Faculty of Engineering and Technology

Joint Master Program in Electrical Engineering (JMEE)

Detecting Misbehaving Activities in Current /Future Wireless Networks

Student Name: Eng. Ruba Eid

Supervisor : Dr. Wael Hashlamoun

This Thesis is submitted in partial fulfillment of the requirements for the Master’s Degree in Electrical Engineering from the Faculty of Graduate Studies at Birzeit University, Palestine

Jan 18, 2024

جامعة بيرزيت
BIRZEIT UNIVERSITY

Detecting Misbehaving Activities in Current /Future Wireless Networks

كشف الاختراق في الشبكات اللاسلكية الحالية / المستقبلية

Submitted by:

Ruba Kamal Ahmad Eid

Approved by the Examining Committee

Supervisor

Dr. Wael Al-Hashlamon ...Wael...Hashlamoun

Examiners

Dr. Mohammad Jubran ...mohammad Jubran...

Dr. Qadri Mayaleh...Qadri...

BIRZEIT, PALESTINE

Jan 2024

Declaration of Authorship

I declare that this thesis entitled “Detecting Misbehaving Activities in Current /Future Wireless Networks” is the result of my own research except as cited in the references. It was submitted to the master’s degree in Electrical Engineering from the Faculty of Engineering and Technology at Birzeit University, Palestine. The thesis has not been accepted for any degree and is not concurrently submitted in the candidature of any other degree.

Signed: Ruba Eid

Date: Jan 18, 2024

Abstract

Cognitive Radio (CR) is a widely used wireless radio communication to utilize the available spectrum space of licensed users (Primary Users) efficiently. In CR, secondary users (SUs) try to sense and utilize the vacant spectrum of the legitimate primary user (PU) in an efficient manner. The process of cooperation among SUs makes the sensing more authentic with minimum disturbance to the PU in achieving maximum utilization of the vacant spectrum. Although cooperative spectrum sensing (CSS) in current/future wireless network has the problems of multipath fading, shadowing and noise uncertainty, CSS is vulnerable by spectrum sensing data falsification attacks (SSDF) which occurs by malicious users (MUs) sending false data to the fusion center (FC). In literature, these attacks are alleviated using reputation schemes in which the history of the user is traced and accumulated for future contacts. Reputation-based solution might hack the privacy of user [1].

In this study, the detection probability is raised using the coefficient of variation (CV), which measures the variation of the sampled signals. If the signal variation measurements at FC exceed a certain level, it is assumed that another user is using the spectrum bands. In order to reduce user misbehavior in the CR network, the FC makes a global decision based on the hard binary decisions received from all SUs without identifying or knowing the precise location of each user. Numerical simulations demonstrate that the two suggested methods achieve a good detection performance of CR network. Also, a comparison between the fixed measurement approach and the sequential measurement method was made to confirm that the last one minimizes system overhead. MATLAB was used to investigate the impact of the amount of malicious users, the probability of their attacks, and the number of measures on FC detection.

المستخلص

Cognitive Radio (CR) هو اتصال لاسلكي واسع الاستخدام للاستفادة من مساحة الطيف المتاحة للمستخدمين المرخصين (المستخدمون الأساسيون) بكفاءة. في CR ، يحاول المستخدمون الثانويون (SUs) استشعار واستخدام الطيف الشاغر للمستخدم الأساسي الشرعي (PU) بطريقة فعالة. عند حدوث عملية تعاون بين المستخدمين الثانويين اثناء استشعار الطيف (بدلا من استشعار فرديا لكل مستخدم) ، فإن عملية الاستشعارتكون أكثر واقعية مع تقليل الإزعاج لـ PU ، مما يساعد في تحقيق اقصى استفادة من الطيف الشاغر. على الرغم من أن الاستشعار التعاوني للطيف (CSS) في الشبكة اللاسلكية الحالية / المستقبلية يواجه مشاكل الخبو متعدد المسارات والتظليل وعدم اليقين من الضوضاء ، إلا أن الاستشعار التعاوني للطيف يكون عرضة لهجمات تزوير بيانات استشعار الطيف (SSDF) التي تحدث من قبل المستخدمين الخبثاء (MUs) الذين يرسلون بيانات خاطئة إلى مركز دمج البيانات (FC). في الأدبيات ، يتم تخفيف هذه الهجمات باستخدام مخططات السمعة التي يتم فيها تتبع تاريخ المستخدم وتجميعه لجهات الاتصال المستقبلية. الحل القائم على السمعة قد يخترق خصوصية المستخدم [1].

في هذه الدراسة ، يتم رفع احتمالية الاكتشاف باستخدام معامل التباين (CV) ، الذي يقيس تباين الإشارات التي تم أخذ عينات منها. إذا تجاوزت قياسات تغير الإشارة عند FC مستوى معينًا ، يُفترض أن مستخدمًا آخر يستخدم نطاقات الطيف. من أجل الحد من سوء سلوك المستخدم في شبكة CR ، يتخذ FC قرارًا عالميًا بناءً على القرارات الثنائية (التي تتمثل بأصفار وواحدات) التي يتم تلقيها من جميع وحدات النظام دون تحديد أو معرفة الموقع الدقيق لكل مستخدم. توضح عمليات المحاكاة العددية أن الطريقتين المقترحتين تحققان أداء كشف جيد لشبكة CR. كما تم إجراء مقارنة بين أسلوب القياس الثابت وأسلوب القياس المتسلسل للتأكد من أن الأسلوب الثاني يقلل من الحمل الزائد للنظام. تم استخدام برنامج MATLAB لتحليل وتوضيح ماهية تأثير عدد المستخدمين الضارين، واحتمالية هجماتهم، وعدد البيانات المطلوب ارسالها الى مركز دمج البيانات(FC).

Keywords— Primary User, Secondary User, Malicious User, Detection, Security, Energy Detector, Cognitive Radio, Probability of Detection, Gaussian Approximations, Cooperative Sensing, Spectrum Sensing, Probability of False Alarm, Fixed Measurement Approach, Sequential Measurement Approach.

Acknowledgements

First of all, I am sincerely grateful to Allah for assisting me in successfully completing my project. Days passed, and I began my life with a step, and here I am today, reaping the fruits of years in which my aim was clear, and I worked every day to attain it and reach it no matter how difficult it was...

Today I stand before you, and I am here with a flame of knowledge in my hand, which I will carefully keep so that it does not go out, and I thank God first and foremost for assisting me and continuing to assist me in my efforts. Then I would like to thank the kind heart that has been by my side through all of these stages, my beloved mother. And to the one who taught me to stand and how to begin the thousand miles by step, to my right hand, to the one who taught me to ascend while keeping his eyes on me, my father.

Then, I would like to express my deep appreciation to my supervisor, Dr. Wael Al-Hashlamon, for guiding me through my thesis successfully. Dr. Loqman's assistance will remain in my memory. Thank you for all of your support and explanations. I would also like to express my thanks to my brothers and sisters, my love, and my friends.

Contents

List of Figures

List of Tables

List of Abbreviations

ANMU	Always No Malicious User
AWGN	Additive White Gaussian Noise
AYMU	Always Yes Malicious User
CET	Continuous Wavelet Transform
CLT	Central Limit Theorem
CR	Cognitive Radio
CSD	Cyclostationary Detection
CSS	Cooperative Spectrum Sensing
CV	Coefficient of Variation
$\mathrm{CV}_{\mathrm{H}0}$	Coefficient of Variation at FC under H_0
$\mathrm{CV}_{\mathrm{H}1}$	Coefficient of Variation at FC under H_1
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
ED	Energy Detector
FC	Fusion Center
H_0	Hypothesis 0
H_1	Hypothesis 1
ITU	International Telecommunication Union
LRT	Likelihood Ratio Test
MF	Matched Filter
MUDO	Malicious User Detection by Ordering
MUs	Malicious Users
N_m	MU Total Number
N_n	LU Total Number

$\mathrm{N_u}$	Number of SU Sensors
NP	Neyman-Pearson
OFDM	Orthogonal Frequency Division Multiplexing
OMU	Opposite Malicious User or Always False
$\mathrm{P_d}$	Local Detection Probability of the Sensing Node.
pdf	Probability Density Function
$\mathrm{P_{d_{LU}}}$	Detection Probability of LU Nodes
$\mathrm{P_{d_{MU}}}$	Detection Probability of MUs
$\mathrm{P_{D_{FC}}}$	Detection Probability of the FC
$\mathrm{P_{error}}$	Error Probability at FC
$\mathrm{P_{fa_{LU}}}$	False Alarm Probability of LU Nodes
$\mathrm{P_{fa_{MU}}}$	False Alarm Probability of MUs
$\mathrm{P_{fa}}$	Local False Alarm Probability of the Sensing Node.
$\mathrm{P_{FA_{FC}}}$	False Alarm Probability of the FC
Pi_{0}	Probability of $\mathrm{H_0}$
Pi_{1}	Probability of $\mathrm{H_1}$
$\mathrm{P_{md}}$	Missed-Detection Probability
PU	Primary User
PUD	PU Detection
Q	Gaussian-Q Function
R1, R2	Roots of Test Statistic Y
ROMU	Random Opposite Malicious User
S	PU Signal
SNR	Signal to Noise Ratio
SS	Spectrum Sensing

SSDF	Spectrum Sensing Data Falsification Attacks
Sus	Secondary Users
T	Total Number of Samples for Each SUs Sensor
w(t)	Noise Signal
X(t)	Signal Detected for Each Sensor
Y	Local Test Statistic
Z_s	Summation of Local Binary Decisions Received at FC
Z_{sj}	($\ell \times (N_m+N_n)$) - Dimensional Frame Matrix Signal.
α	Attacking Probability of MUs
$\sigma^2{}_s$	Variance of PU Signal
$\sigma^2{}_w$	Variance of the Noise Signal
$\sigma^2{}_X$	Variance of x
μ_y	Mean of y
$\sigma_y{}^2$	Variance of y
$\hat{\mu}_{Zs}$	Mean of Z_s
$\hat{\sigma}_{Zs}{}^2$	Variance of Z_s
η	Test Statistic Threshold at FC
λ	ED Threshold
ℓ	Forwarding Times from All SUs
γ	Threshold of Local Test Statistic
$\chi_1{}^2$	Chi-Square with 1 Degree of Freedom
Γ	Gamma Distribution
$\hat{Z}$	Local Hard Decision
$\hat{Z}_{MU}$	Local Hard Decision of MU
$\hat{Z}_{LU}$	Local Hard Decision of LU

Chapter 1

Introduction

1.1 Background

The radio spectrum of interest in wireless communication systems ranges from 3 Hz to 3000 GHz [2]. Terminals in these systems communicate with each other over a portion of the radio spectrum.

Governments worldwide, through the International Telecommunication Union (ITU), have divided the radio spectrum into several ranges, each of which is allocated for a specific technology-based wireless communication. According to the spectrum regularity bodies, the spectrum allocation process is static. The main advantage of the allocation process being static is that it can generate the best quality of service in terms of interference among the allocated ranges.

Several frequency occupancy measurements, conducted in different countries, show that the static spectrum allocation process is the reason for spectrum underutilization. Since the 1920s, outdated technologies have motivated the static process.

