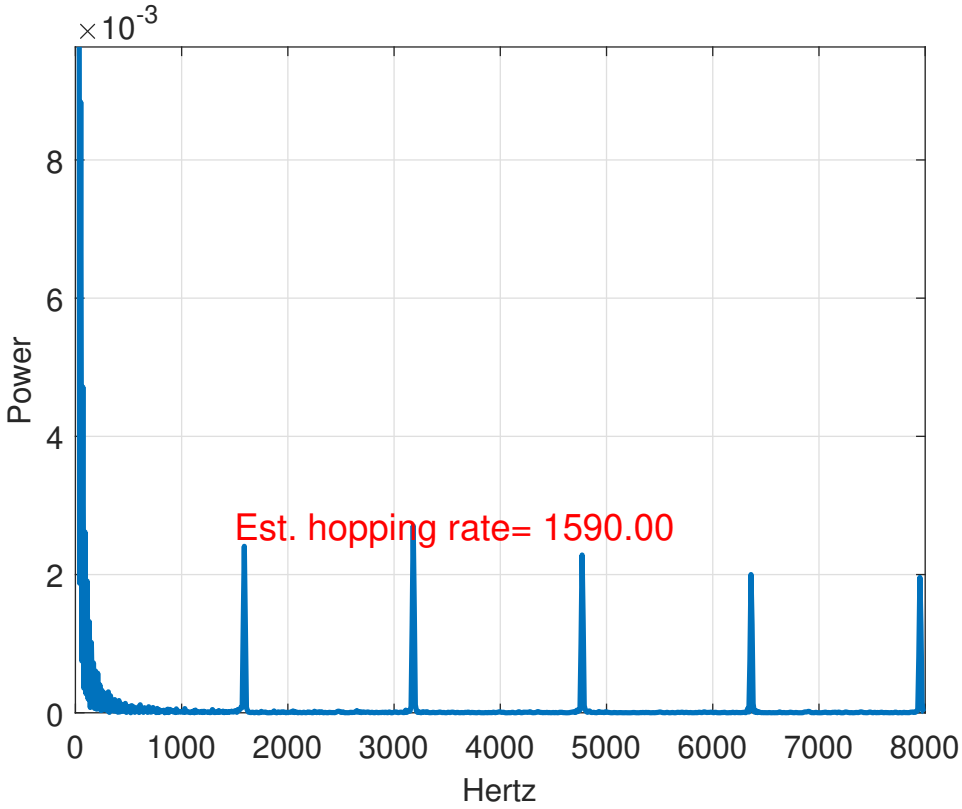


Figure 3.6 : The result of the SCF for the Bluetooth signal which has 1600 hop/sec.

to each other as discussed in Section 3.2. In order to show the output of the cyclostationarity analysis, a Bluetooth signal is simulated which has 1600 hop/sec. As can be seen in Fig. 3.6, cyclic peaks appear in the SCF. The fundamental frequency, which represents the hopping rate of the FHSS signal, is estimated as 1590 Hz. Next, the 4 FHSS signal sources are considered actively occupying the spectrum to employ time-frequency analysis as discussed in Section 3.2. Figure 3.7 exhibits the successful separation of multi FHSS signal sources correctly. Each colored rectangles indicate the consecutive hops that belong to the same FHSS signals. Even though bandwidth and the hopping durations are the same, the interested cluster can be formed by checking whether it starts at the same time or not. Thus, when the signal sources start at a random time, the multi FHSS signals, which show the same specifications, can be separated also.

The performance analyses are conducted with a Monte Carlo simulation. In the simulation environment, the channel conditions are considered as Rayleigh fading and the iteration number is determined as 2000. The probability of detection is obtained for

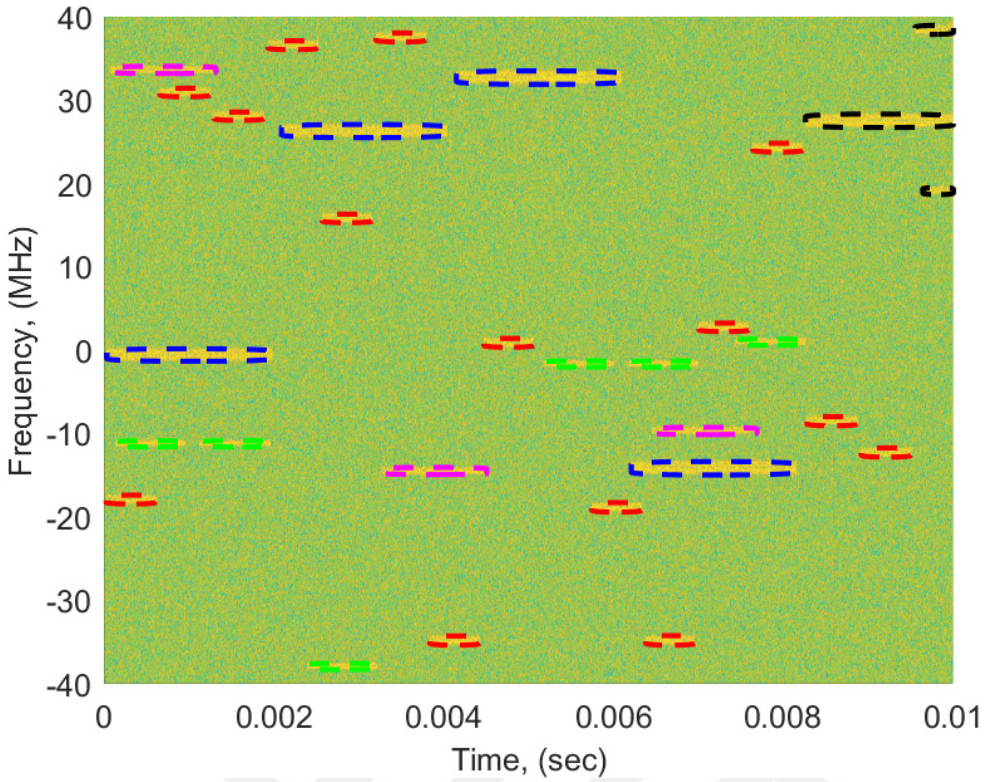


Figure 3.7 : After clustering the hops for different signals.

FHSS signals by comparing the number of clustered hops with the minimum number of hops that can be observed which is 50 hop/sec. For this analysis, the true detection rate is calculated as shown in Fig. 3.8. The results in Fig. 3.8 demonstrate the 0.9 detection accuracy is reached after the -4 dB SNR. Moreover, the detection performance is considered through the ROC curve. ROC curves are achieved for different SNR values as shown in Fig. 3.8. In Fig. 3.8, it can be inferred that the probability of detection has lower slopes in $P_{fa} = 0,1$ and $P_{fa} = 0,01$ for -4 dB SNR and 0 dB SNR values, respectively.

Since the cyclostationarity analysis estimates the hopping rate, it is important the measure the approximation on the true hopping rate. Therefore, the performance of the estimation of the hopping rate is calculated by root–mean–square–error (RMSE) which can be calculated as,

$$\text{RMSE} = \sqrt{\frac{1}{N_s}\sum_{i=1}^{N_s}\left(\hat{f}_i - f_i\right)^2} \tag{3.16}$$

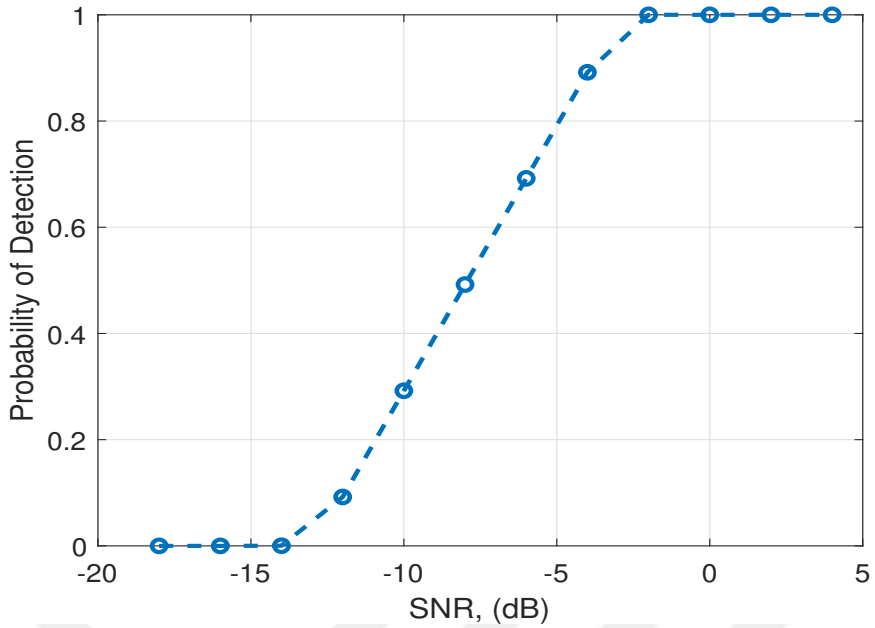


Figure 3.8 : The probability of detection rate is calculated by time-frequency analysis for FHSS signals.

where $\hat{f}$ is the estimated hopping rate and f denotes the true value of hopping rate. Also, N_s represents the number of iteration. For each iteration of the Monte Carlo simulation, the hopping rate of the FHSS signal is randomly changed. The error performance of the cyclostationarity analysis is shown in Fig. 3.10. Since the cyclostationarity analysis is based on matches between adjacent signals, more hops that captured will give a higher peak value in the hopping rate. Therefore, the hopping rate can be distinguishable more accurately for lower SNR values.

