RADIO FREQUENCY TRANSIENT SEGMENT DETECTION BASED ON AKAIKE INFORMATION CRITERION

2022
PhD THESIS
ELECTRIC & ELECTRONIC ENGINEERING

Saleh Abulgasem AJOUAT

Thesis Advisor
Prof. Dr. Necmi Serkan TEZEL

RADIO FREQUENCY TRANSIENT SEGMENT DETECTION BASED ON AKAIKE INFORMATION CRITERION

Saleh Abulgasem AJOUAT

T.C.
Karabuk University
Institute of Graduate Programs
Department of Electric & Electronic Engineering
Prepared as
PhD Thesis

Thesis Advisor
Prof. Dr. Necmi Serkan TEZEL

KARABUK
Feb 2022

I certify that in my opinion the thesis submitted by Saleh Ajouat titled “RADIO FREQUENCY TRANSIENT SEGMENT DETECTION BASED ON AKAIKE INFORMATION CRITERION” is fully adequate in scope and in quality as a thesis for the degree of PhD.

Prof. Dr. Necmi Serkan TEZEL ....
Thesis Advisor, Department of Electric & Electronic Engineering

This thesis is accepted by the examining committee with a unanimous vote in the Department of Electric and Electronic as a PhD of Science thesis. Feb 11, 2022

Examining Committee Members (Institutions)		Signature
Chairman	: Assist. Prof. Dr. Kadir İLERİ (BANU)	....
Member	: Prof. Dr. Necmi Serkan TEZEL (KBU)	....
Member	: Assoc. Dr. Zyodulla YUSUPOV (KBU)	....
Member	: Assoc. Prof. Dr. Adem DALCALI (KBU)	Online
Member	: Assist. Prof. Dr. Zafer ALBAYRAK (SUBU)	Online

The degree of PhD of Science by the thesis submitted is approved by the Administrative Board of the Institute of Graduate Programs, Karabuk University.

Prof. Dr. Hasan SOLMAZ ....
Director of the Institute of Graduate Programs

"I declare that all the information within this thesis has been gathered and presented in accordance with academic regulations and ethical principles and I have according to the requirements of these regulations and principles cited all those which do not originate in this work as well."

Saleh Abulgasem Ajouat

ABSTRACT

Ph.D.

RADIO FREQUENCY TRANSIENT SEGMENT DETECTION BASED ON AKAIKE INFORMATION CRITERION

Saleh ABULGASEM

Karabük University
Institute of Graduate Programs
Department of Electrical and Electronics Engineering

Thesis Advisor:
Prof. Dr. Necmi Serkan TEZEL
Feb 2022, 48 pages

In this thesis, a technique has been developed and modified to catch the onset in transient segment of radio frequency (RF) Bluetooth signal using of the common Akaike Information Criterion (AIC) and also by using the alternative version named Alt-Akaike Information Criterion (Alt-AIC) in automatic mechanism. Definitely the automatic detection of actual signal is essential part in many fields especially in Radio Frequency communications, the optimum process leads to interpret RF data efficiently and quickly for any purposes and abstain handling redundant information like background noise. In this research, a turn on moment of Radio Frequency transmitters has been detected in variety ways with different sampling rate. A comparison has been made between regular method of Akaike Information Criterion (AIC) and Alternative version of Akaike Information Criterion (Alt-AIC) to demonstrate the ability of both methods to estimate the weak up moment in transient of Bluetooth signal. Both methods have been evaluated on most popular cellular smartphones brands by variety ways with different levels of signal to noise ratio

SNR. Both algorithms show high performance, less consuming time, low complexity and robustness in noisy processes with advantage of Alt-AIC over the traditional method AIC. The picking performance demonstrates the feasibility of both methods. The success of automatic estimation leads to precise interpreting of RF data by cease handling useless information such as inescapable noise and study the exact behavior of particular transmitter.

Keywords : Akaike Information Criterion, Alt-AIC, Transient Detection, Bluetooth Signal

Science Code : 92706

ÖZET

DOKTORA TEZİ

AKAIKE BİLGİ KRİTERİ İLE RADYO FREKANSI GEÇİCİ DURUM TESPİTİ

Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Elektrik Elektronik Mühendisliği Anabilim Dalı

Tez Danışmanı:
Prof. Dr. Necmi Serkan TEZEL
Şubat 2022, 48 sayfa

Bu tezde, ortak Akaike Bilgi Kriteri (AIC) ve alternatif Alt-Akaike Bilgi Kriteri versiyonu kullanılarak radyo frekansı (RF) Bluetooth sinyalinin geçici segmentindeki başlangıcı yakalamak için bir teknik geliştirilmiştir. Gerçek sinyalin otomatik olarak algılanması, özellikle Radyo Frekansı iletişimi başta olmak üzere birçok alanda önemli bir konu olup, optimum süreç, RF verilerinin herhangi bir amaç için verimli ve hızlı bir şekilde yorumlanmasına ve arka plan gürültüsü gibi gereksiz bilgilerin işlenmesinden kaçınılmasına yol açar. Bu araştırmada, Radyo Frekansı vericilerinin çalışmaya başladığı zaman farklı örnekleme oranları ile çeşitli şekillerde tespit edilmiştir. Akaike Bilgi Kriteri (AIC) yöntemi ve Alternatif Akaike Bilgi Kriterinin (Alt-AIC) ile geçici durumdaki zayıf Bluetooth sinyalinin başlangıç zamanınım tahmin etme yetenekleri gösterilmiş ve karşılaştırma yapılmıştır. Her iki yöntem de en çok kullanılan hücresel akıllı telefon markalarında farklı sinyal/gürültü oranı seviyeleri ile çeşitli şekillerde değerlendirilmiştir. Her iki algoritma da yüksek performans, düşük işlem süresi, düşük karmaşıklık göstermekle birlikte Alt-AIC'nin bilinen yöntem olan AIC'ye göre gürültüye daha az duyarsız olması sebebiyle üstünlük gösterir. Toplama performansı, her iki yöntemin de uygulanabilirliğini göstermektedir. Otomatik tahminin başarısı, kaçınılmaz gürültü gibi gereksiz bilgileri işlemeyerek ve belirli vericinin kesin davranışını inceleyerek RF verilerinin kesin olarak yorumlanmasına yol açar.

Anahtar Kelimeler : Akaike Bilgi Kriteri, Alt-AIC, Geçici durum tespiti, Bluetooth İşareti

Bilim Kodu : 92706

ACKNOWLEDGMENTS

I would like to express my special gratitude and thanks to my advisor Professor Dr. Necmi Serkan TEZEL for his helpful advice, unparalleled support, and unwavering guidance during my study.

TABLE OF CONTENTS

Page

APPROVAL ii
ABSTRACT iv
ÖZET vi
ACKNOWLEDGMENTS viii
TABLE OF CONTENTS ix
LIST OF FIGURES xi
SYMBOLS AND ABBREVIATION INDEX xii

CHAPTER 1 1
INTRODUCTION 1
CHAPTER 2 4
BLUETOOTH SIGNAL SPECIFICATIONS 4
2.1. BLUETOOTH NETWORK TOPOLOGY 6

CHAPTER 3 11
TRANSIENT SIGMENT DETECTION 11
3.1. THRESHOLD DETECTION APPROACH 12
3.2. BAYESIAN CHANGE POINT DETECTION 13
3.3. SIGNAL PHASE TRANSIENT DETECTION APPROACH 13
3.4. ENERGY CRITERION METHOD EC 13
3.5. PROPOSED METHOD 14
3.5.1. Akaike Information Criterion AIC 15
3.5.2. Alternative-Akaike Information Criterion Alt-AIC 17
3.5.3. Transient Onset Point Detection Based on AIC Algorithm 18

CHAPTER 4 20
IMPLEMENTATION 20
4.1. DATA COLLECTION AND PREPARING 20
4.2. DATA SAMPLING 22

Page

4.3. DOWNSAMPLING PROCESS 22
4.4. BASEBAND DOWN-CONVERSION 23
4.5. EMPIRICAL MODE DECOMPOSITION EMD 24
4.6. SIGNAL-TO-NOISE RATIO DELIBERATION 28

CHAPTER 5 33
PRACTICAL EXPERIMENT AND RESULTS 33
5.1. PERFORMANCE ANALYSIS OF SNR 39

CHAPTER 6 43
CONCLUSION 43

REFERENCES 45

RESUME 48

LIST OF FIGURES

Page

Figure 2.1. Bluetooth operating frequency spectrum. 5
Figure 2.2. Bluetooth layers. 5
Figure 2.3. Bluetooth networks. 6
Figure 2.4. Bluetooth frequency-hopping pattern. 7
Figure 2.5. Bluetooth packet format. 9
Figure 3.1. Sample of bluetooth signal. 11
Figure 3.2. Zoomed in portion of bluetooth segments. 12
Figure 3.3. A sample of bluetooth signals. 15
Figure 4.1. Diagram of signal retrieval system. 20
Figure 4.2. Samples of collected bluetooth signal. 21
Figure 4.3. Down-conversion by frequency shift. 23
Figure 4.4. IMFs components by EMD of one record. 27
Figure 4.5. Flowchart of EMD algorithm. 28
Figure 4.6. Equivalent SNR levels of down-converted signal. 30
Figure 4.7. SNR Levels of down-converted signal. 30
Figure 4.8. Distorted signal at selected level (d=45). 31
Figure 4.9. Distorted signal at selected level (d=100). 31
Figure 4.10. Selected record with spike. 32
Figure 4.11. The onset point spike affection. 32
Figure 5.1. AIC algorithm for finding global minimum value. 34
Figure 5.2. (a) The selected recorded signal and (b) is the equivalent AIC values. 35
Figure 5.3. AIC min of down-converted signal. 36
Figure 5.4. Down-sampling factor effect. 36
Figure 5.5. AICmin of 1st IMF signal, down-converted, and direct applied. 37
Figure 5.6. The equivalent values of (a) AIC & (b) Alt-AIC for a Chosen recorded. 38
Figure 5.7. Samples output of chosen detection method. 39
Figure 5.8. SNR Performance of down-converted and direct applied cases. 41

Page

Figure 5.9. Down-converted signal with AICmin of all SNR levels. 41

Figure 5.10. 1st IMF, down-converted and direct applied SNR performance. 42

SYMBOLS AND ABBREVIATION INDEX

ABBREVIATIONS

ADC	: Analog to Digital Converter
AIC	: Akaike Information Criterion
ALT-AIC	: Alternative- Akaike Information Criterion
EMD	: Empirical Mode Decomposition
FHSS	: Frequency Hopping Spread Spectrum
GFSK	: Gaussian Frequency Shift Keying
IMF	: Intrinsic Mode Decomposition
ISM	: Industrial Science and Medical
LOG	: Logarithmic
LPF	: Low-Pass Filter
RF	: Radio Frequency
SNR	: Signal-to Noise Ratio

CHAPTER 1

INTRODUCTION

Currently, wireless network has a tendency usage of our regular life; it is quite used in both civilian society and military organizations. Subsequently the wireless networking takes an enormously significant role in transmission data; detecting the transmitting data is crucial in RF processing. In order to establish manipulate any transmitter's behavior; it is significant to recover the beginning of signal which named onset point, this point represents switching on instant for that wireless device or transmitter. This can be accomplished by variety ways of the signal characteristics, signal statistics properties, or by exploiting some other kind of features from time or frequency [1].

The direct approach to capture the onset is by watching the transient segment in the time series signal, many definitions or aspects that interchangeably used here for transient start point such as sudden burst, a change point of the signal, onset point, weak up point, or abrupt change.

After turning particular radio transmitter on, the RF signal goes through many phases exactly two phases; transient part which is controlled by circuit components of radio transceiver and nearly unchanged steady state part [2]. These two segments for each transmitter usually have unique RF features especially transient part. The other part noise which usually comes with signal; it is not belong to the transmitter characteristic and many studies trying to find ways to discard it automatically.

The perception of transient is hard to define specifically; transients are small chunks during which the signal grows quickly in unexpected way. In practical, the RF Bluetooth signal comes in three chunks or segments, the most challenge chunk is background noise where; the length of this redundant part is random and altered in unanticipated manner. The onset is a single instant selected to spot the prolonged transient. Generally, the onset will correspond with the beginning of the transient, or the initial time at which the transient can be estimated consistently. A variety of treatments are exist that can be applied to assist the task of onset estimation or make it more precisely.

In the literature, the detection of the onset point of the transient segment has been accomplished by many methods such as defining threshold level to make a decision of detection [8], and the other common method named energy envelope [3], [4]. Relying frequency domain features of steady state signal a study suggested a method for radio transmitter identification [5]. Another method depends on amplitude features called Bayesian Step Change estimator [6]. In this research a present method that exploits phase characteristics to make detection [7]. Energy criteria recently adapted as a technique to find out onset of transient signal [8]. Since the detection of start point plays an utter important aspect in multiple areas like enhance the security by defining RF fingerprints of transmitter [9]. A Threshold is very common sort of indicator that predefines a level and can be handled in different ways like using energy of time window chunks and the matching zero crossings of that signal with adaptive threshold was also presented [10], [11].

Wireless transmitter's signal starts sudden represented by start point of transient segment after a while steady state takes place immediately after end point of transient segment. Relying on a study [12] only start point is considered in this research.

In this work, the start point of the transient signal has been detected by means of the Akaike Information Criterion AIC and also by alternative method belongs to the same AIC technique. The advantage of using the AIC is that there is no need to define threshold values for Bluetooth collected signals. Use of AIC of signals is quite popular technique and involved in many fields. A presented method is applied on a huge amount of data exceeds 10000 records of most popular cellular phones named (Samsung, Huawei, IPhone, LG, Sony, and Xiaomi) to disclose the accurate time instant of onset point of Bluetooth signal [13]. Moreover, it is beneficial to modify the proposed technique for both more practical executions and lower computational instructions.

Akaike's information criterion AIC was formed in 1971 [14]. AIC indicator is an algorithm whose equivalent value can be set for each sample along with the examined signal. The estimated global minimum of AIC tells the optimum splitting line from surrounded noise of that signal and this is the characteristic of AIC detector which is typically taken an advantage in variety applications.

The performance of traditional method AIC has been boosted in computational complexity and consuming time by simplifying the equation into a linear combination of the arithmetic sum and the square sum of the time series.