Several solutions have been proposed to address the issue of spectrum underutilization, including dynamic spectrum sensing-based CR networks. Spectrum sensing (SS) is a prerequisite for the deployment of wireless networks [3]. SS is the mechanism by which an SU transceiver detects the absence of PU in order to use the PU-allocated spectrum. That part of the spectrum resulting from the PU being idle is known as the "hole" or "white space" [4], [5]. In CR networks, there are two types of users: the PU, who has the full right to use licensed spectrum, and the SU, who could have the licensed spectrum if and only if the PU is absent.

The main idea behind CR technology is that it senses the environment of the PU in order to decide if it is active or inactive. If the PU is inactive, the SU can use the licensed spectrum band; otherwise, the SU must keep silent.

There are numerous local detection approaches available for determining whether or not the PU is busy. However, each of these strategies is appropriate for a particular scenario.

In signal processing methods for SS, three main approaches are commonly used [6]:

- Matched filter (MF)
- Energy detector (ED)
- Cyclostationary feature detector

In MF, the SU receivers can identify the PU signal by creating a filter that is appropriate for the received signal type. This method implies that SU is aware of the specifications of the PU signal, such as its bandwidth, frequency, type of modulation, packet format, etc. The ability of the MF to maximize the received signal-to-noise ratio (SNR) is shown in [7]. The advantage of MF is that it takes less time to attain high processing gains due to its coherency. However, a main disadvantage of a MF is the requirement of a unique receiver for each PU. As a result, the aforementioned drawback limits the utilization of the MF.

When using the cyclostationary detection (CSD) approach, the SU searches for semi-periodic features that are relevant to the operating frequency, required bandwidth, frame format, and modulation types [5]. A drawback of the cyclostationary feature detector is that it requires more processing time and computational complexity [8].

Compared to matched or cyclostationary detectors, ED has a significant benefit in that it is simple and does not require any a priori knowledge of the primary signal. In cooperative sensing, it is the most widely used sensing method [9–11]. The SNR wall is a restriction on the ED’s performance that is imposed by the noise uncertainty effect, which has a significant impact on the ED's sensing performance [12–14].

ED has been extensively used in radiometry. Consequently, we only discuss the ED in detail. A signal's energy over a specific amount of time is calculated using an energy detection algorithm, and it is compared to a deterministic threshold value to determine whether the PU is present. The energy detection algorithm's block diagram is shown in Fig.1-1 [27].

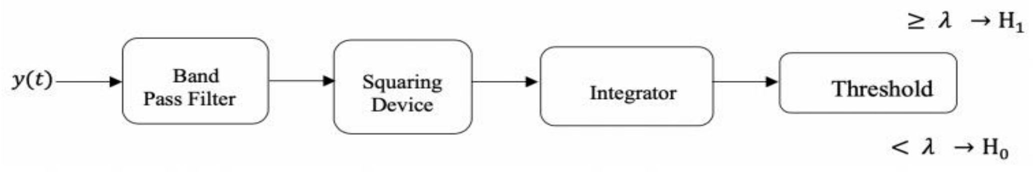


Fig.1-1: Block Diagram of Energy Detection Algorithm [27]

It is composed of four main blocks [37]:

1) Band Pass Filter

2) Squaring Device

3) Integrator

4) Threshold device

This method involves passing the signal through a band pass filter with a bandwidth of W, multiplying it by itself to square it, and integrating the result over a period of time. The presence or absence of the PU is then determined by comparing the output from the integrator block to a predefined threshold. Depending on the channel conditions, the threshold value can either be fixed or variable [37].

Local identification of the status of the PU is highly affected by wireless channel conditions like multipath fading, shadowing, noise uncertainty and hidden terminal problem [15]. For this reason, the CSS is preferred over the individual one. In CSS, group of users make sensing to make a global decision which is more accurate than only one decided. This cooperation can alleviate the problems of fading, error, shadowing and noise uncertainty. However, CSS is highly vulnerable to SSDF [16]. In an SSDF attack, a misbehaving SU shares incorrect information in order to degrade CSS performance.

There are two types of CSS. One is centralized CSS, such that the SUs send their local detection to the FC, where a decision is made about the absence or presence of a legitimate user. The second is decentralized CSS, in which each SU determines the presence of PU based on the information they have independently gathered. The final decision of whether or not PU is present will thereafter be made by the collaborating users as there isn't a fusion center. However, the primary issue with decentralized CSS is that, because the wireless channel is constantly changing, SS made by a single user is useless. Therefore, the decision is inaccurate if any SU decides whether or not PU is present. Additionally, the overhead in the system will rise as a result of the SUs collaborating to share decisions of this type with other groups and with each other. To reduce the overhead and decision-making errors, we employed centralized CSS for this. After that, the decisions are then sent to FC to be summed to determine the system status.

There are four different categories of abnormal SUs (MU): the opposite malicious user or always false (OMU), the random opposite malicious user (ROMU), the always yes malicious user (AYMU), and the always no malicious user (ANMU).

Regardless of the actual PU spectrum status, an AYMU sends a high-energy signal to the FC, which increases the likelihood of false alarms and decreases throughput for the SUs. Because the licensed user channel is always available thanks to the ANMU, the likelihood of a misdetection is increased, and the interference with the PU transmission increases as a result. Similar to how it does with the PU's actual condition, the OMU always negates it. In terms of AYMU and ANMU, it's an extreme case. Due to the OMU, the PU is subjected to increased interference, false alarms, misdetection probabilities, and bandwidth reduction. The ROMU performs malicious acts with a discrete distribution and a specific probability, which makes their malicious nature unpredictable and challenging to eliminate. According to probability α, the ROMU behaves as an OMU, and according to probability 1-α, it expresses as a normal SU [35, 36]. In this research, the proposed method is tested based on the performance of ROMU, as that is the general case for all different categories of MU.

A statistical technique was used in a few studies to examine how well CR performed. However, no one has yet studied this technique in CR while saving privacy in a ROMUshard-decision network. Therefore, this thesis mainly focuses on the performance of the CR system by alleviating the misbehaving behavior of the user without specifically identifying each user.

This thesis proposes two measurement approaches: fixed FC scheme for PU detection (PUD) based on a single threshold is performed using a fixed number of MUs and a sequential FC scheme in which ℓ is a random variable, sufficient measurements are sent to FC from all users, and a double threshold determines the decision made at FC. The work mainly considers the effect of both schemes in the overhead in the system. The study also includes analyzing the effect of the number of malicious and their probability of attacking, as well as the number of measurements, on FC detection.

1.2 Literature Review

Many efforts have gone into developing the SS of the CR system. Many papers have been written about detecting spectrum holes by distinguishing the PU signal from the noise signal. In [17], discrete wavelet transform (DWT) techniques are used to identify spectrum holes in a wide-band power spectrum. In [18], the continuous wavelet transform (CET) and DWT are proposed for edge detection on wide-band SS. The authors of [19] devised a wavelet strategy for SS in CR and compared various wavelet transform algorithms to highlight the significance of choosing the appropriate wavelet schemes. The authors of [20] suggested a higher order moment-based adaptive SS approach and compared it to a multilevel threshold for the decision stage. The discrete cosine transform (DCT) was used by the authors of [21] to create a novel energy-based SS technique rather than the discrete fourier transform

(DFT). However, this approach disregards the relationship between noise extraction and DCT coefficients.

The variation of collected energy in the first and final sub-bands of one-level DWT decomposition is used to identify the PU embedded in noise in [22]. The nature of the first sub-band in the DWT is that it has the highest signal energy (information), as opposed to a noise signal. As a result, each sub-band is approximately gathering the same level of energy.

The most popular detection technique in CSS is still energy detection [23]. This is due to the fact that the diversity benefit of collaboration might somewhat offset the performance degradation caused by noise uncertainty. The detection performance of an ED used for CSS in a CR network is examined over channels with both multipath fading and shadowing. CSS in a frequency-selective fading environment is suggested in [24] and is based on Welch periodogram research. The study concentrated on the detection of orthogonal frequency division multiplexing (OFDM) signals. The impact of the frequency-selective channel was investigated for both single-carrier and multi-carrier transmissions. In [25], a lot of work is done on signal detection utilizing the ideal ED.

The best local threshold should be chosen in order to identify the PU [26]. Double threshold energy detection and choosing the optimal threshold. have been researched in this area. In order to lessen communication traffic, a sensing technique utilizing a double threshold for energy detection was suggested in [26]. Under the assumption that the ED has two threshold values, this technique is used to enhance the macro detection capabilities of CR networks. In [27], the optimal energy level in the fuzzy zone-a region between the low and high energy thresholds-was found using the Bi-Section technique. The Bisection function for cognitive users was used to set the decision threshold for this situation. The proposed approach performs better in terms of detection performance than traditional double-threshold energy-sensing schemes, but it does not account for MUs. The authors of [28] proposed a sensing approach that does not account for MUs and is based on a statistical parameter that represents the ratio between variance and mean energy values as an indicator of whether the received signal is a PU or simply noise.

Attackers will make a defective decision regarding the use of the spectrum during the collaborative SS decision-making process by injecting fabricated observations. More importantly, by interfering with the CSS's normal operation, MUs can unlawfully occupy spectrum bandwidth. As a result, [29], [30], and [31] introduce reputation-based approaches for combating untruthful SUs in a CR Network. In this instance, the MU will be recognized and given the option of being removed from the group or having his local decision discarded. For example, a recurrent neural network boundary detection technique is utilized in [32] to estimate the location of SUs. In order to order them to discard all SUs with the least order because they might be a MU, the Malicious User Detection by Ordering (MUDO) methodology is used. According to [29], a secure CSS method is created to fend off SSDF attacks based on reputation mechanisms, and the beta reputation model is used to assign reputation values to cognitive sensor nodes in accordance with their historical sensing behavior as a method of attacker identification. Using hierarchical clustering architecture, a reputation-based CSS scheme was proposed in [30], which successfully reduced the impact of multipath fading, shadow, and malicious attack by using the two-level reputation estimation. The authors of [42] proposed a sensing approach based on a statistical parameter (that takes into account MUs) as an indicator of whether the received signal is a PU or simply noise. But it’s a soft decision and depending on Rayleigh fading channel and the signals are complex Gaussian not real.

Here, this thesis makes use of the robust CV tool to increase the detection probability by considering the SNR, which is not just one value and in which the percentage of MUs varies from 1-100% of all SUs. The FC makes a decision at the global level based on the hard binary decisions received from all SUs in order to restrict a user's inappropriate behavior in the CR network and avoid privacy violations [33], [34]. Basically, the value of this research is assessed in light of its findings.

In order to achieve the goals of the study, the following working scenario was used to achieve the study's objectives:

1. A fixed FC scheme (which is simple for various system scenarios) for PU detection (PUD) based on a single threshold is performed using a fixed number of MUs (N_m).

2. Analyzing the impact of the number of malicious and their probability of attacking, as well as the number of measurements, on FC detection is another aspect of the study. The analysis of the algorithm was carried out using MATLAB.