3.4 Real World Considerations for Signal Detection and Parameter Estimation

3.4.1 Measurement setup

Experimental setup for FHSS signal detection and parameter estimation is performed in Scientific and Technological Research Council of Turkey (TÜBİTAK) Informatics and Information Security Research Center (BİLGEM). The test–bed used in the data acquisition procedure consists of FHSS–type drone RC signal source and spectrum analyzer to record the signals.

Futaba T8J RC is used during the experiment as the FHSS signal source. It employs the first 50 MHz of a 2.4 GHz ISM frequency band which is divided into 30 RF channels

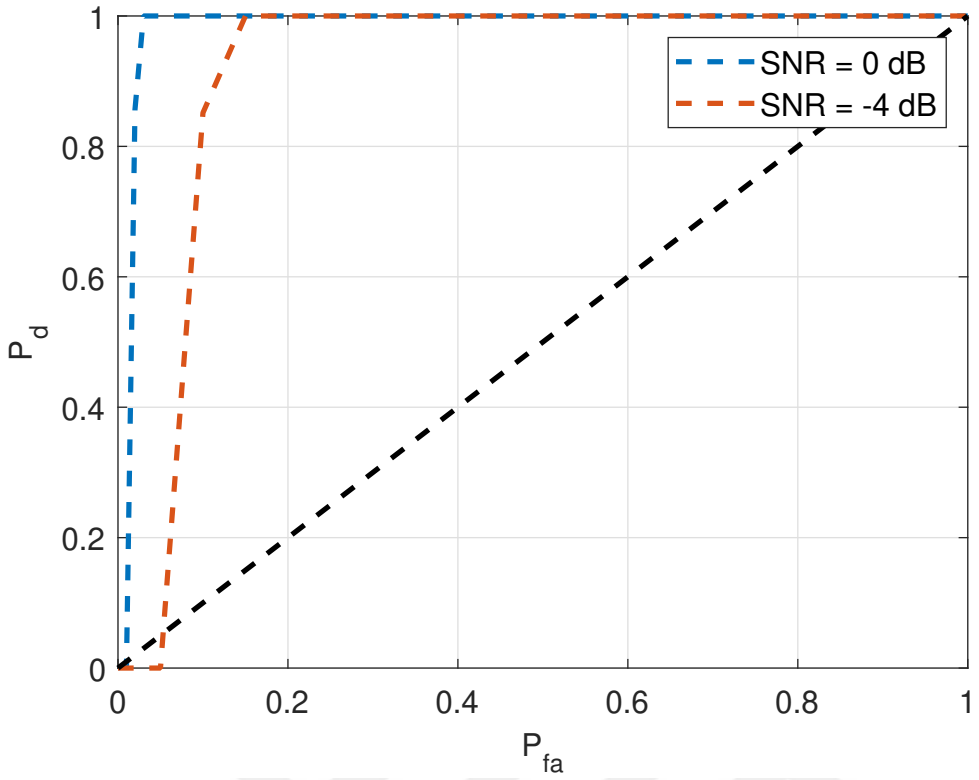


Figure 3.9 : ROC curve for time–frequency analysis in −4 dB and 0 dB SNR.

each with a channel width of 1.5 MHz [44]. The illustration of the hopping pattern of the FHSS signal source is shown in Fig. 3.11 where Δt_1, Δt_2, and Δt_3 represent the time gaps between the hops and their repetitions. These parameters are given by,

$$C_l = \begin{cases} T_h + \Delta t_1, & l \equiv 1 \mod 3 \\ T_h + \Delta t_2, & l \equiv 2 \mod 3 \\ T_h + \Delta t_3, & l \equiv 3 \mod 3. \end{cases} \tag{3.17}$$

The fundamental period of the Futaba T8J RC signal can be calculated as [44],

$$\underbrace{3T_h + \Delta t_1 + \Delta t_2 + \Delta t_3}_{C_1+C_2+C_3} = 6.8 \text{ ms} \tag{3.18}$$

where $\Delta t_1 < \Delta t_2 < \Delta t_3$.

In the receiver side, Rohde&Schwarz FSW 26 signal and spectrum analyzer (SSA) is utilized to record I/Q data. SSA can support the frequency range from 2 Hz to 26.5 GHz. The device provides real–time spectral analysis up to 160 MHz bandwidth. The signals are recorded over the 2.4 GHz ISM spectrum band with an omnidirectional

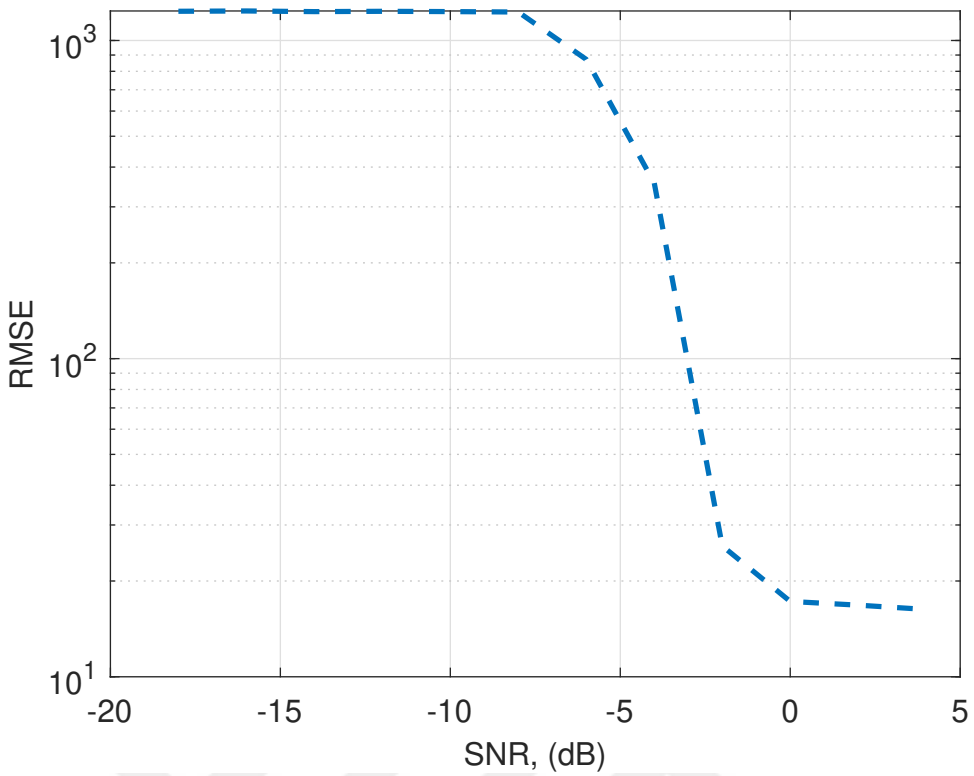


Figure 3.10 : RMSE performance of the cyclostationarity analysis for different SNR values.

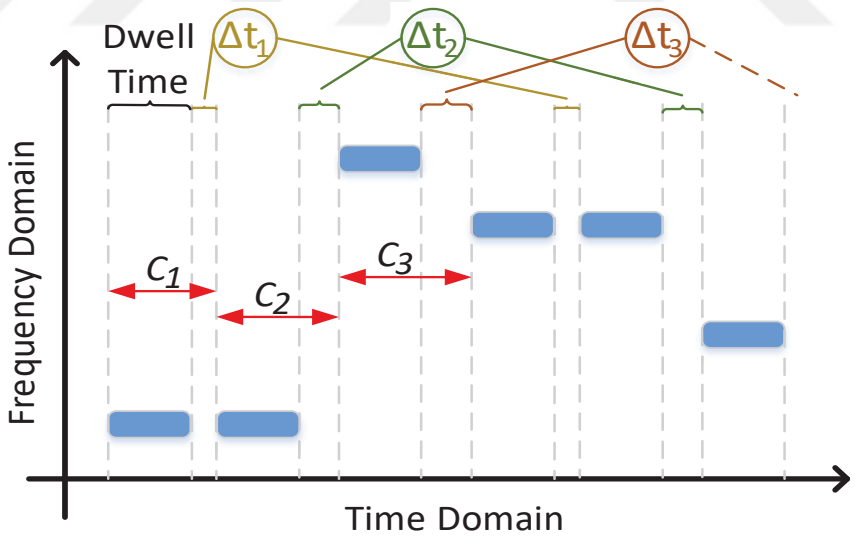


Figure 3.11 : The hopping pattern of the FHSS signal emitted by Futaba T8J RC.

antenna. The center frequency of SSA is set to 2.44 GHz and bandwidth of interest is adjusted to 80 MHz for the purpose of full coverage. Also, SSA is connected to external computer via an Ethernet cable in favor of achieving data storage with ease.