In order to assess the operative of the presented successive signal detector, the detection performances are tested for different levels of Signal to Noise Ratio (SNR). The SNR levels of the transients are declined by adding the recorded channel noise to the signal. The produced noise is added to the tested signal for each record of each type.

Applied noise can be taken from records where; every record has own noise and also can be produced artificially. In order to achieve precise decision and make assessment of noise analysis the produced noise whether it is created artificially or taken from one record must be not changed in its characteristics for every record and every time; otherwise it will not lead to any results

The whole thesis is organized as following: Chapter 1, an introduction is presented. In Chapter 2, Bluetooth signal specification overview. Chapter 3 reveals the theory of proposed method, and states some previous methods to detect the transient segment. In Chapter 4, the Bluetooth records are applied to AIC and Alt-AIC based detection technique. In chapter 5, the test performances of the introduced method are analyzed based on SNR variation. Chapter 6 states the conclusion of study. Chapter 7 lists the references.

CHAPTER 2

BLUETOOTH SIGNAL SPECIFICATIONS

Group of researchers and companies started doing studies in order to find a technique or protocol permitting portable devices to communicate with each other in short range. They manage to produce a standard that work in unlicensed band called unlicensed Industrial, Scientific, and Medical ISM band Figure 2.1. This technique runs on the 2.4 GHz band to convey packets of information from a master node to slave nodes by employing 79 radio frequency channels 1 MHz for each. Bluetooth is a protocol depends on a radio frequency system intended for short-range and for gadgets that are not expensive to swap physical wires of external devices like mouse, keypads, and digital cameras. The used short range of services is referred as Wireless Personal Area Network (WPAN). Bluetooth network architecture distinguishes two types of network configuration named piconet and scatternet Figure 2.3. A piconet is a WPAN formed by a Bluetooth device acting as a dominant or the main piconet and one or more devices acting as slaves. A scatternet is a group of Bluetooth piconets interfering in time and space more than one. As known physical wire data is more secure from wireless, the security is a fundamental issue for wireless networks and Bluetooth wireless network [15]. Bluetooth standard relies on some ways to assure maintaining security of transferred data over wireless network at decent level like authentication and encryption. The other important issue is the interference; to prevent interfering in ISM band; Bluetooth protocol employs a technique called Frequency-Hopping Spread Spectrum FHSS, and consecutive hops occur every 1600 second with time slot of 625 μs for basic and enhanced bit-rate submission [15]. Practically communications protocol bounds the data rate to 723 kbps. The bit error rate will escalate in case of interference during transmission, and in turn the attainable data rate will decrease. It will stay a while for the next channel hop and try a new attempt.

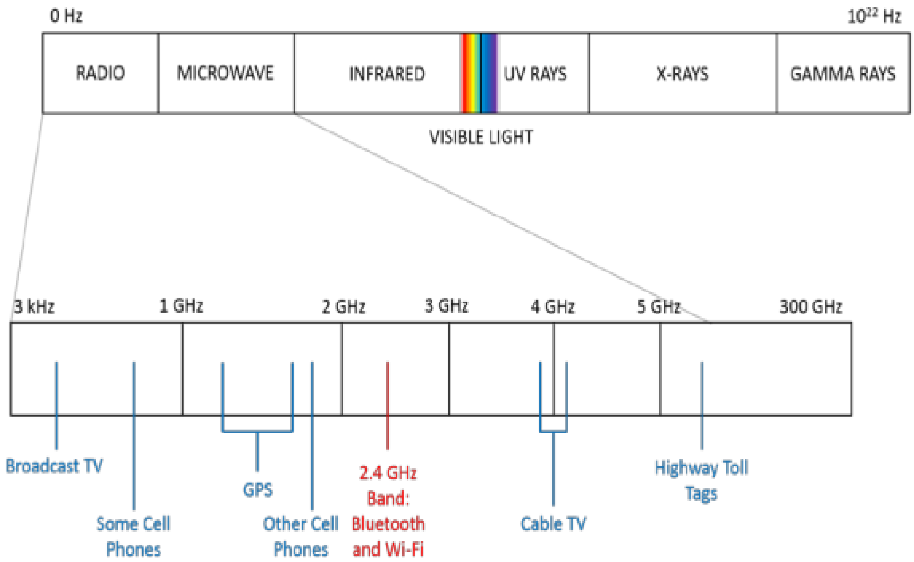


Figure 2.1. Bluetooth operating frequency spectrum.

The Bluetooth technology permits devices from various producers to exchange data in short range around 100 m. Bluetooth technique has many layers protocol as seen in Figure 2.2. The fundamental layers are [16]:

- Radio Frequency layer; responsible for transmission and modulation
- A baseband layer; concerns with connection establishment inside piconet
- Data Link layer; managing the transmission and security services
- Application layer provides usability mean to make user interacting with the application

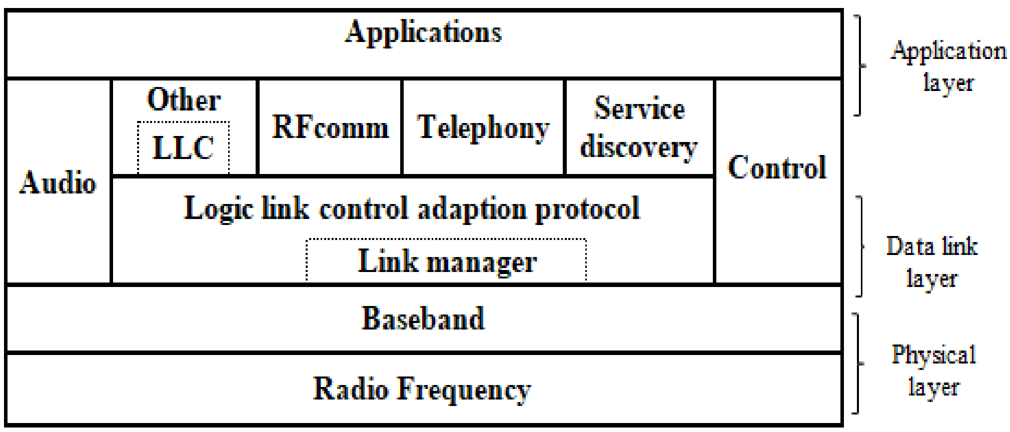


Figure 2.2. Bluetooth layers.

2.1. BLUETOOTH NETWORK TOPOLOGY

Bluetooth technology uses mesh topology for neighboring devices for interconnection in a way as master and slaves also known as server and clients; Bluetooth equipment can work in a master or slave module [17]. That module assigns up to eight devices to be communicated together inside piconet network. In the piconet network one device behaves as master and the other devices act as slaves. Initializing connection is the job of master device and the slaves are synchronized in all subjects with the master. One master controls connection in piconet at same time several slaves can be connected to other piconet then slave can control other piconet, so one slave or many can be a part of multiple piconets. if a number of piconet overlapping their coverage together; this network called scatternet and entire devices on a piconet obey the consecutive frequency hopping of master and timing; where the network can contain more than 7 devices slaves, but only 7 of them are active at one time, and the other is in a parked state, its activity is limited to the synchronization process and it cannot actually participate in the communication process unless it switches to the active state and switches one active devices to pause state [18] Figure 2.3.

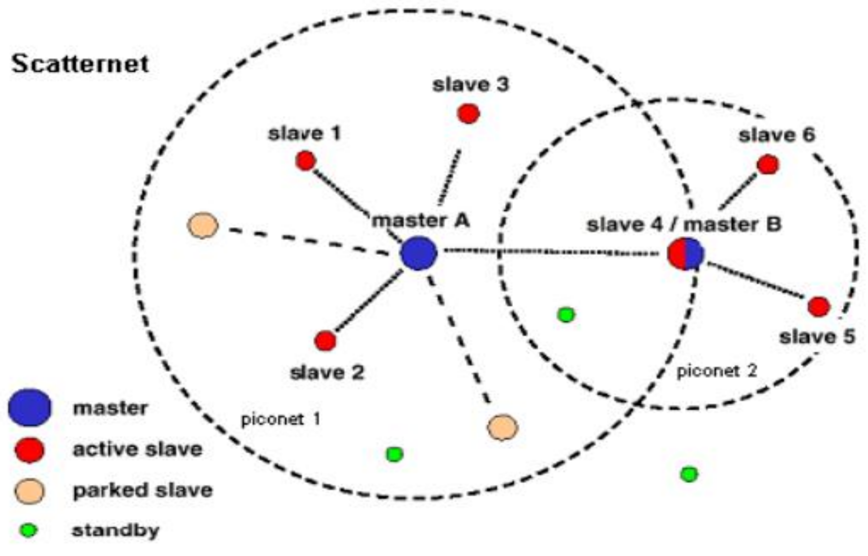


Figure 2.3. Bluetooth networks.

The process of establishing the connection is done by the master device, the slave device can make a request to switch to a master device; where this master is the gateway to all slaves, and then it is not possible to communicate between one slave and another except through it.

2.2. FREQUENCY HOPPING SPREAD SPECTRUM

There are some standards of data telecommunication systems like IEEE 802.11 and ZigBee, BT radio system operates within the free unlicensed ISM band [17]. So intensely there is a chance of interfering same band by other wireless devices. Frequency-Hopping Spread Spectrum FHSS technology is radio communication technique existed to sustain swapping of carrier frequency during radio transmission to avoid interception and interference states. It is also suggested to boost Bluetooth performance by finding clean channel and avoiding congested channels. Principally, FHSS is a technique by which the transmitted packet hops among varied channels inside a network called piconet that contains single master device and slaves. It is possible to have multiple piconets in same place and they will not interfere with each other and the reason is the capability of the signal hop. In this technique the spectrum of Bluetooth begins from 2.4 GHz to 2.4385 and it contains 79 radio frequency channels having bandwidth 1 MHz for each channel as illustrated in Figure 2.4. The Bluetooth creates 1600 hops / second in random way [18].

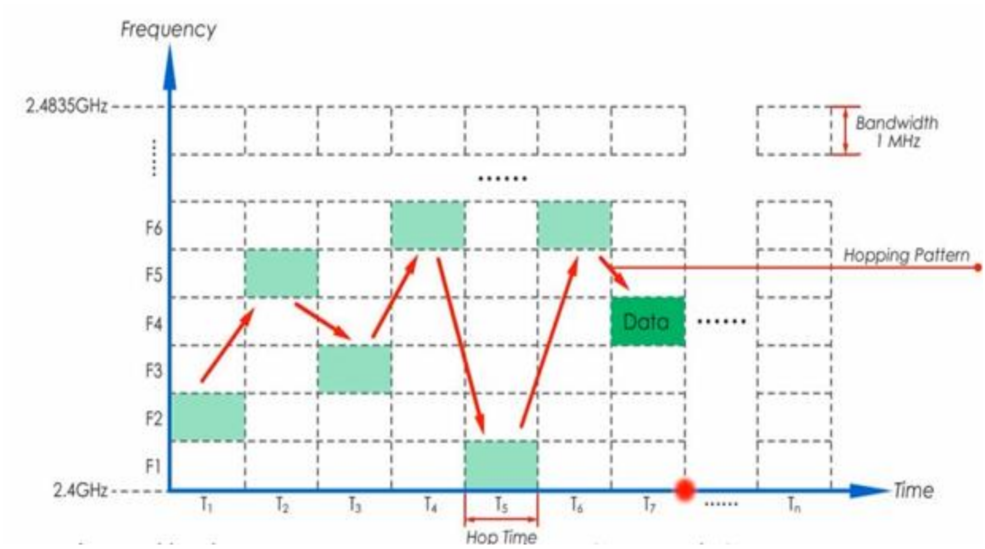


Figure 2.4. Bluetooth frequency-hopping pattern.

In 2.4 GHz ISM band, Wi-Fi defines 14 channels but in case of Bluetooth; it specifies 79 RF channels by 1 MHz for each channel. The spacing frequency begins from 2402 MHz to 2480 MHz as presented in Figure 2.4. The spacing frequency can be achieved by this equation [19]:

$$f(MHz) = 2402 + k \qquad (2.1)$$

k = 0, 1, ..., 78

In equation 1; f figures the channel frequency that will be employed for submission, and k denotes the number of channel. The parameter k is defined by a hardware unit and this unit elects a particular hopping chain based on the MAC address of the Bluetooth device [20].

The transmitted bit stream is broken into chunks called packet Figure 2.5, single packet can be sent in one slot. Every packet has the same format excluding the payload part. The size of payload part varies according to the existing data.

The packet format composed of three entities; it begins with 72 bits access code, followed by field header 54 bits, it comprises 18 bit that is recurring 3 times, and the last field payload. The Header includes Address 3 bits which is identifying up to 7 slaves, and 4 bits Type followed by F, A and S; these symbols are referring to Flow control, Acknowledgement, and Sequence number respectively, the last is 8 bit Checksum to detect errors. The access code is employed to detect the existence of packet and determining whether to send to slave or receiving from master. The packet header holds all control information that linked with the packet like address of regarded slave. It is bounded to repeated pattern bits in order to confine the overhead [21]. Eventually, the payload part will hold the bits that are being submitted coming from other layers.

The physical layer is split into time slots. In which the time slots linked with a particular hop frequency 1600 times/s. Inside a network, the data is conveyed among Bluetooth gadgets by packet that is set in certain time slot. A single packet can be exchanged between two channels. The next packet for a new channel is selected randomly [15].

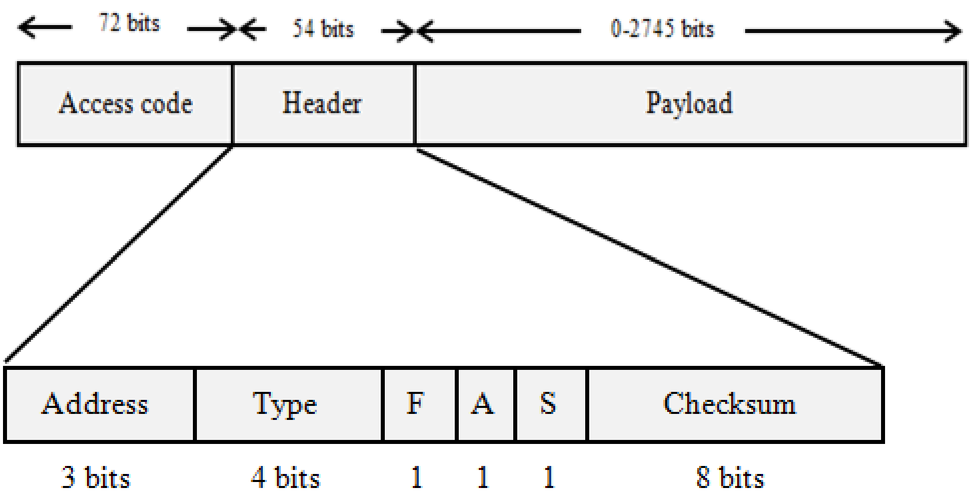


Figure 2.5. Bluetooth packet format.