3. A sequential FC scheme in which ℓ is a random variable, sufficient measurements are sent to FC from all users, and a double threshold determines the decision made at FC.

1.3 *Thesis Outline*

The remainder of this thesis is organized into the following four chapters: The model, performance metrics, the concept of local detection, ED principles, the analysis of FC global decisions using fixed and sequential proposed algorithms, the explanation of the closed form expression for CV, and the majority rule principle are all introduced in Chapter 2. The next chapter, Chapter 3, introduces the simulation results of the system that was carried out using MATLAB. The two proposed algorithms (the sequential technique and the fixed method), the majority rule, and the analytical and numerical forms for the CV are all examined in this chapter. Additionally, it illustrates and analyzes how changing the SNR, number of malicious, and attacking probability affects the CV values and error probability. Chapter 4 concludes and highlights the accomplishments of this thesis, emphasizing its importance.

Chapter 2

Models and Performance Metrics

2.1 System Description

We consider $\mathrm{N_u}$ is the number of SU sensors; some are MU sensors and others are legitimate user sensors. Each sends a hard decision to FC, who makes the final decision of whether or not PU is present. Each SU senses the spectrum to determine if the PU signal (S) present or not. S is the PU signal, which is a Gaussian process randomly received by each sensor and has different values for zero mean and variance $\sigma^2{}_s$. Then the w(t) is added which is zero mean and variance $\sigma^2{}_w$. X(t) which is the signal detected for each sensor makes sensing over a specific time interval and taking T samples is entered into the ED to compare with the threshold λ. Following that, the local hard decision ($\hat{Z}$) is sent to FC so that it can make a decision based on the forwarding times (ℓ). This global decision is determined based on the estimated mean, variance values at each attacking probability and SNR values.

For this thesis, we have two models:

- For single threshold: the ℓ is fixed and equal to the total number of measurements sent to FC by all users.
- For double threshold: the ℓ is random variable that equals the enough number of measurements that all users have sent to FC.

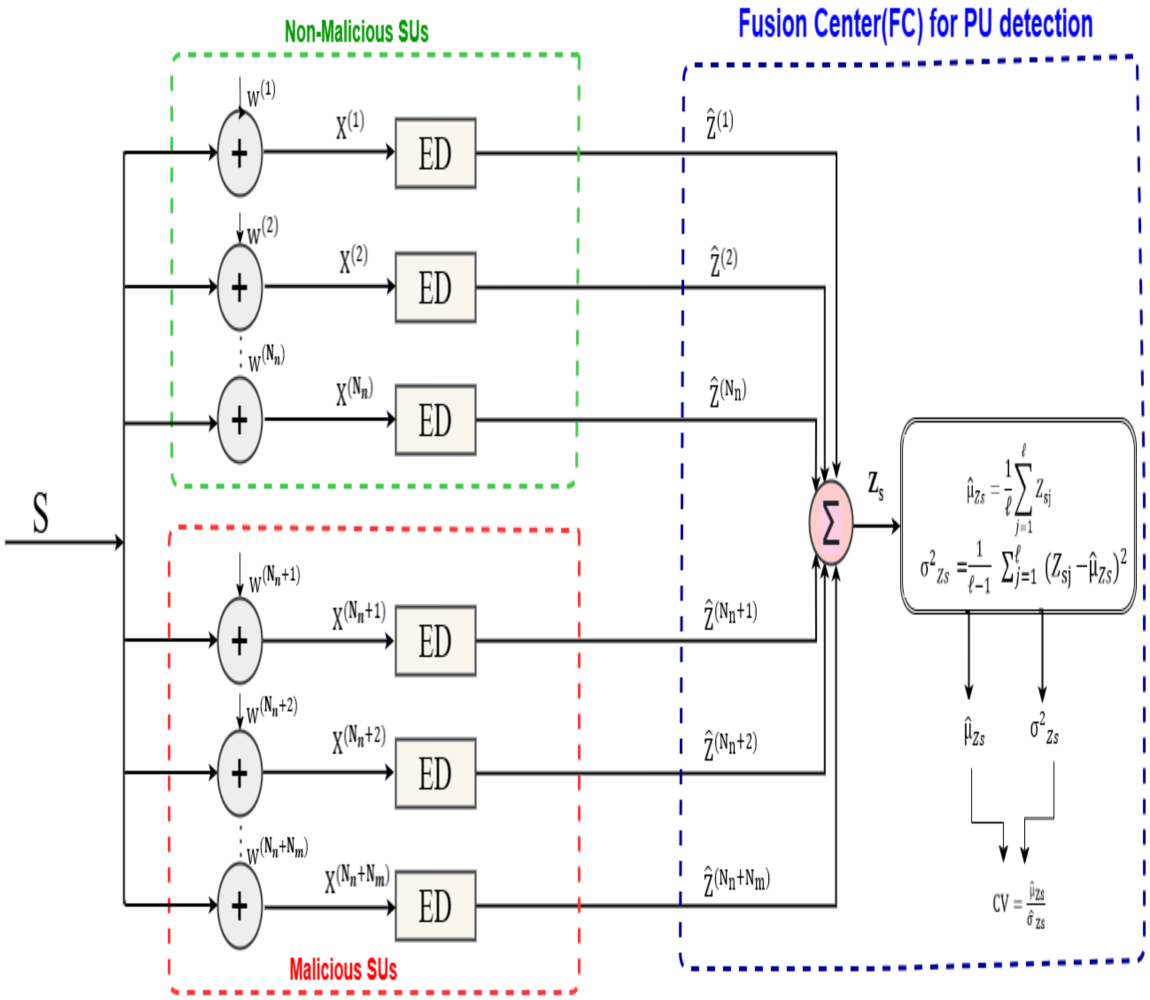


Fig.2-1: System Description

2.2 System Model

In CR networks, SS is a crucial component that enables SU to identify unutilized spectrums that belong to the primary system and to significantly utilize unutilized frequency bands without interfering with primary systems [38].

Through the sensing channel, all cognitive sensor nodes will detect the PU's signal, and then they will report their local decisions to the FC. The legitimate sensor nodes in the SS process share actual energy levels, while the malicious sensor nodes provide the FC their fabricated sensing data for final combining.

2.2.1 *Binary Hypothesis Testing Problem*

Signal detection at the SU can be modeled as a Binary Hypothesis Testing Problem, given as:

Hypothesis 0 (H_0): PU signal is absent

Hypothesis 1 (H_1): PU signal is present

Based on binary hypotheses, the spectrum sensing for a specific frequency band can be generally formulated by:

$$X(t) = \begin{cases} w(t)\,, & H_0 \\ S(t) + w(t), & H_1 \end{cases} \quad \text{, where } t = 1, 2, 3 \ldots\ldots\text{ T} \qquad (1)$$

where S(t) and w(t) are zero-mean, Gaussian-distributed random variables with variances $\sigma^2{}_s$ and $\sigma^2{}_w$, that is, S(t)~N (0,$\sigma^2{}_s$) and $w(t)$~N (0, $\sigma^2{}_w$), representing the PU signal and the additive white Gaussian noise (AWGN), respectively, as a detecting signal for the SUs. The variance $\sigma^2{}_s$ of PU signal being independent of the $w(t)$ variance $\sigma^2{}_w$. We assumed that variances are identical for all t =1, 2, 3...T. where T is the total number of samples.

The SNR in the system is calculated by equation SNR= $\frac{\sigma^2{}_s}{\sigma^2{}_w}$.

2.2.2 Test Statistic for Local Detection

For the detection of the signal at each one of SUs, ED is implemented for detection in SS. Collect the test statistic and compare it to a threshold γ to decide whether the PU exists. The test statistic Y of any sensor node for T samples (T is the number of measurements that enter to each SUs sensor to make its own local decision) is calculated by:

$\mathrm{X(t)}$ is a vector of T measurements such that:

$$\mathrm{X(t)} = \mathrm{X_t} = [\mathrm{X_1}, \mathrm{X_2}, \mathrm{X_3} \dots \dots ., \mathrm{X_T}] \tag{2}$$

Under $\mathrm{H_0}$: X~N (0, $\sigma^2{}_w$)

Under $\mathrm{H_1}$: X~N (0, $\sigma^2{}_s + \sigma^2{}_w$)

From equation(2), the symbol $\mathrm{X(t)}$ will replace with $\mathrm{X_t}$for simplicity.

$$\mathrm{Y} = \sum_{t=1}^{T} (\mathrm{X_t})^2 \tag{3}$$

The distribution of Y is chi square distribution which approximated as Gaussian by virtue of the central limit theorem (CLT) [39]. So, we can find the mean and variance of Y as follow:

$$\mu_Y = E\left[\sum_{t=1}^{T} {X_t}^2\right] = E[{X_1}^2 + {X_2}^2 + \cdots .. {X_T}^2] = T^* \, \sigma^2{}_X \tag{4}$$

$$\sigma_Y{}^2 = \text{var}\,(\textstyle\sum_{t=1}^{T} {X_t}^2) = E\left[{X_t}^2 - \mu_{X_t}{}^2\right]^2 = 2T\sigma^4{}_X \tag{5}$$

a) Under H_0 :

$X \sim N\,(0, \sigma^2{}_w)$

$$Y = \sum_{t=1}^{T} X_t^2 \;\sim\; \chi_T{}^2 = \Gamma\,(\tfrac{T}{2}, 2) \tag{6}$$

The chi-squared distribution is a special case of the gamma distribution. Then the mean and variance Under H_0 are as follow compared with equations (4) and (5).

$$\mu_{Y/H_0} = T\,{}^*\sigma^2{}_w \tag{7}$$

$$\sigma^2{}_{Y/H_0} = 2^*\, T\,{}^*\sigma^2{}_w \tag{8}$$

The variance $\sigma^2{}_s$ being independent of $\sigma^2{}_w$. We assumed that variances are identical for all t =1, 2, 3...T. where T is the total number of samples. Also, under H_0 we have only the noise so the equation (5) be as above.

b) <u>Under H_1 :</u>

$X \sim N\ (0, \sigma^2{}_s + \sigma^2{}_w)$

$$Y = \sum_{t=1}^{T} (w(t) + S(t))^2 \tag{9}$$

$$\text{Then: } \sum_{t=1}^{T} X_t^2 \sim \Gamma\left(\frac{T}{2}, 2*(\sigma^2{}_s + \sigma^2{}_w)\right) \tag{10}$$

Then the mean and variance under H_1 are as follow compared with equations (4) and (5).

$$\mu_{Y/H_1} = T*(\sigma^2{}_s + \sigma^2{}_w) \tag{11}$$

$$\sigma^2{}_{Y/H_1} = 2*T*\ (\sigma^2{}_s + \sigma^2{}_w)^2 \tag{12}$$

Y follows the Chi- square distribution. If the number of samples T is large, with the central limit theorem (CLT), we can assume that the Chi-square distribution is approximate as Gaussian distribution [39].