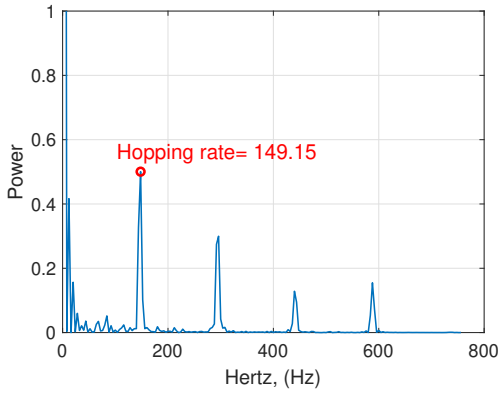


Figure 3.12a : Cyclostationarity signal analysis for drone RC signal.

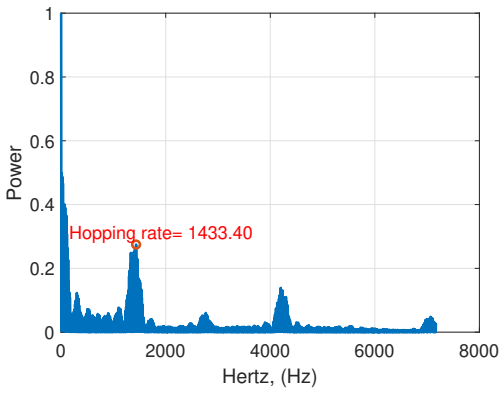


Figure 3.12b : Cyclostationarity signal analysis for Bluetooth signal.

Figure 3.12 : FHSS signal detection: Cyclostationarity Feature Detection.

Table 3.2 : Estimated parameters of FHSS signal.

Start Time (ms)	***Stop Time (ms)***	***Dwell Time (ms)***	***Center Frequency (GHz)***
1.7930	3.2403	1.4472	2.4271
5.1742	6.6086	1.4344	2.4414
6.7623	8.1967	1.4344	2.4414
8.6066	10.0410	1.4344	2.4211
11.9749	13.4221	1.4472	2.4039

The sampling rate depends on the analysis bandwidth of the real–time spectrum which is selected as 80 MS/s.

3.4.2 Measurement results

Over–the–air data collection is realized and the performance of time–frequency analysis method is evaluated. Captured signal includes real–world propagation effects such as multipath fading, interference, carrier frequency offsets. The drone RC signal and the Bluetooth signal are identified with the maximum peak of the cyclostationarity function that described the hopping rate of FHSS signals as seen in Fig. 3.12a and Fig. 3.12b.

Some of the estimated parameters of the real signal which measured at 25m distance can be found in Table 3.2. Considering the resolution in both time and frequency, the parameters are estimated within the ± 1 sample.

4. DIRECTION OF ARRIVAL ESTIMATION FOR FHSS SIGNALS

In Section 3 detection of FHSS signals and parameter extraction of each specific signal source are discussed. Using this information, the direction of the signal sources can be achieved with a passive system. Here, it is important to note that radio-–DF has a rich history and a very well–established literature on a wide variety of its application scenarios. Although, the majority of the DF algorithms present in the literature focus on a non–hopping carrier and operate on a narrow–band spectrum [45, 46].

DF techniques can be grouped under the following two categories: switched beam system (SBS) and adaptive array system (AAS) [47]. SBS method uses overlapping beams to scan the azimuth plane. The AoA is then determined by a search carried out across all over the candidate beam positions. Output is chosen to be the position yielding a maximum value for a defined cost function. It is important to state here that the SBS method benefits from the following two key points: firstly, it operates with a mechanically agile directional single antenna, and secondly, it does not require any baseband signal processing. Of course, these key points come at the expense of several shortcomings. For instance, the accuracy of SBS method relies heavily on SNR. This points out that detection range affects the performance significantly. Furthermore, statistical nature of wireless propagation generally implies poor SNR regimes for links especially within regulated but unlicensed bands where strict power limitations are imposed on the transmitters. Hence, optimal performance could only be achieved within the time slots when SNR is above a certain threshold. Therefore, the overall performance could be improved by prolonging the observation intervals, which is against the nature of the problem of interest. Such shortcomings necessitate more robust and responsive algorithms.

In contrast to SBS, AAS methods take advantage of smart antennas to steer the main beam in any desired direction and establish a continuous tracking. Beam steering is achieved by combining the weights of each antenna array element so that the maximum power is transferred spatially for a desired location or direction. Equipped with beam

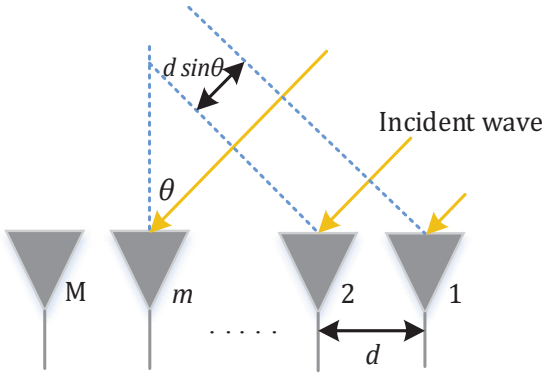


Figure 4.1 : The incident wave is impinging upon elements of the ULA structure for θ angle.

steering/tracking capability, AAS could be used in DF with the following two groups of techniques: conventional and subspace–based. Conventional methods form a power spectrum in such a way that look–direction gain is forced to be at unity gain while those of all other directions are minimized [48]. This way, a peak search could be carried out across the spectrum for the candidate angles/directions for the signal source of interest. It is noteworthy to indicate here that conventional techniques could operate in low SNR regimes to some extent. However, their computational complexities are higher as compared to those of AAS. On the other hand, subspace–based techniques focus on separating the signal subspace orthogonal to the noise subspace. With the advances in digital signal processing techniques and systems, subspace–based methods could be implemented and deployed rapidly [49].

In the AAS, different time delays occur since the impinging signals arrive to the antenna elements at different times as shown in Fig. 4.1. Therefore, after defining a reference element, the delay between the mth element and the reference element can be calculated as,

$$\tau_m = \frac{(m-1)\, d\, sin\theta}{c} \tag{4.1}$$

where d represents distance between adjacent elements, θ denotes the direction of arrival of a signal impinging upon the uniform linear array (ULA), and c stands for the speed of light. The received signal at mth element can be formed by using the delay amounts as,

$$
\begin{aligned}
y_m(t) &= e^{-j\omega\tau_m} y_1(t) = e^{-j\frac{2\pi}{\lambda}d(m-1)\sin\theta} x(t) \\
&= e^{j(m-1)\psi} x(t) = a(\psi)x(t)
\end{aligned}
\tag{4.2}
$$

where $y_1(t)$ represents the impinge signal to the reference element, $\psi = -\frac{2\pi}{\lambda}d\sin\theta$ is the spatial frequency, and $a(\psi)$ denotes the steering vector for the $x(t)$. Considering all the elements in ULA and the additive noise samples, we can write the received signal in a matrix format for p signal sources as,

$$
\mathbf{Y} = \mathbf{AX} + \mathbf{N}, \quad \mathbf{Y} \in \mathbb{C}^{M\times N} \tag{4.3}
$$

where $\mathbf{A}$ is the $M \times p$ matrix to the p steering vectors, $\mathbf{N}$ represents additive noise for M element.

4.1 Direction–Finding Algorithms

There have been various approaches for the direction of arrival algorithms. In this regard, subspace-based algorithms have shown better performance against minimum variance distortionless response (MVDR), the sum and delay which are spatial correlation methods. Among the aforementioned algorithms, the correlative interferometer needs a calibration process to fill a phase offset table and requires an odd number of antennas. In addition to this, pseudo-Doppler has a resolution problem. Regarding expectation-maximization, the result has a prominent accuracy but has difficult implementation problems, and also it requires prior information. Also, considering the real-world applications such as cluttered environment or NLOS conditions, correlative interferometry and pseudo-Doppler are not robust and the performance of these algorithms is dropped tremendously. Furthermore, MUSIC algorithm is robust under the multipath and mobility affects comparing the classical methods. Thus, we focus on MUSIC algorithm in this thesis.