Three factors control Bluetooth versions; range, bitrates, and power consumption; these factors imply using proper binary modulation scheme and when a particular modulation scheme is chosen; it regards those factors for robustness since in free ISM band the bandwidth of the signal is restricted to one mega Hertz. The very first version of Bluetooth protocol employs Gaussian-frequency shift keying (GFSK) modulation. Bluetooth also uses Phase Shift Keying (PSK) modulation with 1 Mb/s. There are two different PSK modulation schemes can be employed named 4/π – DQPSK Differential Quadrature Phase-Shift Keying modulation, and 8-DPSK Differential Phase-Shift Keying modulation is used [22].

Bluetooth standard uses Gaussian frequency shift keying modulation technique. In Frequency Shift Keying; frequency shift means modulating or shifting the frequency of the carrier and keying persisted from manually operation in the past, frequency shift keying encodes data as a series of frequency changes in a carrier which means that a binary 1 is encoded by increasing the carrier frequency and 0 is encoded by decreasing the carrier frequency to a known value some of the advantages of FSK are you can fairly easily design a transmitter and receiver also the noise signals change the amplitude of a signal making frequency modulation relatively more immune to noise than amplitude modulation technique. One of the great challenges of FSK can be comprehended by examining the transmission of a zero followed by a one it requires the signal to instantaneously jump from a sinusoid of frequency fc – fd (frequency deviation) to fc + fd this sharp switching generates higher frequency components at the output resulting in a wider output spectrum or significant amounts of out of band energy to combat this problem; filtration the modulating signal using a Gaussian filter then this filtered signal modifies the carrier signal due to this the resulting transitions are gradual and smoother thus Gaussian filtering is a standard way to reduce the spectral width and it is often referred to as pulse shaping technique [22], [23].

Considering the previous example of switching from 1 to 0 or 0 to 1 in case of ordinary non-filtered FSK this jump causes the modulated waveform to change rapidly which introduces large out of band spectrum if the pulse is changed going from 0 to 1 on and ultimately if this smoother pulse is used to determine the carrier frequency then the out of band spectrum is reduced by a significant amount, a narrow spectral bandwidth also ensures reduction in the interference with other frequencies, the most basic GFSK implementation is called two level GFSK; two different frequencies are used to encode symbols 0 and 1. To transmit 1 the carrier frequency is increased by a certain deviation and to transmit 0 the carrier frequency is decreased by the same deviation. The rate at which the data is sent through the system is called the symbol rate; it takes several cycles to determine the frequency of the underlying carrier and whether a 1 or 0 was transmitted, thus the symbol rate is a very small fraction of the carrier frequency thus even if the carrier frequency is roughly 2.4 billion cycles per second the symbol rate is only one or two million symbols per second [15].

CHAPTER 3

TRANSIENT SIGMENT DETECTION

An automatic detecting the onset signal is regarded to be the most significant stage. Since the transient signal represents the actual behavior that discriminates the arisen signal of a particular transmitter from surrounded background noise. So, exact detecting is required for high precision of efficient processing.

The transient signal happens when the device is switched on. It takes place in a very short period of time. The transient signal has been formed by the attributes to the variety of circuit components such as physical layer precisely modulator, power amplifier, and antenna [2]. Meanwhile the detection of onset point plays crucial rule. So that it should be specified appropriately and automatically in order to create exact and efficient processing. In doing so; there are many common ways have been mentioned in literature that can be used and looking forward for more efficient techniques that overcome the deficiency of previous techniques.

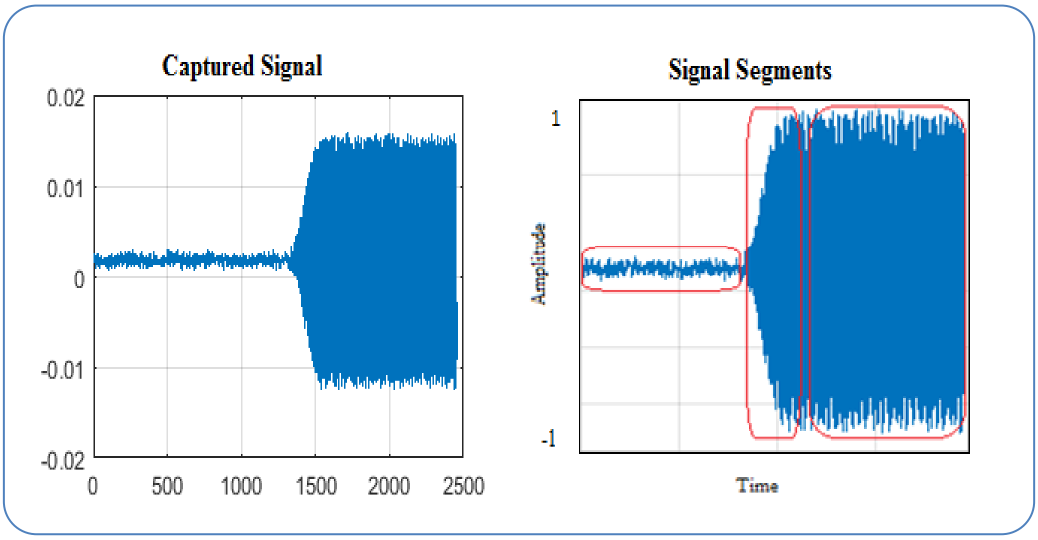


Figure 3.1. Sample of bluetooth signal.

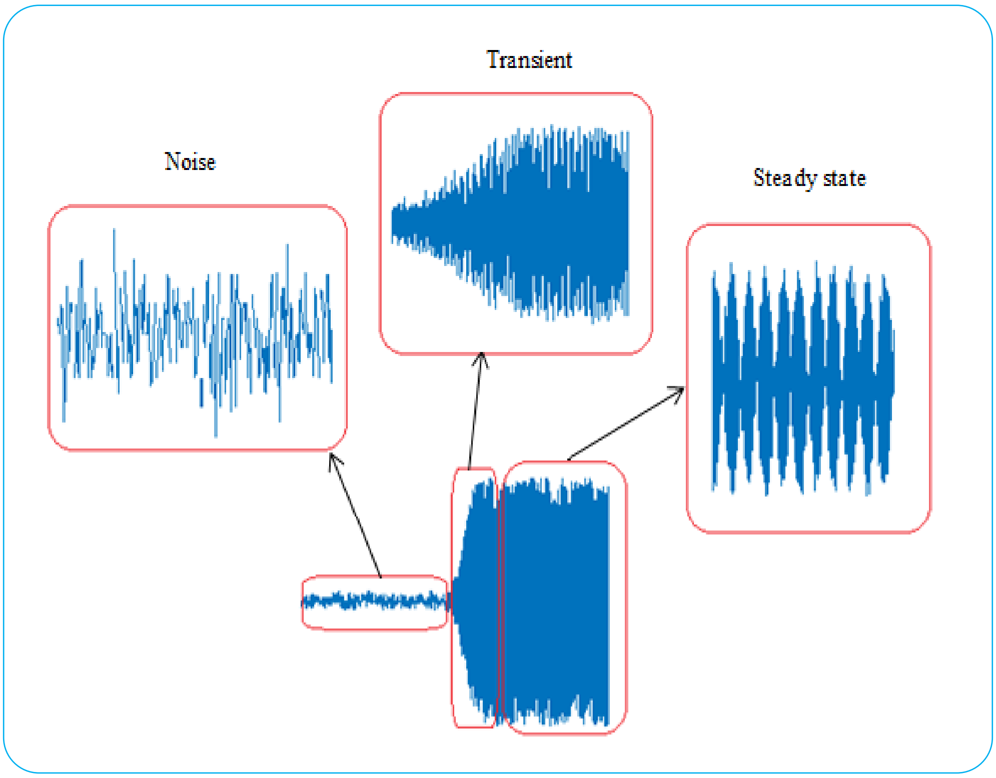


Figure 3.2. Zoomed in portion of bluetooth segments.

In the preceding researches, many techniques have been done on RF signal Figure 3.1 for estimation purposes and applied on the transient and steady state segments Figure 3.2 of. The onset of the transient of a wireless signal can be spotted depend on the signal characteristics. These characteristics can be taken out from both time domain and frequency domain, in the time domain the feature is stated by signal amplitude, while in the frequency domain frequency or phase can be used.

The onset point of the transient signal can be distinguished by many techniques. Some of methods will be briefly introduced to estimate the beginning of transient signal.

3.1. THRESHOLD DETECTION APPROACH

Basically, onset detection is executed using a pre-defined threshold value, this can be accomplished by different ways where the time of change point of signal higher than a chosen value indicates the onset of the signal [24], [10], [11]. The basic issue in using this manner is the suitable picking of the threshold level with respect to the mixed noise. Choosing the pre-defined level too low can leads to early impulse by noise and picking a level too high might give outcome in absent the time of examined signal change point. The level of detection threshold may be improved for certain values of signal-to-noise ratio, however in practical applications a variation of signal strength can be anticipated which always stands for a weakness to evaluation errors.

3.2. BAYESIAN CHANGE POINT DETECTION

Bayesian Change Detection is an approach that identifies the transients with involving Bayes' rule using of a posterior probability distribution function [6]. Both mentioned approaches used amplitude characteristics by different ways in order to catch the onset point of the transient part of a transmission signal. Bayesian Technique is liable upon learning from experience; meaning that the new data are created in spot of preceding data.

3.3. SIGNAL PHASE TRANSIENT DETECTION APPROACH

From being some famous methods like Threshold detection and Bayesian step change detector have delay in performance restrictions in some application, using the time domain characteristic and relying on sudden abrupt change at the transient start sometimes not works, because moving from the noise state to transient state may come steadily. A study in [7] for transient detection has been introduced to overcome this issue depends on phase characteristic. Relying on phase characteristics rather than amplitude characteristics is more efficient and can cover most signals and more immune to noise either.

3.4. ENERGY CRITERION METHOD EC

This method commonly used to give location of partial discharges in power transmission [25]. Recently this method is used for RF data [8], the clue underlying the EC technique is that the instant which the transient signal occurs, will be the same instant that the energy curve of the signal has sudden change, which depends on cumulative sum. Spotting this sudden change will be guided to spot the transient onset point. The EC technique has high performance in many applications. The energy criterion method can be implemented in two different ways; based on amplitude signal or based on phase signal as stated in more details in [8].

In this work, the start point has been detected by means of Akaike Information Criterion AIC algorithm. By using this technique there is no need to define threshold level for all Bluetooth dataset. The selected method is comparing characteristics of two chunks of signal to detect the start point for all records without tuning, and that is helpful when enormous amount of data is used.

3.5. PROPOSED METHOD

The goal of the detection phase is to distinguish the correct time sample when the transmitter is powered up, it is possible to do that manually by visualizing the signal but it is very tough job especially in case of using huge amount of data. An attaining of the detection step is significant because implies avoiding noise and going ahead to transmitter arisen signal; this detection positively affects the treatments of that transmitter and the most important thing is doing that automatically.

The Bluetooth signal is comprised of three parts, named as, noise, transient, and steady state Figure 3.2. Noticeably the features that can be deducted from studied signals are not existed in the noise portion also the time duration of this redundant segment differs unpredictably Figure 3.3 besides the noise part is not belong to transmitter's signal. Because of all that the first process of any treatment procedure is to ensure that the noise is eliminated from the manipulating followed by knowing the start and end of each segment automatically, so they can be studied separately.

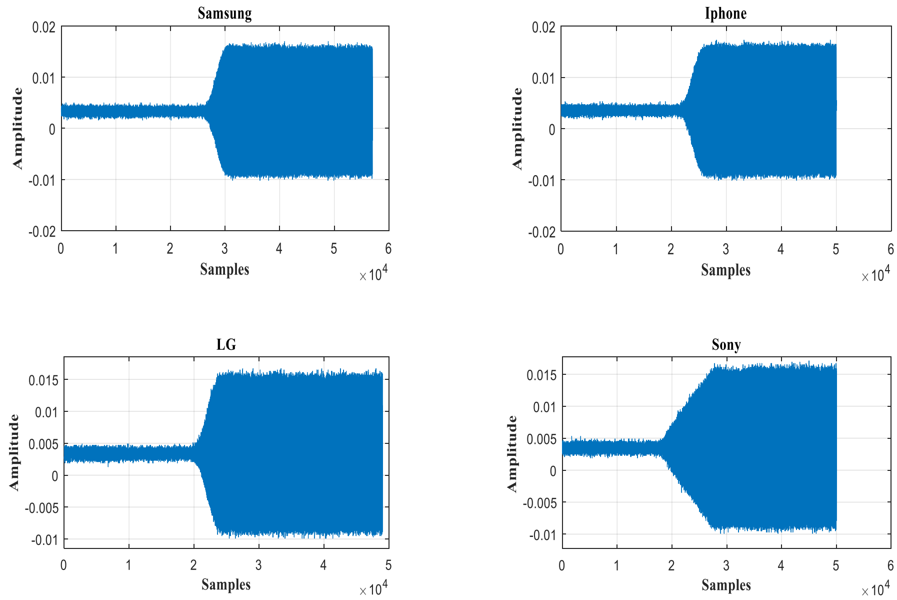


Figure 3.3. A sample of bluetooth signals.

As stated the RF signals come with unavoided random noise with specific characteristics as a result of circuit components deficiency, also the growing amount of digital data sets created by wireless networks; these facts motivate the examiners to look for an automatic way to properly treat them and eradicate background noise. In this work, more than 10000 records belong to Bluetooth signal [13] of most popular smartphones will be applied and executed by means of Akaike Information Criterion method and alternative method of AIC named as Alt-AIC in order to improve time consumption and compare the ability and performance of both methods

3.5.1. Akaike Information Criterion AIC

Akaike's information criterion AIC was developed under this name and originally designed for time series fit model to describe data from observations [26]. AIC is used in many fields such as ultrasound signals [27], arrival time of partial discharge in power cables [25], [28] and quite often used in seismic records [29], [30], [31].