The classical Neyman-Pearson (NP) approach [40] for hypothesis testing defines the test statistic as likelihood ratio test (LRT) which is found based on the approximation of the statics' given by:

$$\frac{f(Y/H_1)}{f(Y/H_0)} \quad \overset{>^{H_1}}{<_{H_0}} \quad \gamma \qquad (13)$$

Where Y is the test statistic given in equation (3), γ is the threshold.

$$\frac{\frac{1}{\sqrt{2\pi\sigma^2{}_{Y/H_1}}}\; e^{\frac{-\left(Y-\mu_{Y/H_1}\right)^2}{2\sigma^2{}_{Y/H_1}}}}{\frac{1}{\sqrt{2\pi\sigma^2{}_{Y/H_0}}}\; e^{\frac{-\left(Y-\mu_{Y/H_0}\right)^2}{2\sigma^2{}_{Y/H_0}}}} \quad \overset{>^{H_1}}{<_{H_0}} \gamma \qquad (14)$$

$$\frac{\sigma_{Y/H_0}}{\sigma_{Y/H_1}} \; \frac{e^{\frac{-\left(Y-\mu_{Y/H_1}\right)^2}{2\sigma^2{}_{Y/H_1}}}}{e^{\frac{-\left(Y-\mu_{Y/H_0}\right)^2}{2\sigma^2{}_{Y/H_0}}}} \quad \overset{>^{H_1}}{<_{H_0}} \gamma \qquad (15)$$

$$\frac{\left(Y-\mu_{Y/H_0}\right)^2}{2\sigma^2{}_{Y/H_0}{}^2} - \frac{\left(Y-\mu_{Y/H_1}\right)^2}{2\sigma^2{}_{Y/H_1}} \quad \overset{>^{H_1}}{<_{H_0}} \quad \ln\left(\gamma\frac{\sigma_{Y/H_1}}{\sigma_{Y/H_0}}\right) \qquad (16)$$

$$\frac{Y^2-2Y\mu_{Y/H_0}+\mu^2{}_{Y/H_0}}{2\sigma^2{}_{Y/H_0}} - \frac{Y^2-2Y\mu_{Y/H_1}+\mu^2{}_{Y/H_1}}{2\sigma^2{}_{Y/H_1}} \quad \overset{>^{H_1}}{<_{H_0}} \quad \ln\left(\gamma\frac{\sigma_{Y/H_1}}{\sigma_{Y/H_0}}\right) \qquad (17)$$

$$\sigma^2{}_{Y/H_1}\left(Y^2-2Y\mu_{Y/H_0}+\mu^2{}_{Y/H_0}\right)-\sigma^2{}_{Y/H_0}\left(Y^2-2Y\mu_{Y/H_1}+\mu^2{}_{Y/H_1}\right) \overset{>^{H_1}}{<_{H_0}} \quad \ln\left(\gamma\frac{\sigma_{Y/H_1}}{\sigma_{Y/H_0}}\right)2\sigma^2{}_{Y/H_1}\,\sigma^2{}_{Y/H_0} \qquad (18)$$

$$Y^2(\sigma^2{}_{Y/H_1} - \sigma^2{}_{Y/H_0}) - 2Y[\mu_{Y/H_0}\sigma^2{}_{Y/H_1} - \mu_{Y/H_1}\sigma^2{}_{Y/H_0}] + \mu^2{}_{Y/H_0}\sigma^2{}_{Y/H_1} - \mu^2{}_{Y/H_1}\sigma^2{}_{Y/H_0}) \underset{H_0}{\overset{H_1}{\gtrless}} \ln\left(\gamma\frac{\sigma_{Y/H_1}}{\sigma_{Y/H_0}}\right) 2\,\sigma^2{}_{Y/H_1}\,\sigma^2{}_{Y/H_0} \tag{19}$$

$$\text{Let: } a=\sigma^2{}_{Y/H_1} - \sigma^2{}_{Y/H_0} \tag{20}$$

$$b=\mu_{Y/H_0}\sigma^2{}_{Y/H_1} - \mu_{Y/H_1}\sigma^2{}_{Y/H_0} \tag{21}$$

$$c= (\mu^2{}_{Y/H_0}\sigma^2{}_{Y/H_1} - \mu^2{}_{Y/H_1}\sigma^2{}_{Y/H_0}) - \ln\left(\gamma\frac{\sigma_{Y/H_1}}{\sigma_{Y/H_0}}\right) 2\sigma^2{}_{Y/H_1}\,\sigma^2{}_{Y/H_0} \tag{22}$$

$$aY^2 - 2Yb + c \quad \underset{H_0}{\overset{H_1}{\gtrless}} \quad 0 \tag{23}$$

$$Y^2 - \frac{2b}{a}Y + \frac{c}{a} \quad \underset{H_0}{\overset{H_1}{\gtrless}} \quad 0 \tag{24}$$

By complete square: add and subtract $\frac{b^2}{a^2}$

$$\left(Y - \frac{b}{a}\right)^2 \underset{H_0}{\overset{H_1}{\gtrless}} \frac{b^2}{a^2} - \frac{c}{a} \tag{25}$$

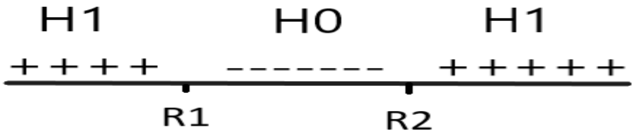
$$|\,Y - \frac{b}{a}\,| \underset{H_0}{\overset{H_1}{\gtrless}} \pm\sqrt{\max(\,0\,, \frac{b^2}{a^2} - \frac{c}{a}\,)} \tag{26}$$

I take the maximum to make sure that answer is positive or zero if negative.

The roots are:

$$R1 = \frac{b}{a} - \sqrt{\max\left(0, \frac{b^2}{a^2} - \frac{c}{a}\right)} \quad , \quad R2 = \frac{b}{a} + \sqrt{\max(0, \frac{b^2}{a^2} - \frac{c}{a})}$$

There are 3 regions as follow with the sign in each region:



The performance of energy detector is characterized by using following metrics, which have been introduced based on the test statistic under the binary hypothesis:

- False alarm probability (P_{fa}): the probability of deciding the signal is present while H_0 is true.
- Missed-detection probability (P_{md}): the probability of deciding the signal is absent while H_1 is true.
- Detection probability (P_d): the probability of deciding the signal is present when H_1 is true.

1- <u>Under H_0:</u>

The false alarm probability can be given as:

$P_{fa} = \mathrm{pr}(Y < R1 \text{ or } Y > R2)\ /H_0)$. Consider the IEEE 802.22 wireless regional area network, which is one of the most common CR standards for accessing unused licensed frequencies in the TV band; according to this standard, the false-alarm probability of CR should be 0.1 and the P_d must be ≥ 0.9 [41]. Further, the detection and false-alarm probabilities are greatly affected by the selected threshold value in the SS approach and selection of the threshold is a crucial step to yield the status (presence or absence) of PU [41].

$$P_{fa} = \int_{-\infty}^{R1} \frac{1}{\sqrt{2\pi\sigma^2{}_{Y/H_0}}} \quad e^{\frac{-\left(Y-\mu_{Y/H_0}\right)^2}{2\sigma^2{}_{Y/H_0}}} dY + \int_{R2}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2{}_{Y/H_0}}} \quad e^{\frac{-\left(Y-\mu_{Y/H_0}\right)^2}{2\,\sigma^2{}_{Y/H_0}}} dY \qquad (27)$$

$$P_{fa} = 1 - Q\left(\frac{R1-\mu_{Y/H_0}}{\sigma_{Y/H_0}}\right) + Q\left(\frac{R2-\mu_{Y/H_0}}{\sigma_{Y/H_0}}\right) \qquad (28)$$

where $Q(u)=\frac{1}{\sqrt{2\pi}}\int_u^{\infty} e^{\frac{-(u)^2}{2}} du$ is the Gaussian-Q function.

2- **Under H_1 :**

The detection probability, P_d can be derived as:

$$P_d = pr((Y < R1 \text{ or } Y > R2)/H_1) = \int_{-\infty}^{R1} \frac{1}{\sqrt{2\pi\sigma^2{}_{Y/H_1}}} e^{\frac{-\left(Y-\mu_{Y/H_1}\right)^2}{2\sigma^2{}_{Y/H_1}}} dY + \int_{R2}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2{}_{Y/H_1}}} e^{\frac{-\left(Y-\mu_{Y/H_1}\right)^2}{2\,\sigma^2{}_{Y/H_1}}} dY \qquad (29)$$

$$= 1 - \int_{R1}^{R2} \frac{1}{\sqrt{2\pi\sigma^2{}_{Y/H_1}}} e^{\frac{-\left(Y-\mu_{Y/H_1}\right)^2}{2\sigma^2{}_{Y/H_1}}} dY \qquad (30)$$

$$= Q\left(\frac{R2-\mu_{Y/H_1}}{\sigma_{Y/H_1}}\right) - Q\left(\frac{R1-\mu_{Y/H_1}}{\sigma_{Y/H_1}}\right) \qquad (31)$$

$$P_d = 1- \left[Q\left(\frac{R1-\mu_{Y/H_1}}{\sigma_{Y/H_1}}\right) - Q\left(\frac{R2-\mu_{Y/H_1}}{\sigma_{Y/H_1}}\right) \right] \qquad (32)$$

It’s appeared that the P_{fa} depends only on the mean, variance of Y under H_0 which means dependency on $\sigma^2{}_w$. But the P_d depends on the $\sigma^2{}_s , \sigma^2{}_w$.

As a result, the n-th SU local decision is:

$$\hat{Z} = \begin{cases} 0, & R1 < Y < R2 \\ 1, & Y < R1 \text{ or } Y > R2 \end{cases} \qquad (33)$$

2.2.3 Secondary User Signal Processing at Output of Energy Detector:

The sensor node takes part in CSS and transmits to FC, for a subsequent global fusion decision, the local outcome, which is 0 or 1, indicating that the channel is idle and occupied.

We consider a N_u number of SUs sensors. Among them, the legitimate user (LU) nodes share the real energy values in the SS process, but the MU nodes send their falsified sensing data to the FC which need to decide the final state of PU.

As $N_u = N_m + N_n$.Then, SUs are two types:

a) MU which is present as N_m of the total number N_u, and the exact number of MU is not important for FC as it must be robust to decide.

b) LUs number is N_n.

The main attack steps used by MUs are as follows:

(1) All malicious nodes begin spectrum sensing with the same local spectrum sensing as normal nodes and also make their own local sensing decisions.

(2) With a probability of α, each malicious node independently chooses whether to attack or not.

(3) The malicious node will send reporting that conflicts with the local sensing data to the FC if it decides to launch an attack. If not, the malicious node simply reports the actual local sensing data instead of launching an attack.

(4) On the basis of malicious and non-malicious nodes sharing their local sensing results, the FC decides in CSS that the primary user does not exist, or the global decision indicates that the primary user exists.