4.1.1 Multiple signal classification algorithm

The input covariance matrix calculated as,

$$
\mathbf{R}_{yy} = \mathbb{E}[\mathbf{YY}^H] = \mathbf{AR}_{xx}\mathbf{A}^H + \sigma^2\mathbf{I}_M \tag{4.4}
$$

where $(\cdot)^H$ is the Hermitian transpose operator, $\mathbf{R}_{xx}$ stands for the signal correlation matrix, σ^2 denotes the noise variance with identity matrix $\mathbf{I}_M$. However, in practical applications, $\mathbf{R}_{yy}$ usually can not be directly obtained and only sample covariance can be used [50],

$$\tilde{\mathbf{R}}_{yy} = \frac{1}{L}\sum_{l=1}^{L} \mathbf{y}(t_l)\mathbf{y}^H(t_l) \tag{4.5}$$

where L represent the number of snapshot. In order to achieve the frequency content of the signal, multiple signal classification (MUSIC) uses the eigenvalue decomposition. If the corresponding eigenvalues of the $\tilde{\mathbf{R}}_{yy}$ are sorted in decreasing order, the largest p eigenvalues indicate the signal subspace and the remaining $(\mathrm{M}-p)$ eigenvalues of the $\tilde{\mathbf{R}}_{yy}$ represents the noise subspace. Therefore, using the signal and noise subspaces, pseudo–spectrum of phase can be calculated [51],

$$f_r(\theta) = \frac{1}{A_x(\theta)^H U_n U_n^H A_x(\theta)} \tag{4.6}$$

where $A_x(\theta)$ denotes the steering vector for $x(t)$ and U_n refers to the matrix of eigenvectors associated with the noise subspace. A search over **(4.6)** is performed to find maximum points as,

$$\hat{\theta} = \arg\max_{\theta} f_r(\theta) \tag{4.7}$$

where $\hat{\theta}$ is the estimated AoA of the signal.

4.1.2 root–MUSIC algorithm

The root–MUSIC method, in comparison to the MUSIC algorithm, finds the roots of a polynomial rather than plotting the pseudo spectrum or searching for peaks in the pseudo spectrum [52]. Same as the MUSIC algorithm, the covariance matrix can be estimated from several snapshots. Then, eigenvalue decomposition of the estimated covariance matrix is employed to obtain spectral function. The polynomial can be obtained by taking the inverse of the MUSIC spectrum and is given as [53],

$$f_r(\theta)^{-1} = A_x(\theta)^H U_n U_n^H A_x(\theta) \tag{4.8}$$

where steering vector and noise subspace are the same as in **(4.6)**. Considering the roots of the polynomial that are inside the unit circle, the closest p roots to unit circuit are selected. Finally, the estimation of the AoA can be determined by,

$$\hat{\theta} = \sin^{-1}\left[\psi \frac{\lambda}{2\pi d}\right] \tag{4.9}$$

where d is the distance between two adjacent elements, λ denotes the wavelength and ψ stands for the roots of $f_r(\theta)$.

4.2 Direction Finding of FHSS Signals

Although FHSS signals occupy a wide spectrum, each hop of FHSS signals has a lower bandwidth. On the other hand, an accurate estimation of the AoA needs continuity in the spectrum. For the case of FHSS signals, presence in a certain frequency with a short time is not enough for an accurate estimation. Many hops are combined sufficiently, the accumulated signal samples can be increased in a certain frequency which is the pre–processing step. In Fig. 4.2, the flow graph explains how the system works in brief. First, the received multi–channel signal is achieved using the ULA and cyclostationarity analysis of the received signal obtained from the first antenna is performed as discussed in Section 3.1.2.1. After ensuring the cyclostationarity feature of the drone RC, parameters of the signal are estimated to reconstruct the FHSS signal for the received signal array. Furthermore, the resampling process is employed to decrease the signal sample rate and reduce the computational complexity. In the last step, AoA of the FHSS signal is achieved by using subspace–based algorithms.

4.2.1 Reconstruction of FHSS signals

There are many different topologies for the antenna array. Considering the ULA enumerated with $0, 1, \ldots, \mathrm{M}$ elements, **(2.5)** can be expanded for any mth antenna element as,

$$r_m(t) = \underbrace{h_m(t) * x(t)}_{y_m(t)} + n_m(t) + i_m(t) \tag{4.10}$$

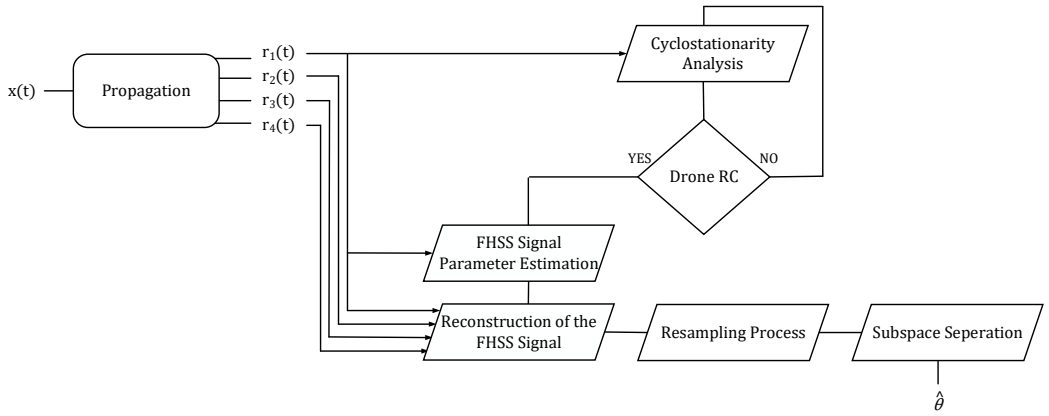


Figure 4.2 : Overall block diagram of the system.

$h_m(t)$ is the channel impulse response between the mth element and signal source, which has frequency flat fading and $n_m(t)$ stands for the complex AWGN in which I and Q components are i.i.d $\sim \mathcal{N}(0, \sigma^2/2)$.

A signal received in a wideband spectrum bears much higher noise level for each hop of an FHSS signal that makes it almost impossible to distinguish it from the desired signal. Therefore, extraction each hop from the wideband spectrum and estimation of parameters of the FHSS signal are required as discussed in Section 3.2. Then, the received signal can be filtered by using the lower and upper frequency band, i.e, $[f_L, f_H]$, of each hop for a estimated start and end time interval. A bandpass filter is designed to obtain each hop from the spectrum and suppress other signals in the same time interval. This approach also eliminates the unwanted noise from the signal. After filtering the hops of the FHSS signal, each hop is shifted to achieve equivalent baseband signal considering estimated center frequencies.

Let $\hat{z}(t)$ be the filtered and shifted version of each hop to its baseband frequency. It can be described as,

$$\hat{z}(t) = r(t) \times \sum_{k=1}^{K} e^{-j(2\pi \hat{f}_k t)} w_k(t - B_k) \tag{4.11}$$

where $r(t)$ is the received signal, $\hat{f}_k = (f_L + f_H)/2$ denotes the estimated center frequency of kth hop, $B_k = \sum_{l=1}^{k-1} C_l$ and C_l refers to the time difference between start time of lth and $(l+1)$th hop. Then, $\hat{z}_k(t)$, which is baseband equivalent and also shifted to the interval $[0, T_h]$ of the kth hop, can be expressed as,

$$\hat{z}_k(t) = \begin{cases} \hat{z}(t+(k-1)T_h+B_k),\ t \in [O, T_h] \\ 0, \qquad\qquad\qquad\quad \text{others} \end{cases} \tag{4.12}$$

In order to increase the signal resolution at baseband frequency, time gaps between hops should be removed. Therefore, we define a concatenated function, $\hat{f}(t)$, as,

$$\hat{f}(t) = \sum_{k=1}^{K} \hat{z}_k(t-(k-1)T_h). \tag{4.13}$$

As a result, by combining **(4.11)**, **(4.12)**, **(4.13)** the whole reconstruction process from $r(t)$ to $\hat{f}(t)$ can be seen as:

$$\hat{f}(t_k) = \sum_{k=1}^{K} \left[r(t_k+B_k) \times \sum_{m=1}^{K} e^{-j(2\pi \hat{f}_m(t_k+B_k))} w_m(t_k) \right] \tag{4.14}$$

where $t_k \in [(k-1)T_h, kT_h]$. Note this process is realized for every received signal from each antenna.

In the final step before executing the AoA algorithm, the resampling process is employed. Considering the multi-rate filters, it can provide upsampling and downsampling with a P-to-Q rational rate. Since the measurements consist of the wideband spectrum, each hop of the FHSS signal has a smaller bandwidth than the captured wideband spectrum. After achieving the reconstructed version of the FHSS signal, the signal can be modeled as none frequency hopping which eliminates the spreading. Thus, the signal can be sampled with a much lower sampling rate depending on each hop's bandwidth. In this regard, the P-to-Q rate can be determined with the bandwidth of each hop of the FHSS signal and sampling rate [54, 55]. The input signal is upsampled by adding zeros between samples of the original signal. After that, an FIR anti–aliasing filter was applied to eliminate discontinuities. In the last step, filtered signal samples are discarded to decimate the signal, and samples are kept at each downsample step size. It is important to note that, phase of the input signal can change while applying the resampling process [54]. However, since the resampling process shifts the phase of each reconstructed signal in the same manner, the phase difference between channels does not change. Thus, the result of the AoA is not affected. Furthermore, this approach also reduce the computational complexity during covariance matrix evaluation.