Originally there are two approaches used for AIC computations with and without Auto-Regressive coefficients. The AIC picker is count on the concept that the intervals before and after weak up time are two different stationary time series. In The first approach AIC algorithm is formulated as [14]:

$$\boldsymbol{AIC(k)} = (k - M) \times \log\left(\sigma_{1,max}^2\right) + (N - M - k) \times \left(\log\left(\sigma_{2,max}^2\right)\right) + C \qquad (3.1)$$

Where; k is sliding step all over the samples

In equation 2, to retrieve the AIC equivalent values, the coefficient C and the order M must be considered, which have a high grade of computational complexity.

The second approach of computing the AIC function which adapted here is done without using AR coefficients, which can be calculated directly from the time series. The turn on change point is again the minimum of the AIC function. For Bluetooth record x of total samples N, the AIC_{min} sample is recovered by [28], [30]:

$$\boldsymbol{AIC(k)} = k \times \log\left(var\left(x(1,k)\right)\right) + (N - k - 1) \times \left(\log\left(var\left(x(1 + k, N)\right)\right)\right) \qquad (3.2)$$

Where; k is movement step all over the samples from 1 to k and samples from k to end of signal. The AIC detector specifies the weak-up point as the global minimum of whole signal. In this research, downsampling is obligatory to speed up the process by reducing the high sample rate, otherwise the process will take long time with same result, and then estimating AIC values by equation 3 which is built as a function in MATLAB.

The common AIC detector provides one specific weak-up point as the absolute minimum of entire signal. AIC detector always has a value along the time series. All these values have one smallest value called global minimum value of AIC which gives the optimum splitting point of time series.

3.5.2. Alternative-Akaike Information Criterion Alt-AIC

The second method which stated here in this research is accomplished without using AR coefficients, which can be calculated immediately from the time series. The sudden change point is once more the lowest value of the AIC function. For a particular Bluetooth record x of total samples N, the AIC_{min} value is clarified by equation 3:

$$\boldsymbol{AIC(k)} = k \times \log\left(var\left(x(1,k)\right)\right) + (N-k-1) \times \left(\log\left(var(x(1+k,N))\right)\right) \quad (3.3)$$

In order to improve time consumption of AIC method the equation need to be altered where; in Alt-AIC case the above equation will be reformed into a linear combination of the alternative sum and the square sum of the samples sequence. Then it shrinks the repetitive computation, and considerably boosts the calculation efficiency. Equation 3 is modified and expressed to become:

$$\log\left(var\left(x(1,k)\right)\right) = \log\left(\frac{1}{k}\sum_{i=1}^{k}(x_i-\bar{x})^2\right)$$

$$= \log\left(\frac{1}{k}\sum_{i=1}^{k}x_i^2 + \frac{1}{k}\sum_{i=1}^{k}\bar{x}^2 - \frac{2\bar{x}}{k}\sum_{i=1}^{k}x_i\right)$$

$$= \log\left(\frac{1}{k}\sum_{i=1}^{N}x_i^2 - 2\bar{x}\frac{1}{k}\sum_{i=1}^{k}x_i - \bar{x}^2\right) \quad (3.4)$$

And

$$\log\left(var(x(1+k,N))\right) = \log\,(\frac{1}{N-k}\sum_{i=k+1}^{N}(x_i-\bar{x})^2)$$

$$= \log\,(\frac{1}{N-k}\sum_{i=k+1}^{N}x_i^2 + \frac{1}{N-k}\sum_{i=k+1}^{N}\bar{x}^2 - \frac{2\bar{x}}{N-k}\sum_{i=k+1}^{N}x_i)$$

$$= \log\,(\frac{1}{N-k}\sum_{i=k+1}^{N}x_i^2 - 2\bar{x}\frac{1}{N-k}\sum_{i=k+1}^{N}x_i - \bar{x}^2) \quad (3.5)$$

Concatenate (4), (5)

$$\boldsymbol{Alt-AIC(k)} = k \times \log\left(\frac{1}{k}s_2 - 2\bar{x}\frac{1}{k}s_1 + \bar{x}^2\right) + (N-k-1) \times \left(\log\left(\frac{1}{N-k} \times (s_m - s_2) - \frac{2\bar{x}}{N-k} \times (N\bar{x} - s_1) + \bar{x}^2\right)\right) \quad (3.6)$$

Where:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x(i) \qquad s_m = \sum_{i=1}^{N} (x(i))^2$$

$$s_1 = \frac{1}{N}\sum_{i=1}^{k} x(i) \qquad s_2 = \sum_{i=1}^{k} (x(i))^2$$

Where; in Bluetooth signal x(t), k in range [1, N] is the length of time window corresponding to x(i), and N is the entire record length.

The advantage of using equation 6 is that when the Bluetooth record length is not changed, s_m and $\bar{x}$ require to be computed only once. During change of k, s_1 and s_2 have to be recalculated; there is no need to repeat the process of computation all values for the entire time series. Putting in only the value of a new point or its square value noticeably lessens the processing instructions.

3.5.3. Transient Onset Point Detection Based on AIC Algorithm

The change point of transient segment is identified from the Bluetooth transmitted signal via the following phases for both traditional AIC or Alternative AIC algorithm:

- The signal should be normalized, and centered.
- The signal is down-converted to baseband using designed Low pass filter followed by frequency shifting to the origin..
- The first IMF is found by Empirical Mode Decomposition EMD

- Down-sampling factor n is needed as a key role for speeding up the entire process
- One record each time is called by AIC function without specifying threshold value
- After determining the global minimum by the algorithm, then the matched time sample is multiplied by factor n.

CHAPTER 4

IMPLEMENTATION

4.1. DATA COLLECTION AND PREPARING

Precise analysis and inquiries of detection and estimation process is the main target of this study. This can be accomplished by using real and huge amount of data and right procedures. Bluetooth transmission signals are documented from a variety of mobile phones brands models with multiple serial numbers. Figure 4.1 displays the signal retrieval system which was considered to record Bluetooth signals from cell phones. Dataset have been recorded in laboratory by high sampling rate oscilloscope. Some factors like temperature, humidity and influence of other devices have been taking in account; the laboratory is chosen in an underground floor where no other wireless signals or equipment is turned on. Also the temperature and humidity are very stable in the laboratory as the alteration in environmental conditions has direct impact on the performance of signal recording. In this research; six different devices with one hundred fifty records are examined for each model.

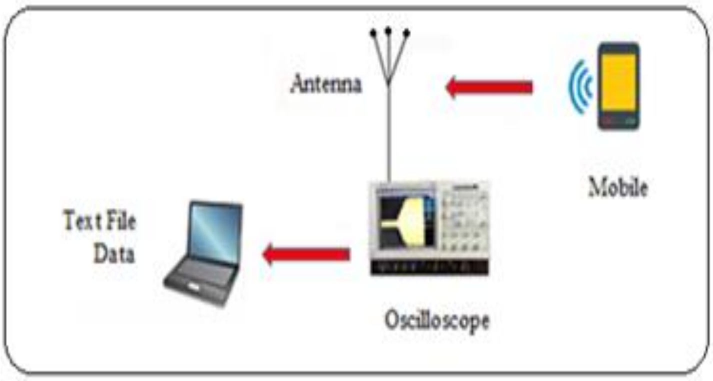


Figure 4.1. Diagram of signal retrieval system.

The data were recorded in the lab and stored as plain text format. BT signal has a carrier frequency between 2400 MHz and 2483.5MHz. BT signals are conveyed to a typical modem antenna and then recorded by an Oscilloscope. The distance between antenna and cell phone is small enough to keep the Signal to Noise Ratio (SNR) in a good level as it is depicted in Figure 4.2.

The lowest limit of sampling rate has been stated by Nyquist theorem. Captured signals are sampled by digitizer that has at least 4.8 GHz sampling frequency. According to Nyquist theory, for a 2.4 GHz signal, ADC must be at least 5 GHz sampling frequency. By using this information Bluetooth signals were recorded by different GHz sampling frequency. Samples of collected signals from Samsung, IPhone, LG, and Sony are seen in Figure 4.2.

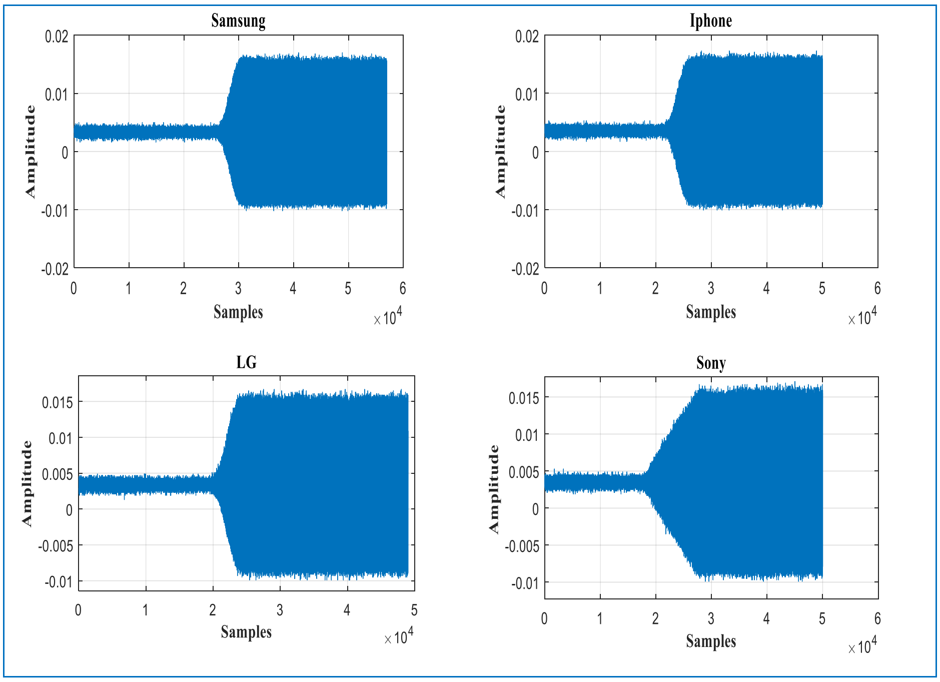


Figure 4.2 Samples of collected bluetooth signal.

The sampling rate has direct effect on the recorded signal; where the high sampling rate is essential to capture the exact behavior of certain sender, in some application like determining fingerprint of transmission; fingerprint consists of the features, which can be taken out from characteristics of signal like amplitude, frequency or phase. In case of insufficient sampling rate, this information may get missing. As a result, the achieved fingerprint of the transmitter would not denote the actual features of the produced signal. So sufficient sampling rate will immune signal from sampling distortion and too high sampling rate will not lead to results improvements except exhausting storage capacity of devices.

The purpose of this study is not looking for features that embedded in Bluetooth signal parts but looking for catching real transmitter

The studied signals have been sampled at the following rates: 5 GHz, 10 GHz, and 20 GHz. Since the collected signals have dissimilar amplitudes, normalization is preferred to keep all the max values of the signals swinging between +1 and -1 which is much better from processing prospective. The filtration process is also needed to get rid of unwanted components and to make the signal smoother.

4.2. DATA SAMPLING

The Bluetooth waveforms data were achieved from [13]. The signals have been acquired at decent condition of humanity, temperature with these sampling rates: 5 GHz, 10 GHz, and 20 GHz. High sampling rate commonly requires high cost. However high sampling rate has positive outcome on some techniques that examine short period of time such as transient segment; those techniques use the high sampling rate to assure observing the precise activities of certain device, but most of these cases too high sampling rate means just extra cost. While in other cases and at exact level will lead to excellent result, for instance the fingerprint of certain device’s signal contains of characteristics, that may revealed from amplitude, or frequency of that signal. With inadequate sampling rate, the yielded fingerprint of the device would not refer the real characteristic achieved from produced signal. In this study, low sampling rate is must by using downsampling process.

4.3. DOWNSAMPLING PROCESS

In signal processing, downsampling is the process of decreasing the sampling rate of a signal. This is usually accomplished to diminish the data transmission rate or the size of the data. The downsampling factor n usually refers to an integer value greater than one. This factor multiplies the sampling time or, correspondingly, divides the sampling rate. The decimation process implies using Low-Pass Filter in combination with discarding samples by an integer number but in case of downsampling no need for LPF; it is simple treatment by throwing some samples [32].

Increasing the rate of sampled signal is Up-sampling whereas decreasing the rate is called downsampling. At any stages in different application sampling rate conversion is demanded. In our case down-sampling process is needed because the available facilities cannot handle it in satisfied time consumption.

4.4. BASEBAND DOWN-CONVERSION

Radio Frequency signals like Bluetooth; typically employ a carrier frequency 2.4 GHz to 2.4358 GHz to travel through air. Generally, RF signal is distinct as the range from nearly 20 kHz – 300 GHz. These frequencies at which energy that coming from electromagnetic equipment can scatter off an antenna and spread over the air.
As mentioned the carrier frequency is 2.4 GHz, like Bluetooth, that means sampling rate at 5 GHz, as stated by Nyquist theorem. Briefly down conversion in the frequency domain as it is shown in Fig. 4.5:

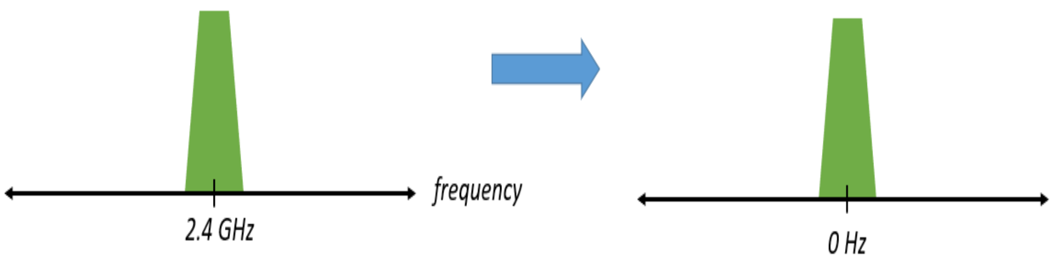


Figure 4.3. Down-conversion by frequency shift.