The following flow chart shows the Bayes theorem tree of the system under H_0, H_1:

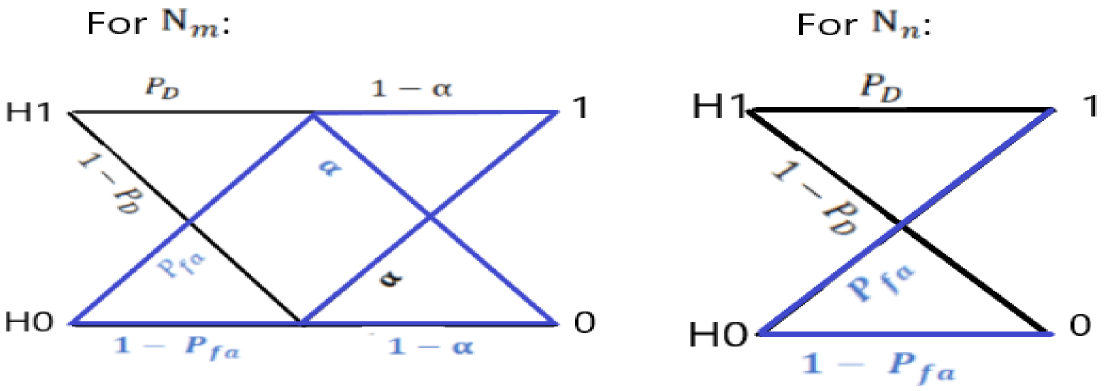


Fig.2 -2: Flow Chart of Decision Tree for MUs, LUs.

In this study, the MU is of the ROMU type, and it attacks with a probability of α. After the attack is determined, the MU node provides the FC with a report that conflicts with the local sensing results. Generally, each SU will send a value of 0 or 1 with the following probabilities to the FC:

$$\hat{\mathbf{Z}}_{\mathrm{MU}} = \begin{cases} 0, & (1-\alpha)(1-\mathrm{p}_1) + \mathrm{p}_1\alpha \\ 1, & \alpha(1-\mathrm{p}_1) + \mathrm{p}_1(1-\alpha) \end{cases} \tag{34}$$

$$\hat{\mathbf{Z}}_{\mathrm{LU}} = \begin{cases} 0, & 1-\mathrm{p}_1 \\ 1, & \mathrm{p}_1 \end{cases} \tag{35}$$

Based on Fig.2-2: p1= $\mathrm{P_{fa}}$ under $\mathrm{H_0}$ and $\mathrm{p1} = \mathrm{P_d}$ under $\mathrm{H_1}$.

The detection probability and false alarm probability of MUs can be written as:

$$\begin{cases} \mathrm{P_{fa_{MU}}} = \mathrm{p}\big(\hat{\mathrm{Z}} = 1\,/\mathrm{H_0}\big) = \alpha(1-\mathrm{P_{fa}}) + \mathrm{P_{fa}}(1-\alpha) \\ \mathrm{P_{d_{MU}}} = \mathrm{p}\big(\hat{\mathrm{Z}} = 1\,/\mathrm{H_1}\big) = \alpha(1-\mathrm{P_d}) + \mathrm{P_d}(1-\alpha) \end{cases} \tag{36}$$

Each LU will send a hard decision over the channel which is assumed to be a perfect channel (error-free) for simplicity. Also, the MUs make a hard decision to transmit it to FC.

The detection probability and false alarm probability of LU nodes can be written as:

$$\begin{cases} \mathrm{P_{fa_{LU}}} = \mathrm{p}\big(\hat{\mathrm{Z}} = 1\,/\mathrm{H_0}\big) = \mathrm{P_{fa}} \\ \mathrm{P_{d_{LU}}} = \mathrm{p}\big(\hat{\mathrm{Z}} = 1\,/\mathrm{H_1}\big) = \mathrm{P_d} \end{cases} \tag{37}$$

where $\mathrm{P_d}$ and $\mathrm{P_{fa}}$ represent the local detection probability and false alarm probability of the sensing node.

2.2.4 Fusion Center for Primary User Detection

The FC fuses the received local binary decisions and makes the global decision about the authorized spectrum according to:

$$\mathrm{Z_s} = \sum_{\mathrm{K}=1}^{\mathrm{N_u}} (\hat{\mathrm{Z}})^{(\mathrm{K})} \tag{38}$$

Depending on the measurements that each SU sends to FC, the FC makes decision depending on the CV tool which estimate the mean, variance for $\hat{Z}$ = [1,0] using sample mean and sample variance estimators. The number of measurements or the forwarding times ℓ is required for FC to be able make decision such that:

$$\mathrm{Z_{sj}} = \begin{bmatrix} \mathrm{Z_{s_1}} \\ \mathrm{Z_{s_2}} \\ \vdots \\ \mathrm{Z_{s_\ell}} \end{bmatrix} \tag{39}$$

where: $\mathrm{Z_{s_1}} = [\ \hat{\mathrm{Z}}^{(1)}{}_1\ ,\ \hat{\mathrm{Z}}^{(2)}{}_1\ ,\ \dots\dots\dots\ ,\ \hat{\mathrm{Z}}^{(\mathrm{N_u})}{}_1\ ]$ the first locally decisions sending from all SUs to FC.

Upon reception of the $\mathrm{Z_{sj}}$ $(\ell \times (\mathrm{N_m}+\mathrm{N_n}))$ - dimensional frame matrix signal. Each row in matrix represents one sending to FC from all SUs. Depending on it, the FC find the following:

The sample mean $\hat{\mu}_{Zs}$ is an estimate of the population mean μ. Given a sample of size ℓ, consider ℓ independent random variables Z_{s_1}, Z_{s_2}, ..., Z_{s_ℓ} ,each corresponding to one randomly selected observation.

Here, first by finding the saparse summation of the hard decision from all SUs, then the temporal summation will be found to have a $\ell \times N_u$ total number of measurements and find the mean and variance based on it.

The sample mean of Z_s is defined to be :

$$\hat{\mu}_{Zs} = \frac{1}{\ell N_u} \sum_{j=1}^{\ell} Z_{sj} = \frac{1}{\ell} \sum_{j=1}^{\ell} \sum_{K=1}^{N_u} \left(\hat{Z}\right)^{(K)} \tag{40}$$

The sample variance of Z_s is:

$$\hat{\sigma}_{Zs}^{\ 2} = \frac{1}{\ell N_u - 1} \sum_{j=1}^{\ell} \left(\sum_{K=1}^{N_u} \left(\hat{Z}\right)^{(K)} - \hat{\mu}_{Zs}\right)^2 \text{ for } \ell \geq 2. \tag{41}$$

$$\mathrm{CV} = \frac{\hat{\mu}_{Zs}}{\hat{\sigma}_{Zs}} \tag{42}$$

2.2.4.1 Fusion Center Detection Using Fixed Measurements Method

For the detection of the signal at FC, collect the test statistic of the fixed number of measurements ℓ sent to FC and compare it to a threshold η to decide whether the PU exists. The test statistic at FC is calculated by:

$$\mathrm{CV} = \frac{\hat{\mu}_{\mathrm{Zs}}}{\hat{\sigma}_{\mathrm{Zs}}} \quad \overset{\mathrm{H1}}{\underset{\mathrm{H0}}{\gtrless}} \quad \eta \tag{43}$$

The maximum CV under H0 and the minimum CV under H1 were used to determine η. In this case, η represents the average value of the gap between the $\mathrm{CV}_{\mathrm{H0}}$ and $\mathrm{CV}_{\mathrm{H1}}$.

$$\eta = \mathrm{CV}_{\mathrm{H0}} + \frac{\mathrm{CV}_{\mathrm{H1}} - \mathrm{CV}_{\mathrm{H0}}}{2} \tag{44}$$

If CV > η, it means the PU is present, and we get 1 detection.

If CV < η, it means the PU is absent, and we get 0 detection. (We ignore the possibility of CV = η).

The detection probability and false alarm probability of the FC can be written as:

$$\begin{cases} \mathrm{P}_{\mathrm{FA}_{\mathrm{FC}}} = \mathrm{p}(\mathrm{CV} > \eta \ / \ \mathrm{H}_0) \\ \mathrm{P}_{\mathrm{D}_{\mathrm{FC}}} = \mathrm{p}(\mathrm{CV} > \eta \ / \mathrm{H}_1) \end{cases} \tag{45}$$

Based on the equation (43). In SS, the error probability at FC is calculated as follows:

$$\mathrm{P_{error}} = \mathrm{Pi}_{\,0} * (\mathrm{P_{FA_{FC}}}) + (\mathrm{Pi}_{\,1}) * (1 - \mathrm{P_{D_{FC}}}) \qquad (46)$$

Where $\mathrm{Pi}_{\,0} = \mathrm{pr}(\mathrm{H}_0), \mathrm{Pi}_{\,1} = \mathrm{pr}(\mathrm{H}_1)$

2.2.4.2: Closed Form Expression for the CV

In this section, the closed form of the CV calculation is explained as follows:

$$\mathrm{Z_s} = \sum_{\mathrm{K}=1}^{\mathrm{N_u}} \left(\hat{\mathrm{Z}}\right)^{(\mathrm{K})} \qquad (47)$$

$$= \sum_{\mathrm{K}=1}^{\mathbf{N_m}} \left(\hat{\mathrm{Z}}\right)^{(\mathrm{K})} + \sum_{\mathrm{K}=1}^{\mathbf{N_n}} \left(\hat{\mathrm{Z}}\right)^{(\mathrm{K})} \qquad (48)$$

As $\left(\hat{\mathrm{Z}}\right)^{(\mathrm{K})}$ is a hard decision that LUs and MUs send to FC. It therefore follows to the Bernoulli distribution.

The mean at FC:

$\hat{\mathbf{Z}}$ follow Bernoulli distribution so:

$$\text{Mean}_{Z_s} = \mathrm{E}\,[Z_s] = \mathrm{E}\left[\ \sum_{K=1}^{\mathbf{N_m}} \left(\hat{Z}\right)^{(K)} + \sum_{K=1}^{\mathbf{N_n}} \left(\hat{Z}\right)^{(K)}\right] \tag{49}$$

$$= \mathrm{E}\left[\ \sum_{K=1}^{\mathbf{N_m}} \left(\hat{Z}\right)^{(K)}\right] + \mathrm{E}\left[\ \sum_{K=1}^{\mathbf{N_n}} \left(\hat{Z}\right)^{(K)}\right] \tag{50}$$

$$= \sum_{K=1}^{\mathbf{N_m}} \mathrm{E}\,[\ \left(\hat{Z}\right)^{(K)}] + \sum_{K=1}^{\mathbf{N_n}} \mathrm{E}\,[\ \left(\hat{Z}\right)^{(K)}] \tag{51}$$

$$= \sum_{K=1}^{\mathbf{N_m}} (1 - p_1)\alpha + p_1(1 - \alpha) \quad + \sum_{K=1}^{\mathbf{N_n}} p_1 \tag{52}$$

To find the means and variances at FC under H_0 and H_1, the value of p_1 in the equation(52) will be substituted as follow:

As the number of malicious is changeable and the P_{fa} is the same for all SUs and has a constant value, the summation in the equation(53) can be expressed as:

1- **Under H_0:** $p_1 = P_{fa}$

As the number of malicious is changeable and the P_{fa} is the same for all SUs and has a constant value, the summation in the equation(52) can be expressed as:

$$\text{Mean}_{{z_s}_{H0}} = N_m((1 - P_{fa})\alpha + P_{fa}(1-\alpha)) + N_n P_{fa} \qquad (53)$$