High resolution in both time and frequency cannot be achieved when calculating STFT. If the window is wider, the better frequency resolution is achieved but this leads to less time resolution and vice versa. The extraction of the temporal information, carrier frequency, and bandwidth of the signals depends on the resolution of the STFT. For instance, when the window is selected for a higher frequency resolution, the temporal parameters are estimated with margins as shown in Fig. 4.3a. Considering the slicing of the hops in the time domain according to the start and end time which are estimated with margins, the reconstructed signal contains more noise samples. Since the eigenstructure-based algorithms separate the signal and noise subspaces, it is expected that result of the direction of arrival is barely affected or even not, due to resolution errors. Furthermore, if the time parameters are estimated more accurately, the frequency parameters are estimated with margins as shown in Fig. 4.3b. Therefore, the shift in the frequency domain might be affected by frequency resolution slightly, but the low pass filter ensures that the hops of the FHSS signal remain below the cutoff frequency which is determined as the bandwidth of the hops. Moreover, the performance analysis is employed to calculate the RMSE for the ideal signal transition case (the green shaded region in Fig. 4.3a) as well as signal transition with margins (the yellow shaded region in Fig. 4.3b). The result of the RMSE between these conditions has approximately the same form as shown in Fig. 4.4.

4.3 Real World Considerations for Direction–Finding of FHSS Signals

The AoA estimation of FHSS signals is performed for signals captured by using over–the–air received signals by using the ULA. The measurements are taken in the test field of TÜBİTAK BİLGEM in Gebze, Turkey. Measurements are conducted at a suburban area with a hilly terrain structure and foliage, which is close to the Sea of Marmara for both line–of–sight (LOS) and non–line–of–sight (NLOS) conditions.

4.3.1 Hardware setup

The test–bed consists of the Futaba T8J drone RC as an FHSS signal source, four identical quasi Yagi antennas, and one National Instruments (NI) PXIe receiver to support the multiple input structure as shown in Fig. 4.5. Four identical antennas are utilized to construct our AAS. In AAS, it is preferred to utilize ULA for the AoA

Algorithm 1: Resampling process

Input: Complex baseband signal ($\hat{f}(t)$), estimated bandwidth ($\hat{bw}$), sampling rate (f_s)
Result: Resampled signal ($\hat{f}_{RS}(t)$)
Initilizations:
  N = length($\hat{f}(t)$)
  $n \leftarrow$ the numerator for the fractional rate between $\hat{bw}, f_s$
  $d \leftarrow$ the denominator for the fractional rate between $\hat{bw}, f_s$
  $f_{cutoff} = \frac{\pi}{max(n,d)}$ rad/sample
  Filter order $\leftarrow 2 \times k \times max(n,d)$, where $k = 50$
for *i=0 to N-1* **do**
  if $(i/n) == floor(i/n)$ **then**
    $f_M(i) = \hat{f}(i/n)$
  else
    $f_M(i) = 0$
  end
end
$h_{AA} \leftarrow$ *fir*(Filter order, f_{cutoff}, Kaiser window)
$p = f_M * h_{AA}$
for *i=0 to* $n \times N - 1$ **do**
  $\hat{f}_{RS}(i) = p(i \times d)$
end

process. A ULA structure is constructed with four identical quasi Yagi antennas. The separation distance between each adjacent antenna element is kept as $\lambda/2 \approx 6.2$ cm where λ is the wavelength at 2.42 GHz. Furthermore, the height of antennas is set at approximately 1.5–meter and thus, reflections from the ground are avoided. The signal from each antenna are received synchronously with the help of a NI PXIe–1065 four–channel receiver. NI PXIe–1065 receiver chassis consists of four major parts: one NI PXIe–8108 embedded controller, one NI PXI–5652 RF signal generator, four NI PXIe–5622 digitizer which has a 16–bit resolution and four NI PXIe–5601 RF downconverter in which each downconverter covers the frequency range 10 MHz to 6.6 GHz and has a 50 MHz instantaneous bandwidth. The corresponding block diagram of our setup is shown in Fig. 4.6.

4.3.2 Experimental procedures

Since the signal source operates in the 2.4 GHz – 2.45 GHz spectrum, it spans over 50 MHz bandwidth. At this point, while the signal is captured at a high sample rate, only a section of the spectrum has been considered to prevent data overflow. Therefore, the

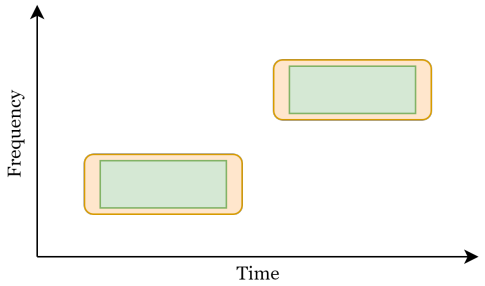


Figure 4.3a : STFT representation under the better frequency resolution. Green box is the ground truth for the signal and yellow box is the estimated region.

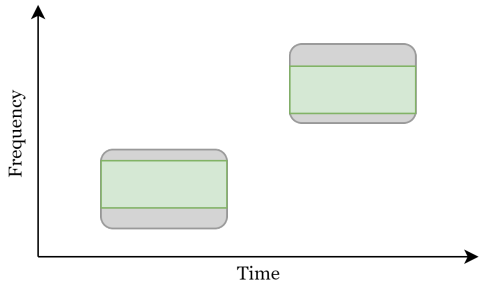


Figure 4.3b : STFT representation under the better time resolution. Green box is the ground truth for the signal and grey box is the estimated region.

Figure 4.3 : Extracting the temporal information, carrier frequency, and bandwidth representation with different resolution.

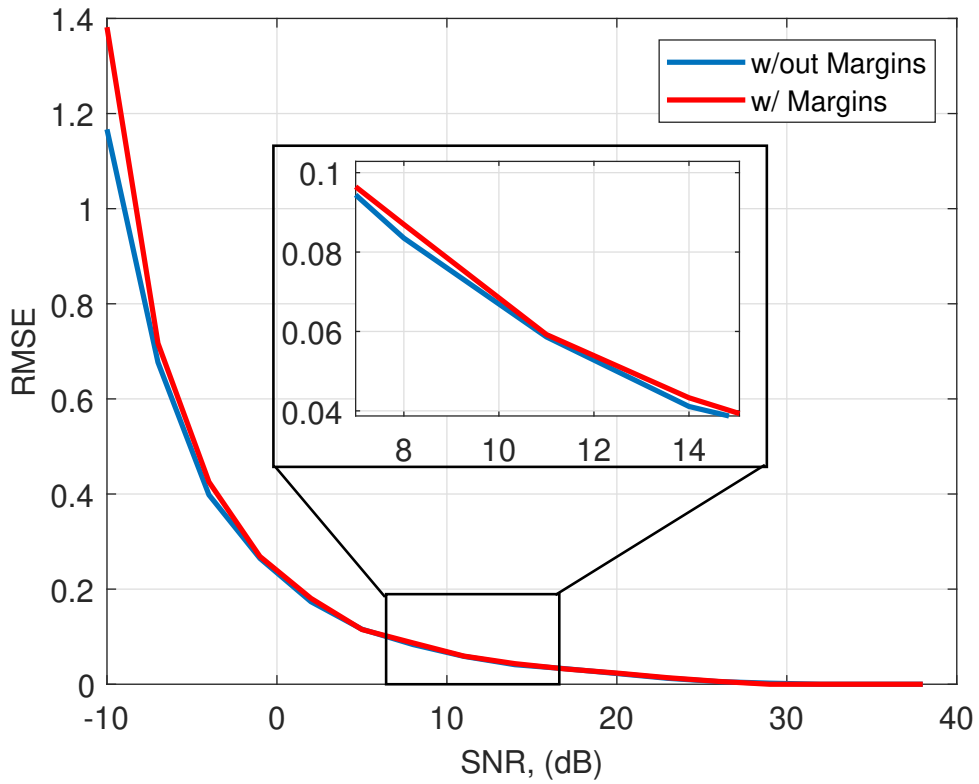
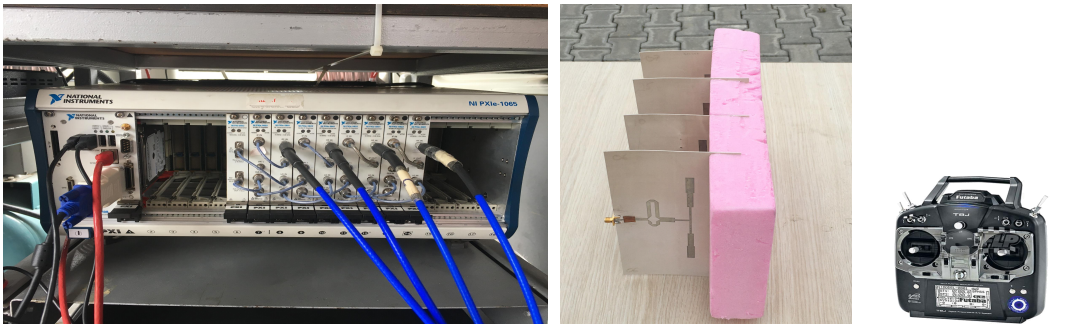


Figure 4.4 : The performance comparison between the perfectly slicing the signal and slicing the signal with margins.

bandwidth of interest is adjusted to 10 MHz and resulting sampling rate is 20 MS/s. The center frequency is set to 2.42 GHz to monitor the spectrum where the hops of the FHSS signal will likely appear the most.