The down-conversion step is actually process of shifting the center frequency into the origin. By using a higher sampling rate $(5, 10, 20\ Gsps)$ will fulfill the Nyquist rate condition. Moreover, to prevent losing any information of the instantaneous characteristics of the transient signal this means decreasing the sampling aliasing

[30]. On the contrary, operating at higher sampling frequency has some disadvantages, which are associated to the claiming enormous amount of memory usage, besides causing too high central processing unit (CPU) instructions. To deal with this issue; the acquired signals will be translated to a baseband signal.

Accomplishing the baseband in time domain can be done by taking the result of multiplying the signal with a complex exponential [22]:

$$x_{bb}(n) = x^{a}(n) \times e^{-iw_o n} \tag{4.1}$$

Equivalently, in frequency domain, the baseband signal will be achieved by creating the convolution process as:

$$X_{BB}(w) = X_H(w) * 2\pi\delta(w + w_o)$$

4.5. EMPIRICAL MODE DECOMPOSITION EMD

In time domain empirical mode decomposition employed to break down a signal into mono-components called intrinsic mode functions (IMF) [33]. The most important characteristic of the EMD is its feasibility and ability to process non-linear and non-stationary data [34], [35]. Already noticed that most of real-world data whether acquiring the data from experiments or from simulations is non-linear and non-stationary so it is a significant advantage of the EMD compared to the other decomposition methods that it is able to cope with such data. The decomposition by the EMD has literal meaning that the sum of all modes and the residual resemble the original data EMD starts with fitting an envelope through maxima which referred to as the upper envelope E_h and also fitting another envelope through minima called the lower envelope E_l the fitting is usually done by cubic spline functions but just have to ensure that both envelopes cover all data in between them [35], next determining the mean envelope E_m which are obtained from the mean of the upper and lower envelope at each point in time:

$$E_m(t) = \frac{E_h(t) + E_l(t)}{2} \tag{4.2}$$

Then determining a residual which is obtained by subtracting obtained mean envelope from the original signal

$$Res(t) = \left(x(t) + E_m(t)\right) \tag{4.3}$$

To decide whether it is IMF or not; selected stopping criterion in use and the original version of the EMD this stopping criterion is essentially a standard deviation which considers the squared difference between the original signal x(t) and the newly obtained residual divided by the squared signal x(t) the values are summed over all time steps and the resulting single outcome is compared to predefined threshold value

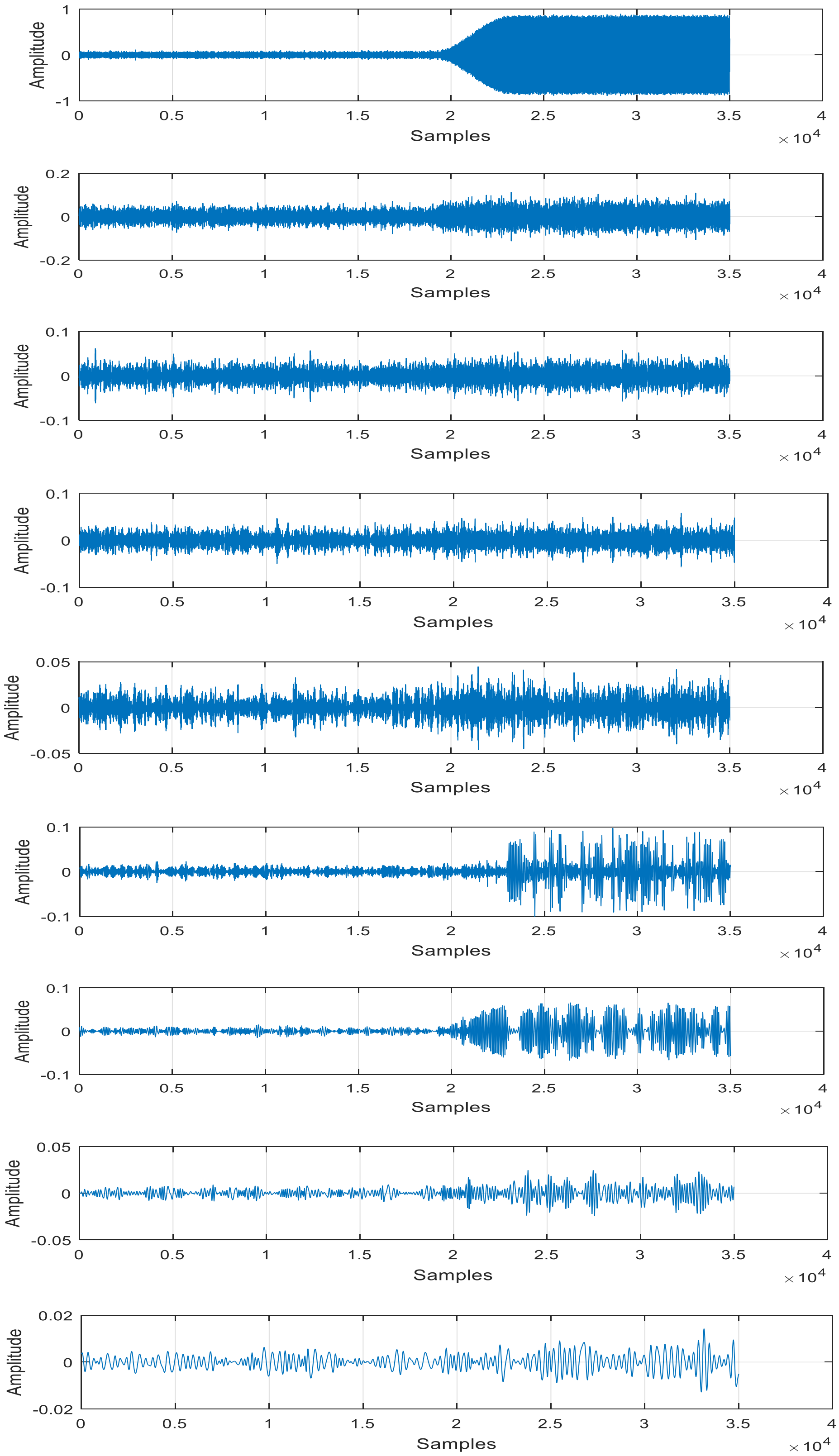
$$\sum_t \frac{(Res(t) - x(t))^2}{(x(t))^2} \leq \epsilon \tag{4.4}$$

If the stopping criterion is not satisfied so this expression here is false and then repeat the process with the residual until the stopping criterion is fulfilled

The yielded IMFs which are a sequence of stationary components must satisfy the two following two conditions [35]:

- The number of zero crossings and the number of maxima or minima for each produced IMF data set, must be either equal
- At any time, the E_m value of two envelops is zero

The EMD method decomposes the IMFs depend on their frequencies, the highest frequency the first decomposed. It can be seen from Figure 4.4 that the dominant IMFs are in descent order from the first IMF to the last. In this research, it has been consider only the first IMF and ignore the others. Accordingly, this will improve Signal-to-Noise Ratio and lessens the computation cost and it will not affect outcomes of transient signal detection, where; mixing two IMFs or more is giving almost the same splitting point.



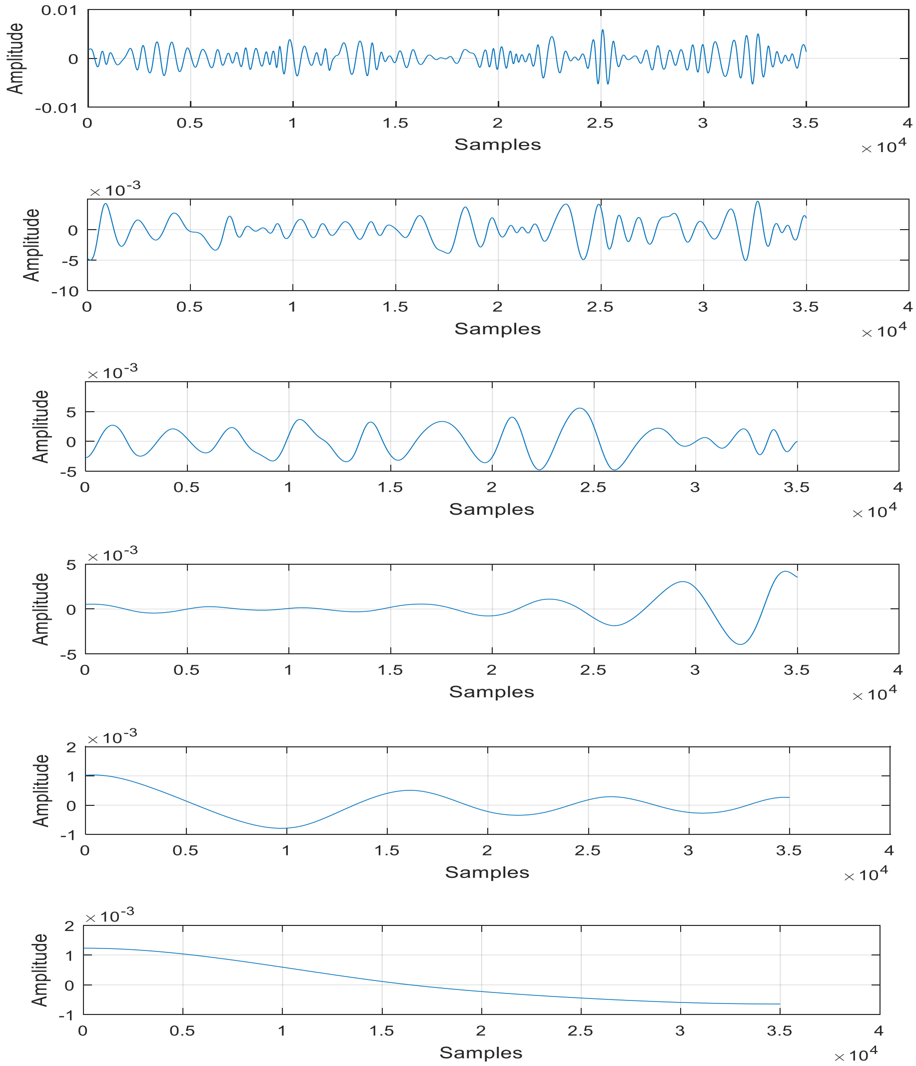


Figure 4.4. IMFs components by EMD of one record.

EMD Procedure in Steps;

- Firstly, EMD is determining of the local maxima and minima of interested signal. This step defining the upper and the lower envelope by using cubic spline function
- Second step, find the mean, *Em(t)* of the upper and the envelopes equation (8).
- Third step is an investigation based on the chosen criteria conditions equation (10) to assess whether the outcome Res(t) equation (9) signifies an IMF or not.
- Fourth step, the first residue Res(t) that is achieved in the last step is treated as input signal. The previous steps need to be repeated based on new original signal.

The next flowchart demonstrated the EMD algorithm. The internal path in the flowchart examine whether IMF has been produced or not. The external loop repeat the process if the result not satisfied

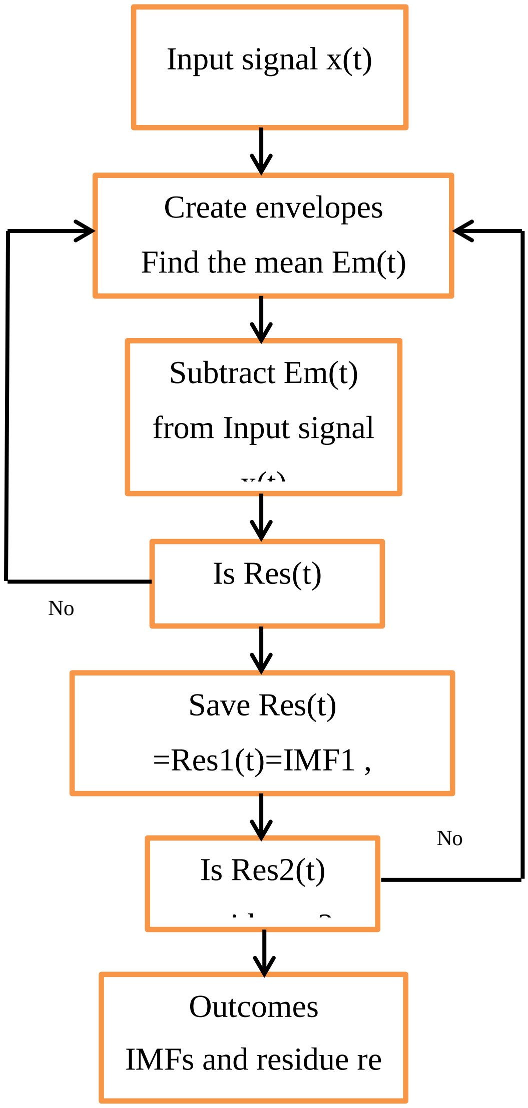


Figure 4.5. Flowchart of EMD algorithm.

4.6. SIGNAL-TO-NOISE RATIO DELIBERATION

The term Signal to Noise Ratio is well-known metric and generally defined as:

$$SNR\_P = 10log10\left(\frac{A_{noisy}}{A_{noise}} - 1\right) \quad (4.5)$$

Or

$$SNR\_P = 10log10\left(\frac{A\_signal}{A\_noise}\right)$$

Where:

$$A\_noisy = A\_signal + A\_noise$$

In same manner SNR is can be defined as the ratio of the mean absolute value after (i.e. noisy signal) and before (i.e. noise) change point sample. To achieve variety of SNR values, the studied signals are handled by different ways, this is done by taking noise that chosen then added to the clean signal and multiplied by factor to that unseen level for the AIC algorithm. The AIC min found before adding any noise is considered as a reference splitting point to find the error when the noise is applied. The exact same noise that produced from a particular record is passed into AIC function in three mentioned ways: direct applied of the original signal, down-converted signal, and the first IMF produced by EMD.

The SNR has been chosen to reflect the capability of AIC algorithm to catch the sudden change when the signal gets distorted:

$$\mathrm{SNR\_MAV} = 20\log 10\left(\frac{\mathrm{N}_2}{\mathrm{N}_1}\frac{\sum_1^k |\mathrm{x}|}{\sum_k^N |\mathrm{x}|}\right) \quad (4.6)$$

Where; N1 is length of signal from 1 to k, and N2 length from k to the N

Because the original record is having background noise most of the AIC values lay in unseen region where the algorithm cannot see the arisen signal and its onset point, it gives an arbitrary onset point does not represent the actual onset point or even close to it, with increasing factor d the error is corrected, see Figure 5.9 and Figure 5.10, and in the other case of down-converted signal most of AIC values are standing in seen region while the signal is getting distortion.