2- Under H_1 : $p_1 = P_d$

$$\text{Mean}_{{z_s}_{H1}} = N_m((1 - P_d)\alpha + P_d(1-\alpha)) + N_n P_d \qquad (54)$$

The variance at FC:

As $\sum_{K=1}^{\mathbf{N_m}} (\hat{Z})^{(K)}$, $\sum_{K=1}^{\mathbf{N_n}} (\hat{Z})^{(K)}$ are independent, hence the variance is the sum of two variances.

$$\text{Variance}_{z_s} = \text{var}(\sum_{K=1}^{\mathbf{N_m}} (\hat{Z})^{(K)}) + \text{var}(\sum_{K=1}^{\mathbf{N_n}} (\hat{Z})^{(K)}) \qquad (55)$$

$$\text{var}(\sum_{K=1}^{\mathbf{N_m}} (\hat{Z})^{(K)}) = \sum_{K=1}^{\mathbf{N_m}}[(1-\alpha)(1-p_1) + p_1\alpha][(1-p_1)\alpha + p_1(1-\alpha)] \quad (56)$$

$$= \alpha + p_1 - 4p_1\alpha + 4\alpha {p_1}^2 \; - \; {p_1}^2 - \alpha^2 \; + \; 4p_1\alpha^2 - \; 4{p_1}^2\alpha^2$$

$$\mathrm{var}(\; \sum_{K=1}^{\mathbf{N_n}} \; \left(\hat{Z}\right)^{(K)}) = \; \sum_{k=1}^{\mathbf{N_n}} [(1 - p_1)p_1 \,] \qquad (57)$$

$$\text{Variance}_{\,Z_s} \; = \; \sum_{K=1}^{\mathbf{N_m}} [(1-\alpha)(1-p_1) + p_1\alpha \,][(1-p_1)\alpha \; + p_1(1-\alpha)]$$

$$+ \; \sum_{k=1}^{\mathbf{N_n}} [(1 - p_1)p_1 \,] \qquad (58)$$

1- Under H_0:

$$\text{Variance}_{\,{Z_s}_{H0}} = \quad \sum_{K=1}^{\mathbf{N_m}} [(1-\alpha)(1- \; P_{fa}) + P_{fa}\alpha \,][(1- \; P_{fa})\alpha + P_{fa}(1-\alpha)] +$$

$$\sum_{k=1}^{\mathbf{N_n}} [(1- \; P_{fa}) \, P_{fa} \,] \qquad (59)$$

2- Under H_1:

$$\text{Variance}_{\,{Z_s}_{H1}} = \quad \sum_{K=1}^{\mathbf{N_m}} [(1-\alpha)(1- \; P_d) + \; P_d\alpha \,][(1- \; P_d)\alpha \; + \; P_d(1-\alpha)] +$$

$$\sum_{k=1}^{\mathbf{N_n}} [(1- \; P_d) \, P_d \,] \qquad (60)$$

The CV at FC:

$$\mathrm{CV} = \frac{\mathrm{Mean}\ z_s}{\sqrt{\mathrm{Variance}\ z_s}} = \frac{\sum_{K=1}^{\mathbf{N_m}}(1-p_1)\alpha + p_1(1-\alpha) \ + \sum_{k=1}^{\mathbf{N_n}} p_1}{\sqrt{\sum_{K=1}^{\mathbf{N_m}}[(1-\alpha)(1-p_1)+p_1\alpha\,][(1-p_1)\alpha + p_1(1-\alpha)] + \sum_{k=1}^{\mathbf{N_n}}[(1-p_1)p_1\,]}} \tag{61}$$

1- **Under H_0:**

$$\mathrm{CV}_{\mathrm{H0}} = \frac{\mathrm{Mean}\ z_{s_{\mathrm{H0}}}}{\sqrt{\mathrm{Variance}\ z_{s_{\mathrm{H0}}}}}$$

$$= \frac{\sum_{K=1}^{\mathbf{N_m}}(1-\mathrm{P_{fa}})\alpha + \mathrm{P_{fa}}(1-\alpha) \ + \sum_{k=1}^{\mathbf{N_n}} \mathrm{P_{fa}}}{\sqrt{\sum_{K=1}^{\mathbf{N_m}}[(1-\alpha)(1-\mathrm{P_{fa}})+\mathrm{P_{fa}}\alpha\,][(1-\mathrm{P_{fa}})\alpha+\mathrm{P_{fa}}(1-\alpha)]+\sum_{k=1}^{\mathbf{N_n}}[(1-\mathrm{P_{fa}})\,\mathrm{P_{fa}}\,]}} \tag{62}$$

2- **Under H_1:**

$$\mathrm{CV}_{\mathrm{H1}} = \frac{\mathrm{Mean}\ z_{s_{\mathrm{H1}}}}{\sqrt{\mathrm{Variance}\ z_{s_{\mathrm{H1}}}}}$$

$$= \frac{\sum_{K=1}^{\mathbf{N_m}}(1-\mathrm{P_d})\alpha + \mathrm{P_d}(1-\alpha) \ + \sum_{k=1}^{\mathbf{N_n}} \mathrm{P_d}}{\sqrt{\sum_{K=1}^{\mathbf{N_m}}[(1-\alpha)(1-\mathrm{P_d})+\mathrm{P_d}\alpha\,][(1-\mathrm{P_d})\alpha + \mathrm{P_d}(1-\alpha)]+\sum_{k=1}^{\mathbf{N_n}}[(1-\mathrm{P_d})\,\mathrm{P_d}\,]}} \tag{63}$$

2.2.4.3: LRT Method (Majority Rule)

Local decisions made by SUs are gathered and forwarded to FC for a final decision denoted as F(x), which can be expressed as follows:

$$F(x)=\begin{cases} H_1 & , \text{ if } Z_s \geq \eta \\ H_0 & , \text{otherwise} \end{cases} \qquad (64)$$

In this case, η is a value between 0 and N_u depends on the number of users, and Z_s is the sum of the local decisions that FC received from all SUs.

Let m represent the percentage of the malicious in the system.

The probability of receiving 1 under H_1 is:

$$P_1=\Pr(\text{receive } 1/H_1) = m(\alpha(1- P_d) + P_d(1-\alpha)) + (1-m)P_d$$

$$= m(\alpha - \alpha P_d + P_d - \alpha P_d) + (1-m)P_d$$

$$= m\alpha - 2m\alpha P_d + mP_d + P_d - mp_d$$

$$= P_d + m\alpha(1-2P_d)$$

$$= 1 - [\alpha m(2P_d - 1) + (1- P_d)] \qquad (65)$$

The probability of receiving 1 under H_0 is:

$$P_0 = \Pr\ (\text{receive } 1/H_0) = 1 - [\ \alpha m(2P_{fa} - 1) + (1 - P_{fa})\ \ ] \tag{66}$$

The MU behaves like the honest one (LU) at low SNR values. As a result, guessing is high since FC is unable to distinguish between illegal and honest users' ones and zeros as the noise is very high in this case.

Here, we want to know the conditions to FC be blind of distinguish between 1,0 under both hypothesis H_1, H_0 at low or high SNR:

1- **0 < m <1** as it is representing the percentage of the malicious.

2- **α** > **0.4** as when α is less than 0.4, the FC will be able to distinguish between 1,0.

$$\Pr\ (\text{receive } 1/H_1) \quad = \quad \Pr\ (\text{receive } 1/H_0)$$

$$1 - [\ \alpha m(2P_d - 1) + (1 - P_d)\ \ ] \quad = \quad 1 - [\ \alpha m(2P_{fa} - 1) + (1 - P_{fa})\ \ ]$$

$$m[\alpha(2P_d - 1) - \alpha(2P_{fa} - 1)\ ] \quad = \quad P_d - P_{fa}$$

$$m = \frac{P_d - P_{fa}}{\alpha(2P_d - 2P_{fa})} \quad = \frac{1}{2\alpha} \tag{67}$$

If $\alpha = 1$, then $m = 0.5$ indicates that 50% of the malicious decisions are sent correctly and 50% are sent falsely, meaning that $P_{error} = 0.5$.

Also, when $m = 1$, $\alpha = 0.5$ then $P_{error} = 0.5$

For explaining the majority rule:

$$Z_s = \sum_{K=1}^{N_u} (\hat{Z})^{(K)} \tag{68}$$

x: is the joint distribution of receiving 1 under H_1 or H_0, which follow Binomial distribution. The probability density function (pdf) of LRT method is:

$$\frac{P(x/H_1)}{P(x/H_0)} \underset{<_{H0}}{\overset{>^{H1}}{}} \gamma \tag{69}$$

$$\frac{\prod_{K=1}^{N_u} (1-P_1)^{1-x} {P_1}^{x}}{\prod_{K=1}^{N_u} (1-P_0)^{1-x} {P_0}^{x}} \underset{<_{H0}}{\overset{>^{H1}}{}} \gamma \tag{70}$$

As m represents the percentage of the malicious in the system.

$P_1 = \Pr\ (\text{receive } 1/H_1) = m(\alpha(1 - P_d) + P_d(1 - \alpha)) + (1 - m) P_d$

$P_0 = \Pr\ (\text{receive } 1/H_0) = m((1 - P_{fa})\alpha + P_{fa}(1 - \alpha)) + (1 - m) P_{fa}$

Here, as all SUs hard decision are independent on each other in numerator and denominator , the multiplication can be simplified as summation.

$$\frac{P_1^{\sum_{K=1}^{N_u} x} \quad (1-P_1)^{\sum_{K=1}^{N_u}(1-x)}}{P_0^{\sum_{K=1}^{N_u} x} \quad (1-P_0)^{\sum_{K=1}^{N_u}(1-x)}} \quad \overset{>^{H1}}{<_{H0}} \quad \gamma$$

$$\frac{P_1^{\sum_{K=1}^{N_u} x} \quad (1-P_1)^{N_u-\sum_{K=1}^{N_u} x}}{P_0^{\sum_{K=1}^{N_u} x} \quad (1-P_0)^{N_u-\sum_{K=1}^{N_u} x}} \quad \overset{>^{H1}}{<_{H0}} \quad \gamma \qquad (71)$$

Let D denote the number of one’s or the number of successes in the vector Z_s so:

$D= \sum_{K=1}^{N_u} x$ which follows the binomial distribution.

$$\frac{P_1{}^{D} \quad (1-P_1)^{N_u-D}}{P_0{}^{D} \quad (1-P_0)^{N_u-D}} \quad \overset{>^{H1}}{<_{H0}} \quad \gamma \qquad (72)$$

$$\left(\frac{1-P_1}{1-P_0}\right)^{N_u} \left(\frac{P_1(1-P_0)}{P_0(1-P_1)}\right)^{D} \quad \overset{>^{H1}}{<_{H0}} \quad \gamma \qquad (73)$$