NI PXIe Receiver | Quasi-Yagi Antenna Set | Futaba T8J Drone RC

Figure 4.5 : The test-bed of the measurement campaign.

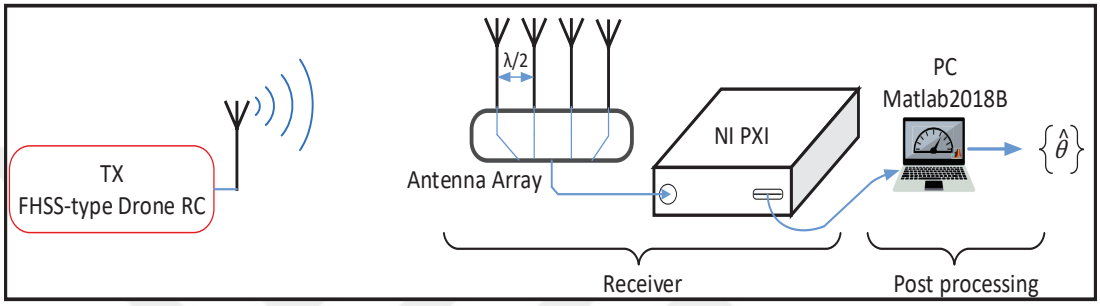


Figure 4.6 : Block diagram of measurement setup.

One should note that the accuracy of the MUSIC and root–MUSIC algorithms highly depends on the phase of the received signal. If there is a phase difference between each receiver before the measurement campaign, the performance of the algorithms degrade tremendously. In order to ensure the phase coherency between each receiver, we perform a calibration procedure to cancel out the possible phase mismatches that can occur from local oscillator errors and environmental factors such as cable length etc. [56].

4.3.2.1 Calibration process

First, a signal generator is configured to generate a narrowband signal at 2.42 GHz. The signal generator is placed right across the ULA to guarantee 0° for AoA. Four–channel receiver is set at 2.42 GHz. Phase differences of each antenna are calculated according to the reference antenna. Also, this process is implemented in the LabVIEW program. Finally, once the phase difference are calculated, each phase difference value is integrated into the measurement process before starting the measurement campaign. Thus, phase coherency is assured across the receivers.

4.3.3 Measurement results

The DF results obtained for the received signals with pre–processing and without pre–processing stages for MUSIC and root–MUSIC algorithms are exhibited. In order to check the accuracy of the proposed method, the true AoA values, θ_G, for each drone RC location are calculated by using Garmin GPSmap 62sc and Google Earth Pro. The true AoA values for each drone RC location are $\{4.43°, 6.41°, 8.55°, 10.33°, 2.1°\}$ for 115.24m, 164.74m, 214.74m, 264.62m and 512m, respectively.

The comparison of estimated AoAs for MUSIC and root–MUSIC algorithms illustrates that the pseudo spectrum is shifted with a miscalculated value. For instance, the phase–spectrum of the measurement that is taken from a 115.24-meter distance is calculated for with processing and without processing as shown in Fig. 4.7. It clearly indicates that pre–processing of the received signal array improves the DF estimation of FHSS signals. As seen in Table 4.1, Table 4.2, Table 4.3, Table 4.4, and Table 4.5, the results are exhibited based on different antenna numbers, processing effects, and different estimators. The results show that angle accuracy is improved with antenna number and pre–processing effect. It is also noted that environment characteristics of the measurement campaign affects the performance of the proposed algorithm. In Table 4.5, the results are calculated for the signal that is captured at the farthest distance while considering LOS condition. According to the Table 4.1, Table 4.2, Table 4.3, and Table 4.4 which are the NLOS cases, the increase in the Tx–Rx separation degrades the results. On the other hand, at 512m which is the LOS case, the difference between true value and estimated value is only 1.10°.

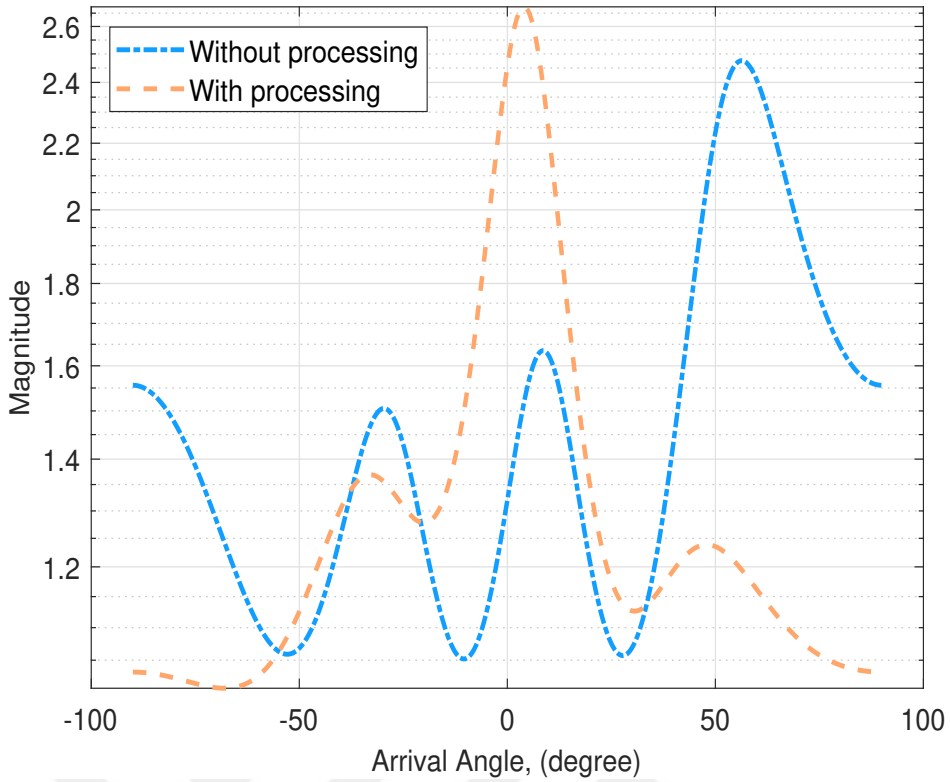


Figure 4.7 : MUSIC phase—spectrum for different processing methods.

Table 4.1 : AoA estimations of drone RC where has a 4.43° angle position at 115.24 meters apart from the antenna array with respect to a different number of antennas (M). The best estimation for drone RC is highlighted in boldface font.

M	**Processing Effect**	**Estimator**	**Angle of Arrival**		
			θ_G	$\hat{\theta}$	Diff.
		Google Earth	4.43°		
2	Without Pre–processing	root-MUSIC		16.74°	12.31°
		MUSIC		16.70°	12.27°
	With Pre–processing	root-MUSIC		28.20°	23.77°
		MUSIC		28.20°	23.77°
3	Without Pre–processing	root-MUSIC		44.28°	39.85°
		MUSIC		43.50°	39.07°
	With Pre–processing	root-MUSIC		16.61°	12.18°
		MUSIC		16.60°	12.17°
4	Without Pre–processing	root-MUSIC		56.29°	51.86°
		MUSIC		56.30°	51.87°
	With Pre–processing	root-MUSIC		4.54°	**0.11°**
		MUSIC		4.30°	−0.13°

Table 4.2 : AoA estimations of drone RC where has a 6.41° angle position at 164.74 meters apart from the antenna array with respect to a different number of antennas (M). The best estimation for drone RC is highlighted in boldface font.

M	Processing Effect	Estimator	Angle of Arrival		
			θ_G	$\hat{\theta}$	Diff.
		Google Earth	6.41°		
2	Without Pre–processing	root-MUSIC		19.53°	13.12°
		MUSIC		19.50°	13.09°
	With Pre–processing	root-MUSIC		30.72°	24.31°
		MUSIC		30.70°	24.29°
3	Without Pre–processing	root-MUSIC		42.67°	36.26°
		MUSIC		42.00°	35.59°
	With Pre–processing	root-MUSIC		19.89°	13.48°
		MUSIC		19.90°	13.49°
4	Without Pre–processing	root-MUSIC		56.15°	49.74°
		MUSIC		56.10°	49.69°
	With Pre–processing	root-MUSIC		7.74°	1.33°
		MUSIC		7.70°	**1.29°**

Table 4.3 : AoA estimations of drone RC where has a 8.55° angle position at 214.74 meters apart from the antenna array with respect to a different number of antennas (M). The best estimation for drone RC is highlighted in boldface font.