The best value of SNR that can be achieved from manipulated signal is shown in Figure 4.6 and Figure 4.7, for instance the highest SNR level of down-converted signal is 60 dB regarding equation 11 which is matching 30 dB equation 12.

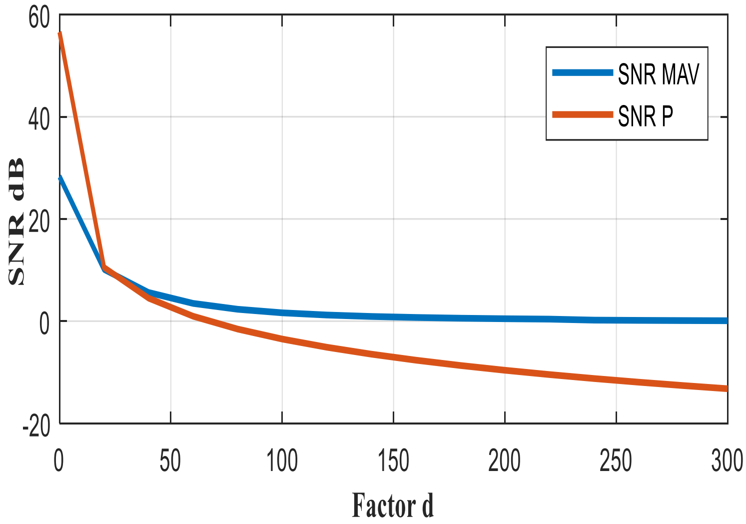


Figure 4.6. Equivalent SNR levels of down-converted signal.

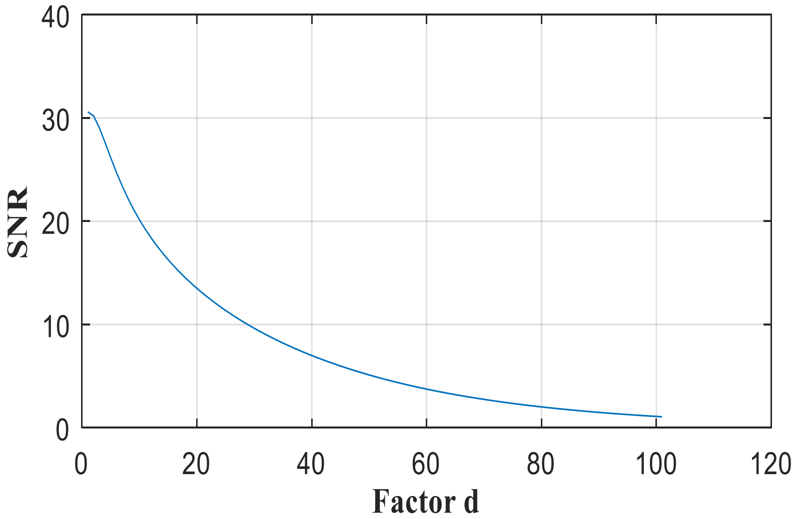


Figure 4.7. SNR Levels of down-converted signal.

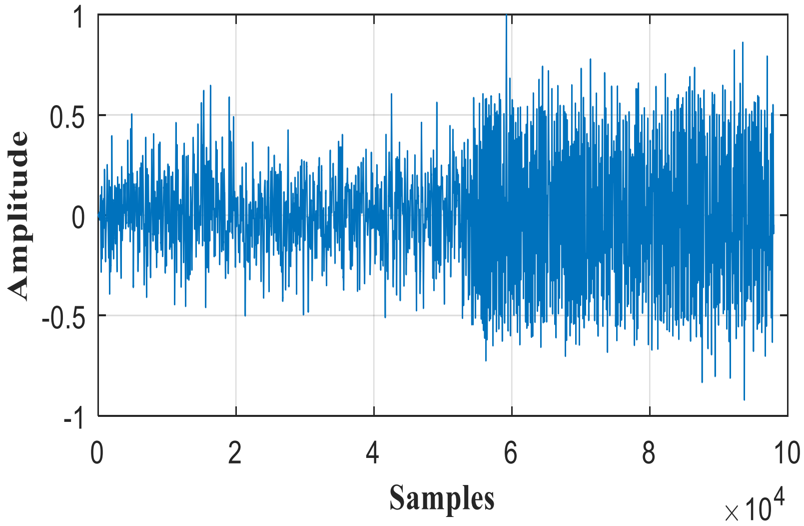


Figure 4.8. Distorted signal at selected level (d=45).

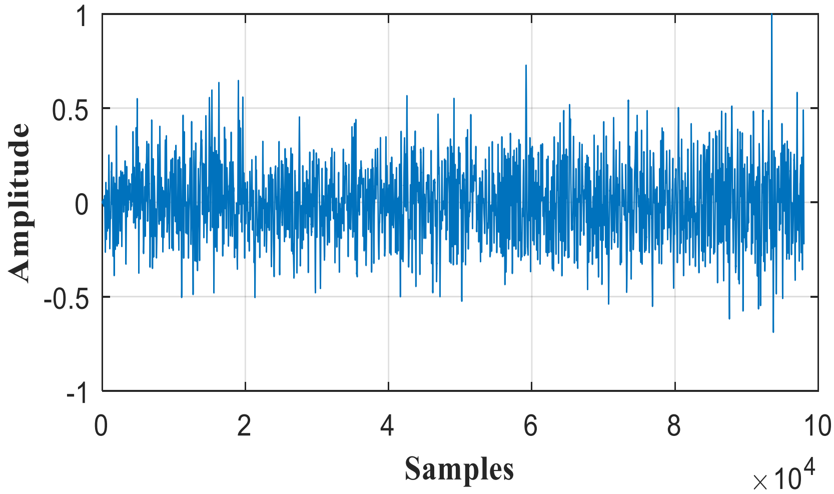


Figure 4.9. Distorted signal at selected level (d=100).

In Figure 4.8 above the signal of examined transmitter can be visualized and easily can be recognized by the algorithm while in Figure 4.9 the distortion is too high; this kind of signal is hard to be detected by the algorithm where; it is obvious from the amplitude of generated noise is nearly the same with the signal.

A few spikes at the beginning of the record which is tiny chunk has been taken from arisen signal Figure 4.10. also have been examined.

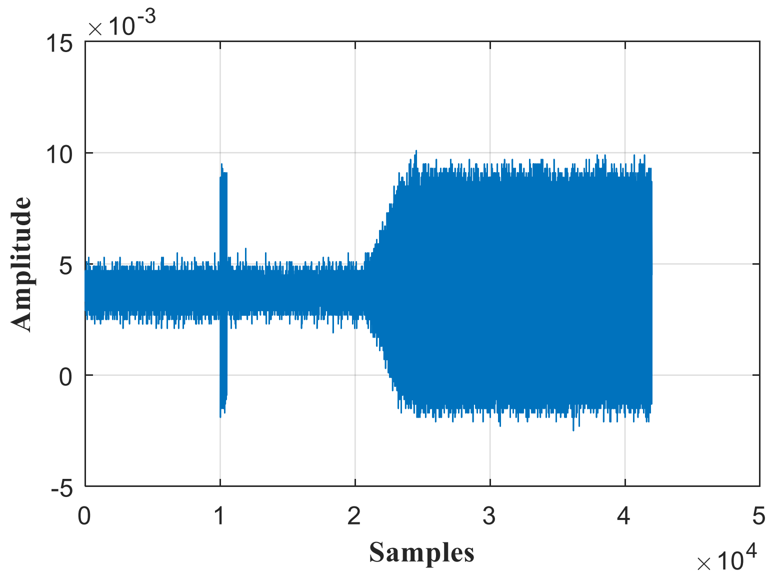


Figure 4.10. Selected record with spike.

The result of detection is seen in Figure 4.11 showing that the onset point represented by splitting line is precise and not affected by that spike.

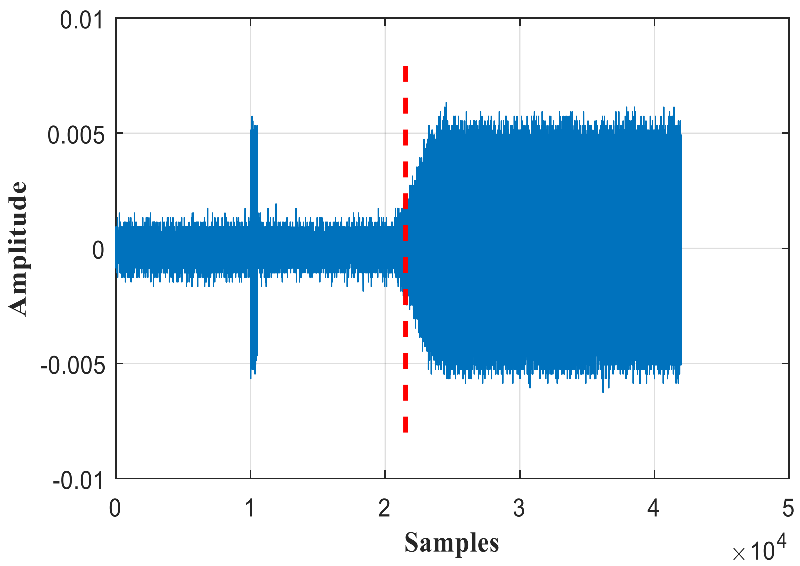


Figure 4.11. The onset point spike affection.

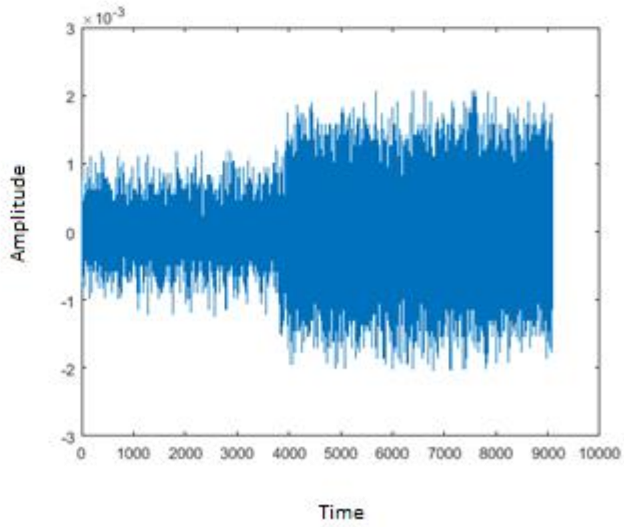
CHAPTER 5

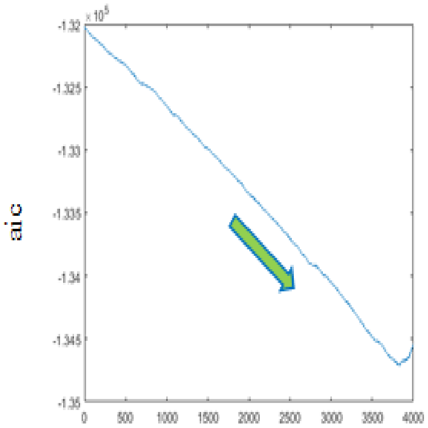
PRACTICAL EXPERIMENT AND RESULTS

As declared in earlier section; there is a reliance of transient segment on the used device type. Some of Bluetooth devices have chunk with small amplitude signal after turning on, and some of other devices reaching steady state at short period of time. However, both these transient starting forms might affect the detection accuracy. Because of that; the AIC method has to be tested by visualizing transient detection point. The performance evaluation has been attained for devices with available datasets.

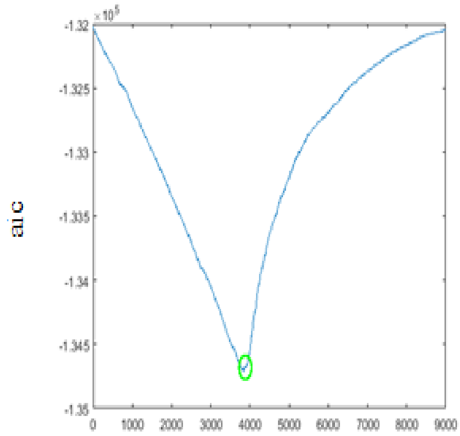
$$error = \frac{|P_r - P|}{f_s} \qquad (sec.) \tag{5.1}$$

The error is found by equation 13, it is the difference between reference start point P_r; which is determined earlier before adding noise, and estimated point P after adding noise divided by sampling frequency. Furthermore, in this study, the error has been determined according to variation of SNR levels by increasing or amplifying noise with factor d. To do so, a chunk noise of one record has been processed and applied for all records to achieve different SNR by increasing factor d one step; or less than one for more details, this is the only way to take decision and make right judgment otherwise every time adding noise will give different result even with same record.





(a) Using part of signal



(b) Using the whole signal

Figure 5.1. AIC algorithm for finding global minimum value.

As illustrated in Figure 5.1, with picked down-sampling factor the moving step k value is multiplied by the log of the variance from sample 1 to k. The variance of segment at the beginning of time series is getting smaller. Then the value is going to drop as k rises. At the sudden change point, the calculated term starts to reverse direction and starts upturning in amplitude.

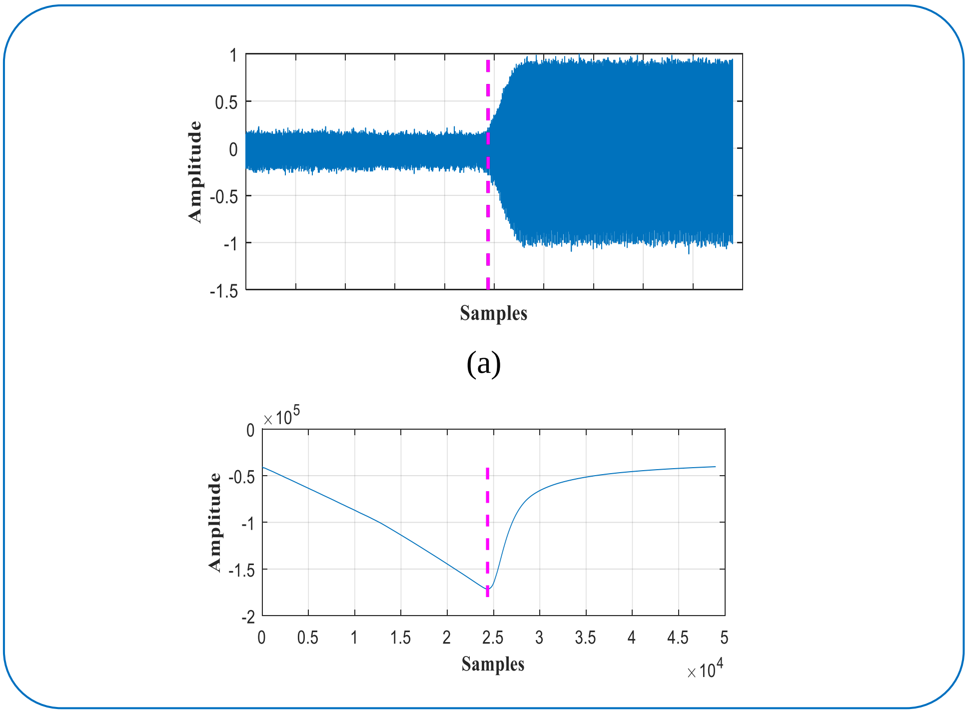


Figure 5.2. (a) The selected recorded signal and (b) is the equivalent AIC values.