Taking the natural logarithms of both sides

$$N_u * \ \ln\left(\frac{1-P_1}{1-P_0}\right) * D * \ln\left(\frac{P_1(1-P_0)}{P_0(1-P_1)}\right) \ \underset{<_{H0}}{\overset{>^{H1}}{}} \ \ln(\gamma) \qquad \text{let } \gamma = 1 \qquad (74)$$

$$N_u * \ \ln\left(\frac{1-P_1}{1-P_0}\right) * D * \ln\left(\frac{P_1(1-P_0)}{P_0(1-P_1)}\right) \ \underset{<_{H0}}{\overset{>^{H1}}{}} \ 0 \qquad (75)$$

To find the threshold for the majority rule:

$$\eta = \begin{cases} \frac{N_u+1}{2} & \text{if } N_u \text{ is odd} \\ \frac{N_u}{2} & \text{if } N_u \text{ is even} \end{cases} \qquad (76)$$

as $N_u = 30$ then $\eta = 15$

The detection probability and false alarm probability of the FC can be written as:

$$\begin{cases} P_{FA_{FC}} = p(D > \ \eta \ / \ H_0) \\ P_{D_{FC}} = \ p(D > \ \eta \ \ / H_1) \end{cases} \qquad (77)$$

$$P_{FA_{FC}} = p(D > \ \eta \ / \ H_0) = \sum_{D=15}^{D=30} \binom{30}{D} P_{fa}{}^{D} \ (1 - P_{fa})^{30-D} \qquad (78)$$

$$P_{D_{FC}} = \ p(D > \ \eta \ \ / H_1) \quad = \sum_{D=15}^{D=30} \binom{30}{D} P_d{}^{D} \ (1 - P_d)^{30-D} \qquad (79)$$

Based on the equation (43). In SS, the error probability at FC is calculated as follows:

$$\mathrm{P_{error}} = \mathrm{Pi}_{\,0} * (\mathrm{P_{FA_{FC}}}) + (\mathrm{Pi}_{\,1}) * (1 - \mathrm{P_{D_{FC}}}) \qquad (80)$$

2.2.4.4: Fusion Center Detection Using Sequential Measurements Method

Sequential analysis, also referred to as sequential hypothesis testing, is a type of statistical analysis where the sample size is not fixed. Rather, data are evaluated as they are collected, and further sampling is stopped in accordance with a predetermined stopping rule when significant outcomes are found. This would reduce system overhead because a decision could be made much faster than with conventional hypothesis testing or estimation.

The FC uses the CV tool to generate a global decision based on the decisions Z_s in equation (38) that each SU provides to the FC. The CV tool uses sample mean and sample variance estimators to estimate the mean and variance for $\hat{Z}$= [1,0]. The number of measurements or the forwarding times ℓ are changed for FC to be able to make a decision.

For the same system model in Section 2.1 in which the number of malicious users in the system is specified, and the FC makes detections based on that information. However, the sequential method differs from the fixed method since ℓ, the estimator size random variable, is equal to the sufficient number of measurements sent to FC from all SUs such that $\ell \geq 2$ as the sample variance is unbiased.

Upon reception of the $Z_{\mathrm{sj}}(\ell \times (\mathrm{N}_m+\mathrm{N}_n))$ - dimensional frame matrix signal as appeared in equation (39). Each row in matrix represents one sending to FC from all SUs. Depending on it, the FC will calculate the cumulative sum of the received data vector Z_{sj}, as new data arrive for j=2,3,4....

The FC makes the global decision about the authorized spectrum according to:

Z_{s}: the sum of local hard decision from all SUs as appear in equation (38) .

$$\mathrm{Z_s} = \sum_{\mathrm{K}=1}^{\mathrm{N_u}} (\hat{\mathrm{Z}})^{(\mathrm{K})} \tag{81}$$

$$= \sum_{\mathrm{K}=1}^{\mathbf{N_m}} (\hat{\mathrm{Z}})^{(\mathrm{K})} + \sum_{\mathrm{K}=1}^{\mathbf{N_n}} (\hat{\mathrm{Z}})^{(\mathrm{K})} \tag{82}$$

Actually: The combiner was utilized in the first method (fixed) to collect the arriving Z_{s} till a decision could be made. Here, to enable comparison, we divided the total of the gathered data by the number of measurements ℓ using the same combiner, as follows:

Let :$\mathrm{Z_j} = [\mathrm{Z_1}, \mathrm{Z_2}, \mathrm{Z_3} \ldots\ldots, \mathrm{Z_{N_u}}]$ is a vector of the local decisions sending from all SUs to FC.

Z_j : The first time that the sum of the data in the vector from all SUs send to FC achieve the threshold (this is a sum of Bernoulli random variable so it follows binomial distribution). But ,this case can't happen as $\ell \geq 2$.

$\overline{Z_\mathrm{j}}$: The previous sum of the hard decision that does not achieve a specified threshold.

$[\overline{Z_\mathrm{j}}, Z_\mathrm{j}]$: The second time the data send to FC till the threshold is achieved (this is also weighted sum of two binomial).

$[\overline{Z_\mathrm{j}}, \overline{Z_\mathrm{j}}, Z_\mathrm{j}]$: The third time till the threshold is achieved (this is also weighted sum of three binomial).

.

.

.

$[\overline{Z_\mathrm{j}}, \overline{Z_\mathrm{j}}, \ldots\ldots\ldots, Z_\mathrm{j}]$: The ℓ times required till the threshold is achieved (this is also a sum of ℓ weighted binomial).

The method's mean, variance, and CV match those determined for the fixed in equations. However, since l is a random variable in this case, our equations use a weighted binomial. The variance follows the weighted binomial, but the mean is not much impacted.

Based on the CLT, the binomial is estimated to be Gaussian.

The FC uses the CV tool to estimate the mean and variance for $\hat{Z}$ = [1,0] based on the data that each SU gives to it. Sample mean and sample variance estimators are used in this process. For FC to be able to make a decision, the number of measurements or the forwarding times are required.

The sample mean and the sample variance are estimated and the CV calculated as appeared in equations (40), (41), and (42) respectively to compare to the double thresholds (λ_1, λ_2) shown in Fig.3-12. If CV is greater λ_2 or less than λ_1, the FC will be able to make a decision. The decision will not be clear for FC if the CV is between λ_1 and λ_2 (fuzzy region). In this case, the FC needs more measurements to make a decision.

Here, a gap is always appear between the CV under H_1 and under H_0 and this gap is depending on the chosen value of SNR, for this method the gap is divided into 3 regions (from -∞ to λ_1, from λ_1 to λ_2 and from λ_2 to ∞)

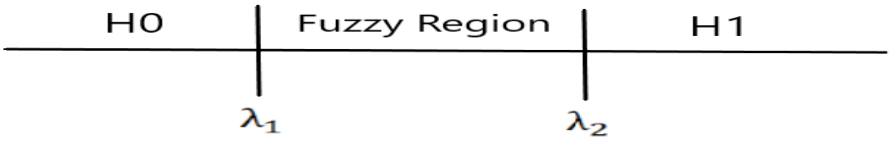


Fig.2 -3: Double Threshold Sequential Method.

The test statistic at FC is calculated by:

$$\begin{cases} \text{if} \quad \mathrm{CV} = \frac{\hat{\mu}_{Zs}}{\hat{\sigma}_{Zs}} > \lambda_2\,, & \text{decide } \mathrm{H}_1 \\ \text{if} \quad \mathrm{CV} = \frac{\hat{\mu}_{Zs}}{\hat{\sigma}_{Zs}} < \lambda_1\,, & \text{decide } \mathrm{H}_0 \\ \text{if } \lambda_1 < \mathrm{CV} = \frac{\hat{\mu}_{Zs}}{\hat{\sigma}_{Zs}} < \lambda_2 \;, & fuzzy\ region(take\ one\ more\ mesurement) \end{cases} \tag{83}$$

The gap between CV under H_0 and CV under H_1 taken and divided to 3 equally regions to determine the double thresholds (λ_1, λ_2) as follow:

$$\lambda_1 = \mathrm{CV}_{\mathrm{H0}} + \frac{\mathrm{CV}_{\mathrm{H1}} - \mathrm{CV}_{\mathrm{H0}}}{3} \tag{84}$$

$$\lambda_2 = \mathrm{CV}_{\mathrm{H0}} + \frac{2(\mathrm{CV}_{\mathrm{H1}} - \mathrm{CV}_{\mathrm{H0}})}{3} \tag{85}$$

If CV > λ_2, it means the PU present and we get 1 detection.

If CV < λ_1, it means the PU absent and we get 0 detection.

If λ_1 <CV < λ_2 , it means no decision can make (continue monitoring).

The detection probability and false alarm probability of the FC can be written as:

$$\begin{cases} \mathrm{P}_{\mathrm{FA}_{\mathrm{FC}}} = \mathrm{p}(\mathrm{CV} > \lambda_2 \quad /\mathrm{H}_0) \\ \mathrm{P}_{\mathrm{D}_{\mathrm{FC}}} = \mathrm{p}(\mathrm{CV} > \lambda_2 \quad /\,\mathrm{H}_1) \end{cases} \tag{86}$$

In SS, the system will stop at FC due to the stopping rule determined by equation (83), which is a simple thresholding scheme for which a desired value of $P_{FA_{\mathrm{FC}}}$ is achieved. The flowchart of Fig.2 -4 illustrates the algorithm used to find the decision of the sequential method at FC.

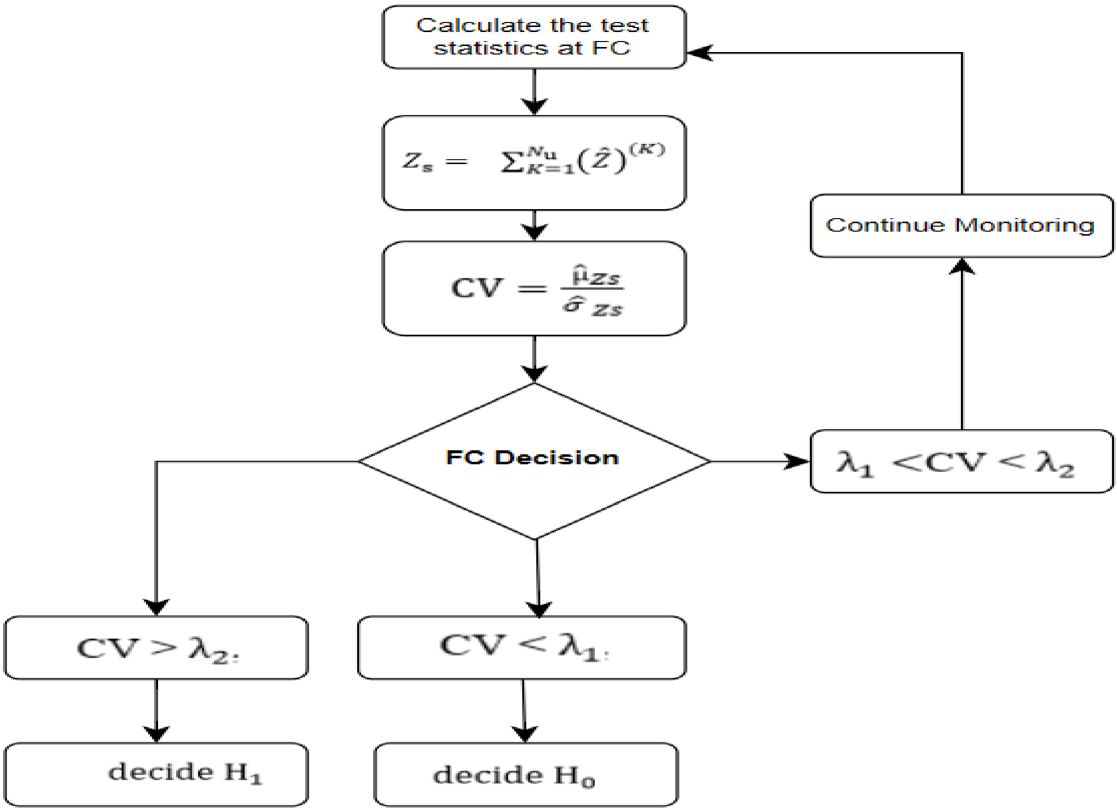

Calculate the test statistics at FC
$Z_s = \sum_{K=1}^{N_u} (\hat{Z})^{(K)}$
$\mathrm{CV} = \frac{\hat{\mu}_{Zs}}{\hat{\sigma}_{Zs}}$
FC Decision
$\lambda_1 < \mathrm{CV} < \lambda_2$
Continue Monitoring
$\mathrm{CV} > \lambda_2$.
$\mathrm{CV} < \lambda_1$.
decide H_1
decide H_0

Fig.2 -4: Flow Chart of Double Threshold Method at FC.