M	Processing Effect	Estimator	Angle of Arrival		
			θ_G	$\hat{\theta}$	Diff.
		Google Earth	8.55°		
2	Without Pre–processing	root-MUSIC		16.63°	8.08°
		MUSIC		16.60°	8.05°
	With Pre–processing	root-MUSIC		33.46°	24.91°
		MUSIC		33.50°	24.95°
3	Without Pre–processing	root-MUSIC		43.47°	34.92°
		MUSIC		42.80°	34.25°
	With Pre–processing	root-MUSIC		23.69°	15.14°
		MUSIC		23.70°	15.15°
4	Without Pre–processing	root-MUSIC		56.82°	48.27°
		MUSIC		56.80°	48.25°
	With Pre–processing	root-MUSIC		10.26°	1.71°
		MUSIC		10.20°	**1.65°**

Table 4.4 : AOA estimations of drone RC where has a 10.33° angle position at 264.62 meters apart from the antenna array with respect to a different number of antennas (M). The best estimation for drone RC is highlighted in boldface font.

M	Processing Effect	Estimator	Angle of Arrival		
			θ_G	$\hat{\theta}$	Diff.
		Google Earth	10.33°		
2	Without Pre–processing	root-MUSIC		16.44°	6.11°
		MUSIC		16.40°	6.07°
	With Pre–processing	root-MUSIC		29.75°	19.42°
		MUSIC		29.70°	19.37°
3	Without Pre–processing	root-MUSIC		44.48°	34.15°
		MUSIC		43.90°	33.57°
	With Pre–processing	root-MUSIC		24.39°	14.06°
		MUSIC		24.40°	14.07°
4	Without Pre–processing	root-MUSIC		56.61°	46.28°
		MUSIC		56.60°	46.27°
	With Pre–processing	root-MUSIC		12.92°	**2.59°**
		MUSIC		13.10°	2.77°

Table 4.5 : AoA estimations of drone RC where has a 2.10° angle position at 512.00 meters apart from the antenna array with respect to a different number of antennas (M). The best estimation for drone RC is highlighted in boldface font.

M	Processing Effect	Estimator	Angle of Arrival		
			θ_G	$\hat{\theta}$	Diff.
		Google Earth	2.10°		
2	Without Pre–processing	root-MUSIC		47.35°	45.25°
		MUSIC		47.40°	45.30°
	With Pre–processing	root-MUSIC		35.50°	33.40°
		MUSIC		35.50°	33.40°
3	Without Pre–processing	root-MUSIC		57.16°	55.06°
		MUSIC		57.20°	55.10°
	With Pre–processing	root-MUSIC		14.20°	12.10°
		MUSIC		14.20°	12.10°
4	Without Pre–processing	root-MUSIC		67.56°	65.46°
		MUSIC		67.20°	65.10°
	With Pre–processing	root-MUSIC		3.33°	1.23°
		MUSIC		3.20°	**1.10°**

5. Concluding Remarks and Future Directions

Safety, security, and privacy are three critical concerns affiliated with the use of drones in everyday life. Considering their ever–shrinking sizes and capabilities, being aware of drone activities in the vicinity becomes an important surveillance item. Therefore, keeping track of drones and preferably their controllers should be included into the already–existing security measures. Therefore, this thesis focuses on the problem of identification and AoA estimation of real–world drone RC signals. For this purpose, cyclostationarity based signal identification and time–frequency analysis are applied to distinguish FHSS signals such as drone RC and Bluetooth signals. Once the drone RC signal is identified, rather than directly feeding wideband signals to the AoA algorithm, the performance of the DF with the reconstruction of FHSS signals is discussed. For this reason, time–frequency analysis is used to get the correct FHSS signal to reconstruct in the baseband center which leads to the accurate estimation of AoA. Also, real–world conditions are considered for the signal detection and estimation of DF. The performance results show that gathering the hopping signal samples at a frequency point against the noise will improve the performance of DF estimation for FHSS signals.

Some of the potential future research directions that require further investigation are:

- Adopting the recently emerging deep learning algorithms to distinguish FHSS signals among the standard-based wireless signals.
- Kalman filtering can be considered for the tracking of the hops of an FHSS signals and use different subspace–based AoA estimation methods such as Fourier domain MUSIC algorithm.
- For the case that the multiple FHSS signals exist, the probability of correct clustering under the different conditions for various SNR values can be examined.

REFERENCES

[1] **Zhang, L.**, **Liang, Y.C. and Xiao, M.** (2018). Spectrum sharing for Internet of Things: A survey, *IEEE Wireless Communications*, *26*(3), 132–139.

[2] **Marcus, M.J.** (2012). Spectrum policy for radio spectrum access, *Proceedings of the IEEE*, *100*(Special Centennial Issue), 1685–1691.

[3] **Wilson, W.J.** (2001). Applying layering principles to legacy systems: Link 16 as a case study, *2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No. 01CH37277)*, volume 1, IEEE, pp.526–531.

[4] **Roberson, D.A.**, **Hood, C.S.**, **LoCicero, J.L. and MacDonald, J.T.** (2006). Spectral occupancy and interference studies in support of cognitive radio technology deployment, *2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, IEEE, pp.26–35.

[5] **Hayat, S.**, **Yanmaz, E. and Muzaffar, R.** (2016). Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint, *IEEE Commun. Surveys Tuts.*, *COMST-18*(4), 2624–2661.

[6] **FAA**, UAS Sightings Report, Available: `https://bit.ly/2ZJIzdy`, Accessed: October 10, 2020.

[7] **Bannister, A.**, Dangerous drone encounters at UK airports jump by more than a third, Available: `https://bit.ly/2VvsDM8`, Accessed: November 20, 2020.

[8] **O'Malley, J.** (2019). The no drone zone, *Engineering & Technology*, *14*(2), 34–38.

[9] **Popovski, P.**, **Yomo, H. and Prasad, R.** (2006). Strategies for adaptive frequency hopping in the unlicensed bands, *IEEE Wireless Communications*, *13*(6), 60–67.

[10] **Russer, P.** *et al.* (2004). Signal processing for wideband smart antenna array applications, *IEEE microwave magazine*, *5*(1), 57–67.

[11] **Dakulagi, V. and Bakhar, M.** (2020). Advances in smart antenna systems for wireless communication, *Wireless Personal Communications*, *110*(2), 931–957.

[12] **Torrieri, D.** (2005). *Principles of spread-spectrum communication systems*, volume 1, Springer.

[13] **Olšovskỳ, P. and Podhoranskỳ, P.** Design and simulation of frequency hopping technique in MATLAB, *Inst. of Electro. and Photonics, Faculty of Electrical Engineering and Info. Tech., Slovak Univ of Tech., Bratislava*.

[14] **Tsai, Y.R. and Chang, J.F.** (1994). Using frequency hopping spread spectrum technique to combat multipath interference in a multiaccessing environment, *IEEE transactions on vehicular technology*, *43*(2), 211–222.

[15] **Gardner, W. and Franks, L.** (1975). Characterization of cyclostationary random signal processes, *IEEE Transactions on information theory*, *21*(1), 4–14.

[16] **Gardner, W.A. and Spooner, C.M.** (1992). Signal interception: performance advantages of cyclic-feature detectors, *IEEE Transactions on Communications*, *40*(1), 149–159.

[17] **Napolitano, A.** (2016). Cyclostationarity: New trends and applications, *Signal processing*, *120*, 385–408.

[18] **Derakhshani, M.**, **Le-Ngoc, T. and Nasiri-Kenari, M.** (2011). Efficient cooperative cyclostationary spectrum sensing in cognitive radios at low SNR regimes, *IEEE Transactions on wireless communications*, *10*(11), 3754–3764.

[19] **Spooner, C.M.**, **Mody, A.N.**, **Chuang, J. and Petersen, J.** (2017). Modulation recognition using second-and higher-order cyclostationarity, *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, IEEE, pp.1–3.

[20] **Dobre, O.A.**, **Abdi, A.**, **Bar-Ness, Y. and Su, W.** (2010). Cyclostationarity-based modulation classification of linear digital modulations in flat fading channels, *Wireless Personal Communications*, *54*(4), 699–717.

[21] **Dobre, O.A.**, **Venkatesan, R.**, **Popescu, D.C.** *et al.* (2011). Second-order cyclostationarity of mobile WiMAX and LTE OFDM signals and application to spectrum awareness in cognitive radio systems, *IEEE Journal of Selected Topics in Signal Processing*, *6*(1), 26–42.

[22] **Serpedin, E. and Giannakis, G.B.** (1998). Blind channel identification and equalization with modulation-induced cyclostationarity, *IEEE Transactions on Signal Processing*, *46*(7), 1930–1944.

[23] **Dandawate, A.V. and Giannakis, G.B.** (1994). Statistical tests for presence of cyclostationarity, *IEEE Transactions on signal processing*, *42*(9), 2355–2369.

[24] **Giannakis, G.B. and Madisetti, V.**, (1998). Cyclostationary signal analysis, Digital Signal Processing Handbook, volume 31, pp.17–1.