As noticed from Figure 5.2 there is one absolute minimum for entire signal, this minimum is selected as the weak up point for AIC algorithm. For a selected record the change point is visible, and AIC algorithm is very fast having a very distinct global minimum.

For the same examined record with process of down-conversion the AIC splitter is more precisely with relatively more consuming time Figure 5. The dotted red line bounds two neighboring time series with altered features. Background noise is discriminated from 1 to k, and arisen signal is recognized from k+1 to N.

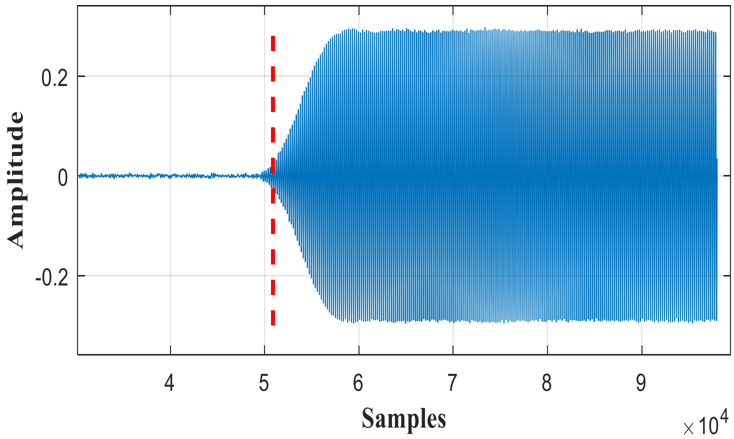


Figure 5.3. AIC min of down-converted signal.

The effect of down-sampling factor n on a particular record is presented in Figure 5.4, having no drawbacks on any other process; it is clear that at small range the splitter line will not affected but at higher value of n will give imprecise splitting point, and incorrect onset point in case of overvalued factor n. In this study, all downsampling factors have been set experimentally.

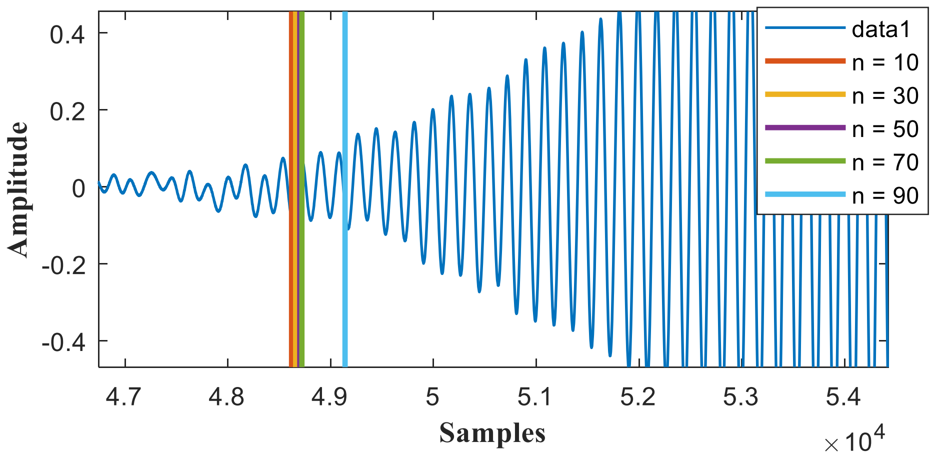


Figure 5.4. Down-sampling factor effect.

Suppose a signal of total length ‘N’ can be broken into stationary components. As distinct here, a stationary process has fixed component over the time of testing. By visualizing or by selecting criteria the 1st IMF is the dominant and chosen to be passed into AIC algorithm.

At global minimum the algorithm is distinguishing that the first chunk is noise and the second chunk is real sender behavior over two intervals as stated in Figure 5.5, the figure shows the onset point of all cases with slightly difference in precision. In case of the three cases the splitter lines usually take place by this order in clean signal.

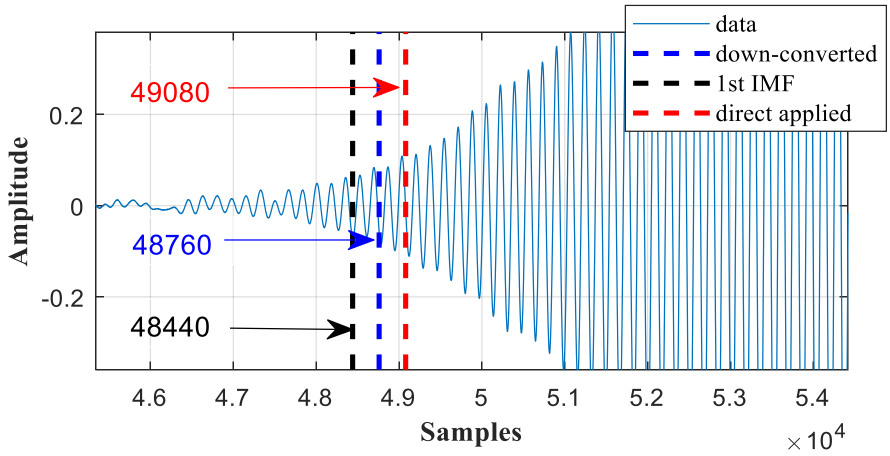


Figure 5.5. AICmin of 1st IMF signal, down-converted, and direct applied.

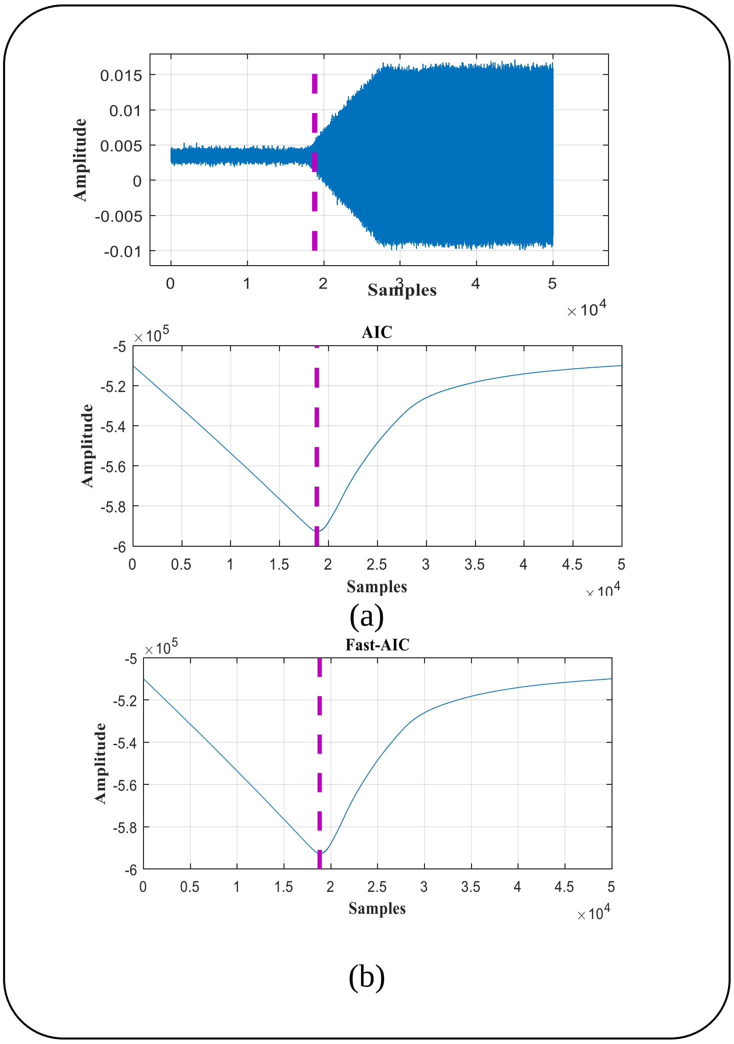


Figure 5.6. The equivalent values of (a) AIC & (b) Alt-AIC for a Chosen recorded.

In case of Alt-AIC Figure 5.6 shows that the Alt-AIC algorithm yields identical result and this algorithm is correspondent to common AIC, the time consuming of Alt-AIC is much better.

The algorithm has been implemented in MATLAB environment and the detection of start point of the transient signal is obtained based on the Akaike Information Criterion (AIC) and Alt-AIC. All onset points have been spotted and kept in plain text files for further processing Figure 5.7.

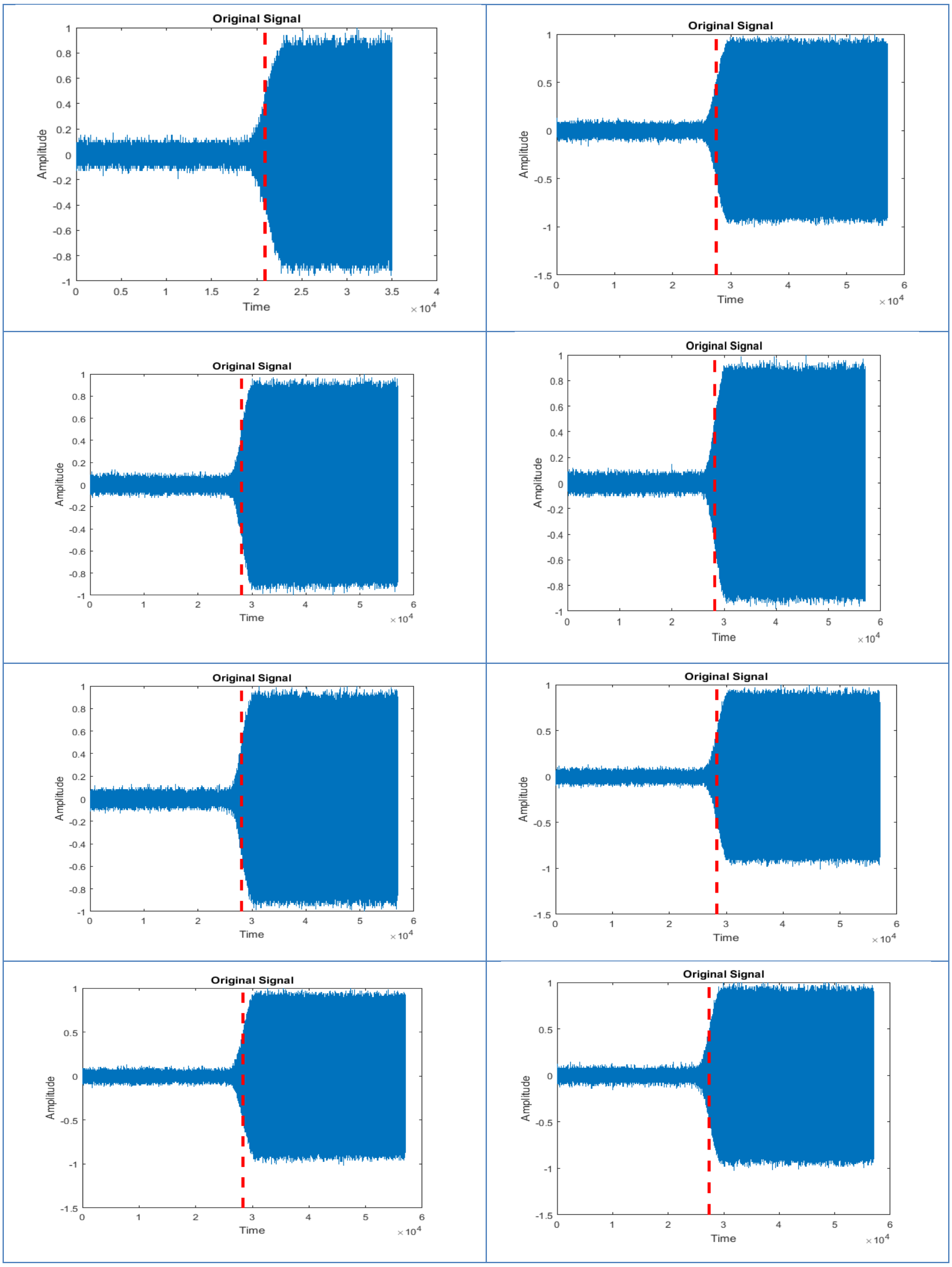


Figure 5.7. Samples output of chosen detection method.

5.1. PERFORMANCE ANALYSIS OF SNR

Almost all onset point of records have been achieved correctly and by visualizing too many samples to make a decision; they are remarkably good attainments and will be regarded as reference points. Next stage is to find these points in noise environments by adding noise to the records and tuning the Signal to Noise Ratio SNR.

Signal to noise ratio SNR is applied to measure to how extent the signal is distorted, which reflects that the higher SNR is achieved by making the effect of noise signal smaller. Accordingly, the power of desired signal will be higher than power of the background noise.

The performance assessment of the progressed transient detection method AIC, and the other method Alt-AIC would be more reliable, if the algorithms manage to perform in lower levels of SNR. In doing this, there are many ways;

The Bluetooth noise signal chunk has been used, as mentioned earlier every record contains own noise, so this part can be taken and amplified, especially the proposed method is suggested to find the noise besides the performance will be accomplished by realistic noise.

Another way; preparing and recording the noise signal before recording the desired signal, and then extending that noise according to the length of Bluetooth signal. This operation can be performed automatically and if the noise signals are the same for all records then will be the best choice.

Last way, producing the noise artificially by built-in function of Matlab, in this way the related outcome inside code should not be changed every loop.