[25] **Gardner, W.A.** (1991). Exploitation of spectral redundancy in cyclostationary signals, *IEEE Signal Process. Mag.*, *8*(2), 14–36.

[26] **Cohen, L.** (1995). *Time-frequency analysis*, volume778, Prentice hall.

[27] **Flandrin, P.**, **Amin, M.**, **McLaughlin, S. and Torrésani, B.** (2013). Time-frequency analysis and applications, *IEEE signal processing magazine*, *30*(6), 19.

[28] **Sejdić, E.**, **Djurović, I. and Jiang, J.** (2009). Time–frequency feature representation using energy concentration: An overview of recent advances, *Digital signal processing*, *19*(1), 153–183.

[29] **Durak, L. and Arikan, O.** (2003). Short-time Fourier transform: two fundamental properties and an optimal implementation, *IEEE Transactions on Signal Processing*, *51*(5), 1231–1242.

[30] **Hess-Nielsen, N. and Wickerhauser, M.V.** (1996). Wavelets and time-frequency analysis, *Proceedings of the IEEE*, *84*(4), 523–540.

[31] **Durka, P.J.**, **Ircha, D. and Blinowska, K.J.** (2001). Stochastic time-frequency dictionaries for matching pursuit, *IEEE Transactions on Signal Processing*, *49*(3), 507–510.

[32] **Candès, E.J. and Wakin, M.B.** (2008). An introduction to compressive sampling, *IEEE signal processing magazine*, *25*(2), 21–30.

[33] **Gilbert, A.C.**, **Indyk, P.**, **Iwen, M. and Schmidt, L.** (2014). Recent developments in the sparse Fourier transform: A compressed Fourier transform for big data, *IEEE Signal Processing Magazine*, *31*(5), 91–100.

[34] **Liu, F.**, **Marcellin, M.W.**, **Goodman, N.A. and Bilgin, A.** (2016). Compressive sampling for detection of frequency-hopping spread spectrum signals, *IEEE Transactions on Signal Processing*, *64*(21), 5513–5524.

[35] **Su, H. and Zhang, Y.** (2016). Time-frequency analysis based on Compressive Sensing, *2016 2nd International Conference on Cloud Computing and Internet of Things (CCIOT)*, IEEE, pp.138–142.

[36] **Davenport, M.A.**, **Laska, J.N.**, **Treichler, J.R. and Baraniuk, R.G.** (2012). The pros and cons of compressive sensing for wideband signal acquisition: Noise folding versus dynamic range, *IEEE Transactions on Signal Processing*, *60*(9), 4628–4642.

[37] **Kim, N.K. and Oh, S.J.** (2017). Comparison of methods for parameter estimation of frequency hopping signals, *International Conference on Information and Communication Technology Convergence (ICTC)*, pp.567–569.

[38] **Smith, J.**, **for Computer Research in Music, S.U.C.**, **Acoustics and of Music, S.U.D.** (2011). *Spectral Audio Signal Processing*, W3K, `https://ccrma.stanford.edu/~jos/sasp/`, online book, 2011 edition.

[39] **Haralick, R.M.**, **Sternberg, S.R. and Zhuang, X.** (1987). Image analysis using mathematical morphology, *IEEE Trans. Pattern Anal. Mach. Intell.*, (4), 532–550.

[40] **Luo, L.** *et al.* (2009). Detection of an unknown frequency hopping signal based on image features, *2nd International Congress on Image and Signal Processing*, pp.1–4.

[41] **Xu, R. and Wunsch, D.** (2005). Survey of clustering algorithms, *IEEE Transactions on neural networks*, *16*(3), 645–678.

[42] Bluetooth Special Interest Group, (2016). Bluetooth Core Specification.

[43] **Rozenbeek, D.J.**, (2020), Evaluation of Drone Neutralization Methods using Radio Jamming and Spoofing Techniques, page=14, Table 2.3.

[44] **Blog, R.E.F.**, Futaba S–FHSS Protocol Overview, Available: `https://bit.ly/2zvueGL`, Accessed: October 10, 2020.

[45] **Tuncer, T.**, **Yasar, T. and Friedlander, B.** (2007). Direction of arrival estimation for nonuniform linear arrays by using array interpolation, *Radio science*, *42*(4).

[46] **Bakhar, M.**, **Vani, R.**, **Hunagund, P.** *et al.* (2014). Implementation and optimization of modified MUSIC algorithm for high resolution DOA estimation, *IEEE Intl. Microwave and RF Conf.*, pp.190–193.

[47] **Badawy, A.**, **Khattab, T.**, **Trinchero, D.**, **ElFouly, T. and Mohamed, A.** (2017). A Simple Angle of Arrival Estimation Scheme, *IEEE WCNC Wireless Commun. and Netw. Conf.*, San Francisco, CA, USA, pp.1–6.

[48] **Capon, J.** (1969). High–resolution frequency–wavenumber spectrum analysis, *Proc. IEEE*, *57*(8), 1408–1418.

[49] **Baig, N.A. and Malik, M.B.** (2013). Comparison of direction of arrival (DOA) estimation techniques for closely spaced targets, *Intl Jnl. of Future Comp. and Comm.*, *2*(6), 654.

[50] **Barabell, A.** (1983). Improving the resolution performance of eigenstructure-based direction-finding algorithms, *ICASSP'83. IEEE International Conference on Acoustics, Speech, and Signal Processing*, volume 8, IEEE, pp.336–339.

[51] **Schmidt, R.** (1986). Multiple emitter location and signal parameter estimation, *IEEE Trans. Antennas Propag.*, *34*(3), 276–280.

[52] **Vesa, A.** (2010). Direction of arrival estimation using MUSIC and root–MUSIC algorithm, *18th Telecom. Forum, Pg*, pp.582–585.

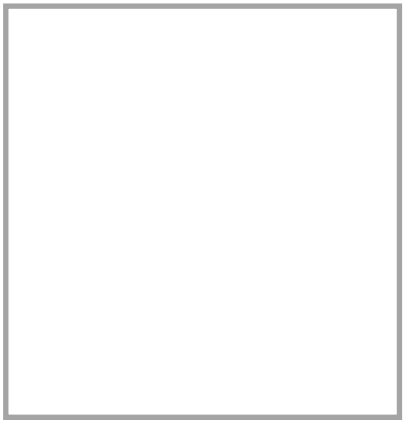
[53] **Liao, Y.**, **Abouzaid, A. and April, R.** (2015). Resolution improvement for MUSIC and ROOT MUSIC algorithms, *J. Inf. Hiding and Multimedia Signal Process.*, *6*(2), 189–197.

[54] **Harris, F.J.** (2021). *Multirate signal processing for communication systems*, River Publishers.

[55] **Hentschel, T. and Fettweis, G.** (2000). Sample rate conversion for software radio, *Communications magazine*, *38*(8), 142–150.

[56] **Tayem, N.**, **Omer, M. and Hussain, A.A.** (2014). Hardware implementation of MUSIC and ESPRIT on NI-PXI platform, *2014 IEEE Military Communications Conference*, IEEE, pp.329–332.

CURRICULUM VITAE



Name Surname : Batuhan KAPLAN

EDUCATION :

- **B.Sc.** : 2018, Department of Electronics and Communication Engineering, Yildiz Technical University

PROFESSIONAL EXPERIENCE AND REWARDS:

- 2019– Researcher at The Scientific and Technological Research Council of Turkey

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- Batuhan Kaplan, İbrahim Kahraman, Ali Rıza Ekti, Serhan Yarkan, Ali Görçin, Mehmet Kemal Özdemir and Hakan Ali Çırpan, "Detection, Identification, and Direction of Arrival Estimation of Drone FHSS Signals with Uniform Linear Antenna Array", in IEEE Access, Vol. 9, pp. 152057–152069, November 2021.

- Batuhan Kaplan, İbrahim Kahraman, Ali Rıza Ekti, Serhan Yarkan and Hakan Ali Çırpan, "Measurement Based Direction of Arrival Estimation for Frequency Hopping Signals", in 28th IEEE Signal Processing and Communications Applications Conference (SIU), pp. 1–4., Gaziantep, Turkey, October 2020.

- Batuhan Kaplan, İbrahim Kahraman, Ali Görçin, Hakan Ali Çırpan and Ali Rıza Ekti, "Measurement based FHSS–type Drone Controller Detection at 2.4 GHz: An STFT Approach", in 91st IEEE Vehicular Technology Conference (VTC2020-Spring), pp. 1–6, Antwerp, Belgium, May 2020.

OTHER PUBLICATIONS, PRESENTATIONS AND PATENTS:

- Burak Ede, Batuhan Kaplan, İbrahim Kahraman, Samed Keşir, Serhan Yarkan, Ali Rıza Ekti, Tunçer Baykaş, Ali Görçin, and Hakan Ali Çırpan, “Measurement-Based Large Scale Statistical Modeling of Air-to-Air Wireless UAV Channels via Novel Time-Frequency Analysis" IEEE Wireless Communications Letters, 2021.