In this study; all methods have been examined and the second method has been adapted, in the second way, and the values of factor d has range from 0-100 by using step 1, to decrease the SNR, the levels of SNR will be accomplished, as shown in Figure 2.14, and corresponding signals in Figure 2.15.

The error of SNR evaluation between reference splitting point and noisy splitting point for two cases is depicted in Figure 5.10, as the signal gets distortion the down-converted case the algorithm can handle more distortion levels than direct applied case

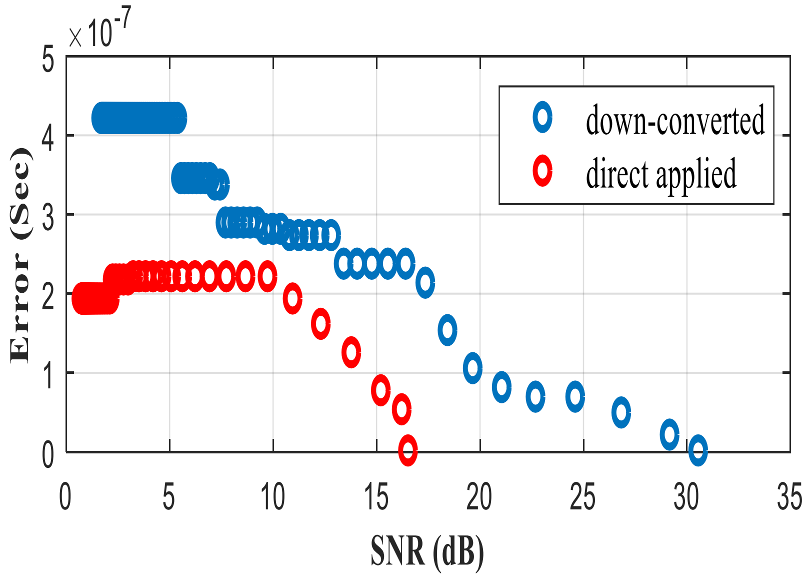


Figure 5.8. SNR Performance of down-converted and direct applied cases.

At low SNR, there are always one global minimum and the algorithm still gives accurately splitting point Figure 5.11 (middle of figure) and will be shifted in direction of imprecise onset point. If SNR is very low, AIC_m global minimum is not yielded correctly onset points represented by unseen onset Figure 5.11 (right side)

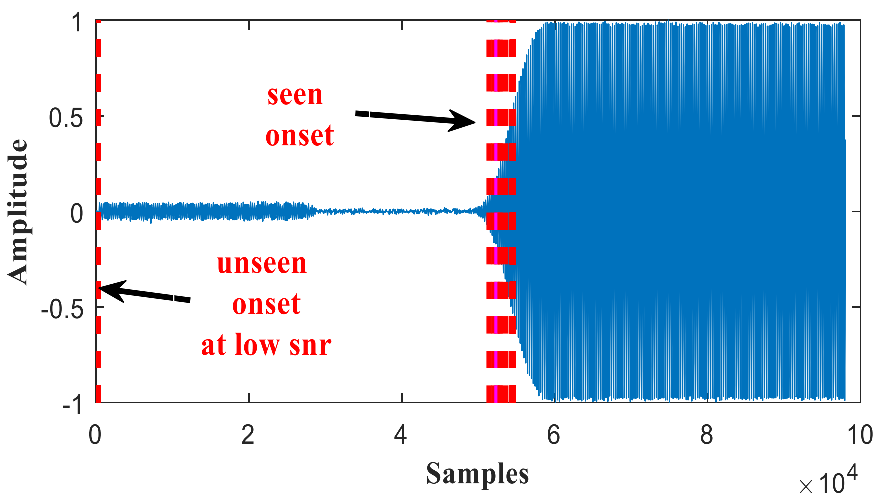


Figure 5.9. Down-converted signal with AICmin of all SNR levels.

The performance of decomposed IMF is seen in Figure 5.12 this case can treat much more levels of SNR. So, combination of EMD and AIC is effective and powerful in presence of noise at high levels for RF data and was the best among adapted methods.

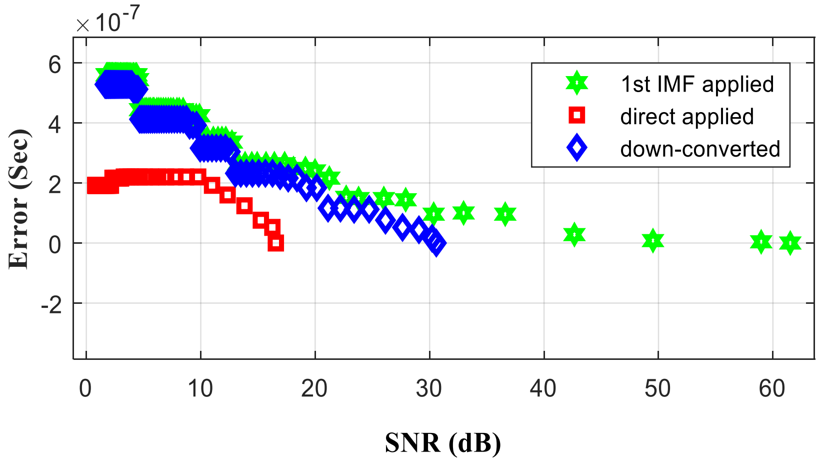


Figure 5.10. 1st IMF, down-converted and direct applied SNR performance.

Retrieving results from applying the original signal directly without any sorts of preprocessing into the algorithm is an advantage of this method, also the average consuming time is around 0.03 sec and in case of Alt-AIC the time is 0.015 sec denoting to that the complexity is lesser.

The performance of the algorithm is effective and good as long as the amplitude of interfered noise is less than the amplitude of sender signal where the algorithm is not affected by just few high amplitude spikes at the beginning of examined signal.

CHAPTER 6

CONCLUSION

In this thesis, huge amount of data from Bluetooth transmitter are examined in RF detection implementation. Bluetooth signals are gathered from many cell phones' brands. Every cell phone of the six transmitters has 2 different devices, each with one hundred and fifty records have been evaluated in this study. The assembled Bluetooth signals are treated by different ways. The first way is done by passing every single record without any kind of preprocessing as it is produced from their equipment; in this method the AIC algorithm presented good results despite the signal is having background noise.

The second way is made by down-converting the examined signal to its baseband. On third way, the signal is decomposed by EMD to its IMFs components then one or two IMFs are selected to be evaluated by the algorithm.

The simulation results demonstrate that both selected method and alternative version are effective for different Bluetooth devices, and its accomplishments quite high performance. After a comparison between the accuracies of the three noted methods; it is realized that the detector precisions are getting better after putting on filtering process.

The transient signals of the wireless transmission signals are detected by using a novel transient detection technique based on Akaike Information Criterion AIC. By using this technique and visualizing the results, the sudden change point of the transient are estimated correctly. However, it is utter importance to boost the performance of suggested methods for more practical execution and lower computational instructions. The algorithm is based on the comparing of two different chunks. In order to improve detection outcomes an alternative method of AIC is used called Alt-AIC; the performance of this method is better and more suitable to available facilities. Both detectors are reliable and they have satisfied consuming time, however the Alt-AIC is always recording half time of the regular method AIC. The proposed detectors are robust and powerful in the presence of random noise with relatively large impulses. Both methods should be employed with assistance of downsampling for higher sampling rate of RF data, otherwise the process will take longer time.

A comparison of time picking methods based upon the Akaike Information Criterion (AIC) has been demonstrated, both AIC and Alt-AIC are showing high precision detecting and highly recommend to be involved in RF data interpreting.

According to evaluation process and the results the proposed algorithm can be used offline and also online detector where it possible to detect onset point with the lack of the prior knowledge of the incoming signal.

REFERENCES

1. Ellis, K. ~J. and Serinken, N., "Characteristics of radio transmitter fingerprints", ***Radio Science***, 36 (4): 585–597 (2001).

2. Poblet, M., "Mobile Technologies for Conflict Management: Online Dispute Resolution, Governance, Participation", (2011).

3. Zhuo, F., Huang, Y., and Chen, J., "Specific Emitter Identification based on the Energy Envelope of Transient Signal", .

4. Rehman, S. U., Sowerby, K. W., and Coghill, C., "RF fingerprint extraction from the energy envelope of an instantaneous transient signal", ***2012 Australian Communications Theory Workshop (AusCTW)***, 90–95 (2012).

5. Kennedy, I. O., Scanlon, P., Mullany, F. J., Buddhikot, M. M., Nolan, K. E., and Rondeau, T. W., "Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach", (2008).

6. Ureten, O. and Serinken, N., "Bayesian detection of radio transmitter turn-on transients.", (1999).

7. Hall, J., Barbeau, M., and Kranakis, E., "Detection Of Transient In Radio Frequency Fingerprinting Using Signal Phase", (2003).

8. Mohamed, I., Dalveren, Y., and Kara, A., "Performance Assessment of Transient Signal Detection Methods and Superiority of Energy Criterion (EC) Method", ***IEEE Access***, PP: 1 (2020).

9. Haataja, K., Hyppönen, K., Pasanen, S., and Toivanen, P., "Bluetooth security attacks: Comparative analysis, attacks, and countermeasures", SpringerBriefs in Computer Science, 1–93 (2013).

10. Waghmare, R., Nalbalwar, S., and Das, A., "Transient Signal Detection on the Basis of Energy and Zero Crossing Detectors", ***Procedia Engineering***, 30: 129–134 (2012).

11. Yuan, Y., Huang, Z., Wu, H., and Wang, X., "Specific emitter identification based on Hilbert-Huang transform-based time-frequency-energy distribution features", ***Communications, IET***, 8: 2404–2412 (2014).

12. Ureten, O. and Serinken, N., "Wireless security through RF fingerprinting", ***Electrical And Computer Engineering, Canadian Journal Of***, 32: 27–33 (2007).

13. Uzundurukan, E., Dalveren, Y., and Kara, A., "A Database for the Radio Frequency Fingerprinting of Bluetooth Devices", ***Data***, 5: 55 (2020).

14. de Leeuw, J., "Information Theory And An Extension Of The Maximum Likelihood Principle By Hirotogu Akaike", (1994).

15. Laurent-Maknavicius, M. and Chaouchi, H., "Mobile and Wireless Networks Security: Proceedings of the MWNS 2008 Workshop : Singapore 9 April 2008", ***World Scientific***, (2008).

16. Zheng, P., Peterson, L. L., Davie, B. S., and Farrel, A., "Wireless Networking Complete", ***Elsevier Science***, (2009).

17. Zahariadis, T. B., "Home Networking Technologies and Standards", ***Artech House***, (2003).

18. Benvenuto, N. and Zorzi, M., "Principles of Communications Networks and Systems", ***Wiley***, (2011).

19. Burbank, J. L., Andrusenko, J., Everett, J. S., and Kasch, W. T. M., "Wireless Networking: Understanding Internetworking Challenges", ***Wiley***, (2013).

20. Albazrqaoe, W., "A Study of Bluetooth Frequency Hopping Sequence: Modeling and a Practical Attack", ***Michigan State University. Computer Science***, (2011).

21. Nicopolitidis, P., Obaidat, M. S., Papadimitriou, G. I., and Pomportsis, A. S., "Wireless Networks", ***Wiley***, (2003).

22. Chew, D., "The Wireless Internet of Things: A Guide to the Lower Layers", ***Wiley***, (2018).

23. Gast, M. S., "802.11 Wireless Networks: The Definitive Guide: The Definitive Guide", ***O'Reilly Media***, (2005).

24. Shaw, D. and Kinsner, W., "Multifractal modelling of radio transmitter transients for classification", ***IEEE WESCANEX 97 Communications, Power And Computing. Conference Proceedings***, 306–312 (1997).

25. Wagenaars, P., Wouters, P., der Wielen, P., and Steennis, E. F., "Comparison of arrival time estimation methods for partial discharge pulses in power cables", (2008).

26. Cavanaugh, J. E. and Neath, A. A., "The Akaike information criterion: Background, derivation, properties, application, interpretation, and refinements", ***WIREs Computational Statistics***, 11 (3): e1460 (2019).

27. Kurz, J., Grosse, C., and Reinhardt, H.-W., "Strategies for reliable automatic onset time picking of acoustic emissions and of ultrasound signals in concrete", ***Ultrasonics***, 43: 538–546 (2005).

28. Wagenaars, P., Wouters, P. A. A. F., van der Wielen, P. C. J. M., and Steennis, E. F., "Algorithms for Arrival Time Estimation of Partial Discharge Pulses in Cable Systems", (2008).

29. Sleeman, R. and van Eck, T., "Robust automatic P-phase picking: an on-line implementation in the analysis of broadband seismogram recordings", ***Physics Of The Earth And Planetary Interiors***, 113 (1): 265–275 (1999).

30. Maeda, N., "A Method for Reading and Checking Phase Time in Auto-Processing System of Seismic Wave Data", ***Journal Of The Seismological Society Of Japan***, 38: 365–379 (1985).

31. Li, X., Shang, X., Morales-Esteban, A., and Wang, Z., "Identifying P phase arrival of weak events: The Akaike Information Criterion picking application based on the Empirical Mode Decomposition", ***Computers & Geosciences***, 100: (2016).

32. Eynde, F. and Sansen, W. M. C., "Analog Interfaces for Digital Signal Processing Systems", ***Springer US***, (2012).

33. Zeiler, A., Faltermeier, R., Keck, I. R., Tomé, A. M., Puntonet, C. G., and Lang, E. W., "Empirical Mode Decomposition - an introduction", (2010).

34. Huang, N., Shen, Z., Long, S., Wu, M. L. C., Shih, H., Zheng, Q., Yen, N.-C., Tung, C.-C., and Liu, H., "The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis", ***Proceedings Of The Royal Society Of London. Series A: Mathematical, Physical And Engineering Sciences***, 454: 903–995 (1998).

35. Kim, D. and Oh, H.-S., "EMD: A Package for Empirical Mode Decomposition and Hilbert Spectrum", ***R Journal***, 1: (2009).

RESUME

Saleh Abulgasem Ajouat was born in Libya. He has accomplished his primary and secondary degrees in the same governorate. He has studied and achieved high school certificate Seventh of April High School in Baniwalid governorate. Then he started undergraduate program and acquired his bachelor degree in Electronic Technology University, Department of Electric and Electronic in 2002. He has got his M. Sc. from Atilim University Ankara 2017.