Chapter 3

Simulation Results

3.1 Design Parameter

In this section, we encoded the signal in MATLAB to simulate the output signal from the ED integrator. It consists of the energy values of each sample signal. Then design an energy detector to detect the energy of different samples from the simulated signal we get. Comparing the energy which we detected with the threshold λ (which we consider it a single threshold technique) to be able to determine the presence or the absence of the PU.

The output signal from the ED integrator follows Chi-square distribution, but in section 2.2.2, we assume the Chi-square distribution as Gaussian distribution when samples are large.

Then we set the values of the parameters to simulate the signal as follow:

N_u = 30; N_m is variable (1-30); SNR = 0 dB (at the sensor nodes); the number of samples (that each sensor makes processing to it to justify the use of CLT) T = 100; and the noise power $\sigma^2{}_w$=1 for simplicity; the $\mathrm{pr}(H_0) = 0.5$ and $\mathrm{pr}(H_1)$= 0.5.

a) **<u>Under H_0 :</u>** X~N (0, $\sigma^2{}_w$) ~ N (0, 1) ; since SNR =0 dB.

So $x_1{}^2$~ $\chi_1{}^2$ is Chi-square with 1 degree of freedom.

Then $\sum_{t=1}^{T} X_t^2 \;\sim\; \chi_T{}^2 = \Gamma\,(\frac{100}{2}, 2)$

μ_{Y/H_0}= 100*1=100

$\sigma^2{}_{Y/H_0}$ =2*100*1=200

b) **Under $\mathbf{H_1}$:** X~N (0, $\sigma^2{}_s + \sigma^2{}_w$) ~$N$ (0, 2)

Then $\sum_{t=1}^{T} X_t^2 \;\sim\; \Gamma\,(\frac{100}{2}, 4)$

μ_{Y/H_1}=100*2=200

$\sigma^2{}_{Y/H_1}$ =2*100*4=800

when γ = 1 (as NP), we determine a, b, and c using equations (20), (21) and (22). Since the Q function cannot be solved analytically, we then used MATLAB to numerically determine the roots R1, R2. P_{fa}=0.1 is the result of the roots based on equation (28).

At R1=82.5 and R2=157.5, P_{fa}=0.1080 is found at these roots. Next, find the P_d by substituting the roots in equation (32): P_d= 0.9335.

After that, the signal, which is encoded as zero-mean, is Gaussian-distributed. The noise is added randomly zero-mean, and Gaussian-distributed too. T samples were taken from each SU and added after being squared to be a Gaussian distribution.

Next, using equation (42) to compute CV for each user, the FC determines the estimated mean and variance. These were carried out under $\mathrm{H}_0, \mathrm{H}_1$. Next, we have 30 CV values from all SUs. The maximum under H_0 and the minimum under $\mathrm{H}_1$are considered to compute η, for example, if SNR=0 dB, α=0.4. In this case, η represents the mean difference between the $\mathrm{CV}_{\mathrm{H0}}$ and $\mathrm{CV}_{\mathrm{H1}}$.

If CV > η, it means the spectrum is occupied by primary users and we get 1 detection.

If CV < η, it means the spectrum is idle and we get 0 detection. (We ignore the possibility of CV = η).

As an example, to show calculation: let $\alpha = 0.4, \mathrm{P}_{\mathrm{fa}} = 0.1,\ \mathrm{P}_{\mathrm{d}} = 0.9335,\ \mathrm{N}_{\mathrm{m}} = 10,\ \mathrm{N}_{\mathrm{n}} = 20$.

Under $\mathbf{H_0}$:

$$\text{Mean } z_{s_{\mathrm{H0}}} = \sum_{K=1}^{10}(1 - \mathrm{P}_{\mathrm{fa}})\alpha + \mathrm{P}_{\mathrm{fa}}(1-\alpha) \quad + \sum_{K=1}^{20} \mathrm{P}_{\mathrm{fa}}$$

$$= \sum_{K=1}^{10}((1-0.1)0.4 + 0.1(1-0.4)\ ) + \sum_{K=1}^{20} 0.1 = 6.2$$

Variance $z_{s_{H0}} = \sum_{K=1}^{10}[(1-\alpha)(1-\ P_{fa}) + P_{fa}\alpha\ ][(1-\ P_{fa})\alpha + P_{fa}(1-\alpha)] +$

$\sum_{K=1}^{20}[(1-\ P_{fa})\ P_{fa}\ ]$

$= \sum_{K=1}^{10}[(1-0.4)(1-0.1) + 0.1 * 0.4\ ][(1-0.1)0.4\ + 0.1(1-$

$0.4)]\ +\ \sum_{K=1}^{20}[(1-0.1)0.1\ ]$ =2.436+1.8=4.236.

$$CV_{H0} = \frac{\text{Mean } z_{s_{H0}}}{\sqrt{\text{Variance } z_{s_{H0}}}}$$

Under H_1 :

Mean $z_{s_{H1}}$ $= \sum_{K=1}^{\mathbf{N_m}}(1-\ P_d)\alpha\ +\ P_d(1-\alpha)\quad + \sum_{K=1}^{\mathbf{N_n}}\ P_d$

$= \sum_{K=1}^{10}((1-0.95)0.4\ + 0.95(1-0.4)\ )\ + \sum_{K=1}^{20} 0.95$ =24.9

Variance $z_{s_{H1}} =$ $\sum_{K=1}^{\mathbf{N_m}}[(1-\alpha)(1-\ P_d) +\ P_d\alpha\ ][(1-\ P_d)\alpha\ +\ P_d(1-\alpha)] +$

$\sum_{K=1}^{\mathbf{N_n}}[(1-\ P_d)\ P_d\ ]$

$= \sum_{K=1}^{10}[(1-0.4)(1-0.95) + 0.95 * 0.4\ ][(1-0.95)0.4\ + 0.95(1-$

$0.4)]\ + \sum_{K=1}^{20}[(1-0.95)0.95\ ]$ = 2.419+0.95=3.369.

$$CV_{H1} = \frac{\text{Mean } z_{s_{H1}}}{\sqrt{\text{Variance } z_{s_{H1}}}}$$

This indicates that the CV depends on α, , N_m, N_n. A 10000 iteration of a Monte Carlo simulation is used to implement the CV. The CV in the MATLAB simulation then matches, within acceptable errors, the CV based on the theoretical equations (60) and (61). As a result, the method works well in the simulation and the results are satisfactory.

3.2 Simulation Results

3.2.1: Parameters Effect on CV

In simulation, based on that CV depends on these variables (α, ℓ, N_m), many runs are done as follow:

1- Changing the number of measurements or the forwarding times ℓ.

2- Changing the attacking probability α.

3- Changing the number of N_m from 1-30.

Fig.3-1 (a) and (b) demonstrate that, when the SNR is equal to zero dB, there is a gap between H_0, H_1 for various attacking probability values (0.1,0.2,0.4,0.5,0.6, and 0.7). Also, it is demonstrated that when the attacking probability increases, the CV gap between H_0 and H_1 decreases, with the largest gap for all SNR values occurring at attacking probability α = 0.1. Additionally, it seems that the gap is least when N_m=30.

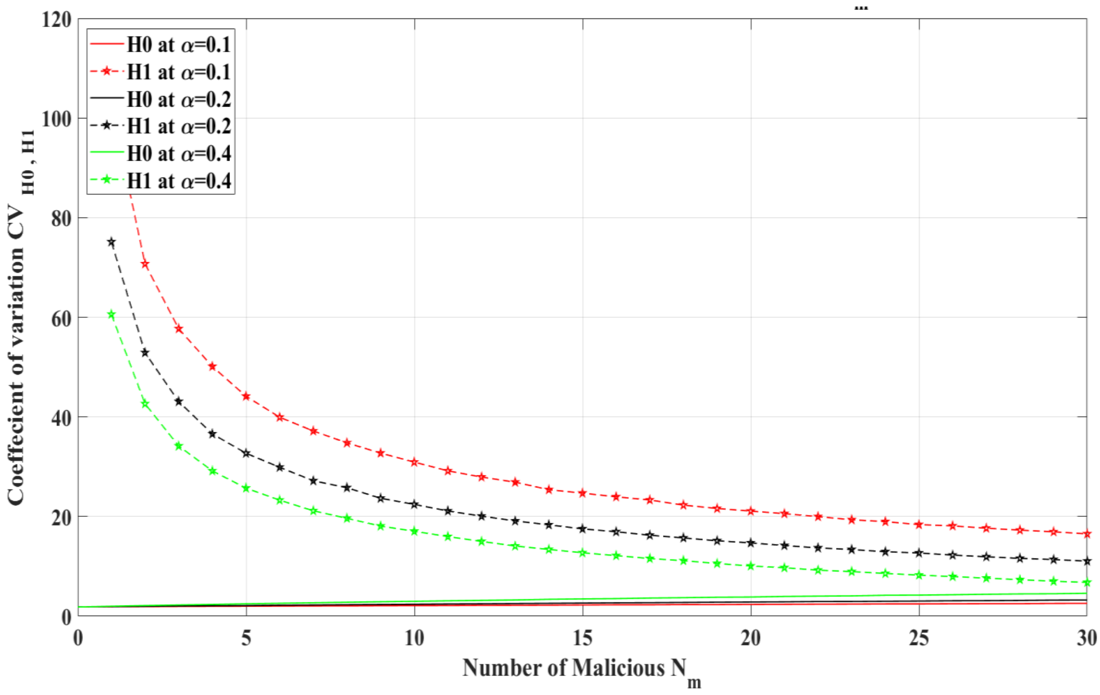


Fig.3-1 (a): Coefficient of variation for α = [0.1,0.2,0.4] as a function of number of malicious.

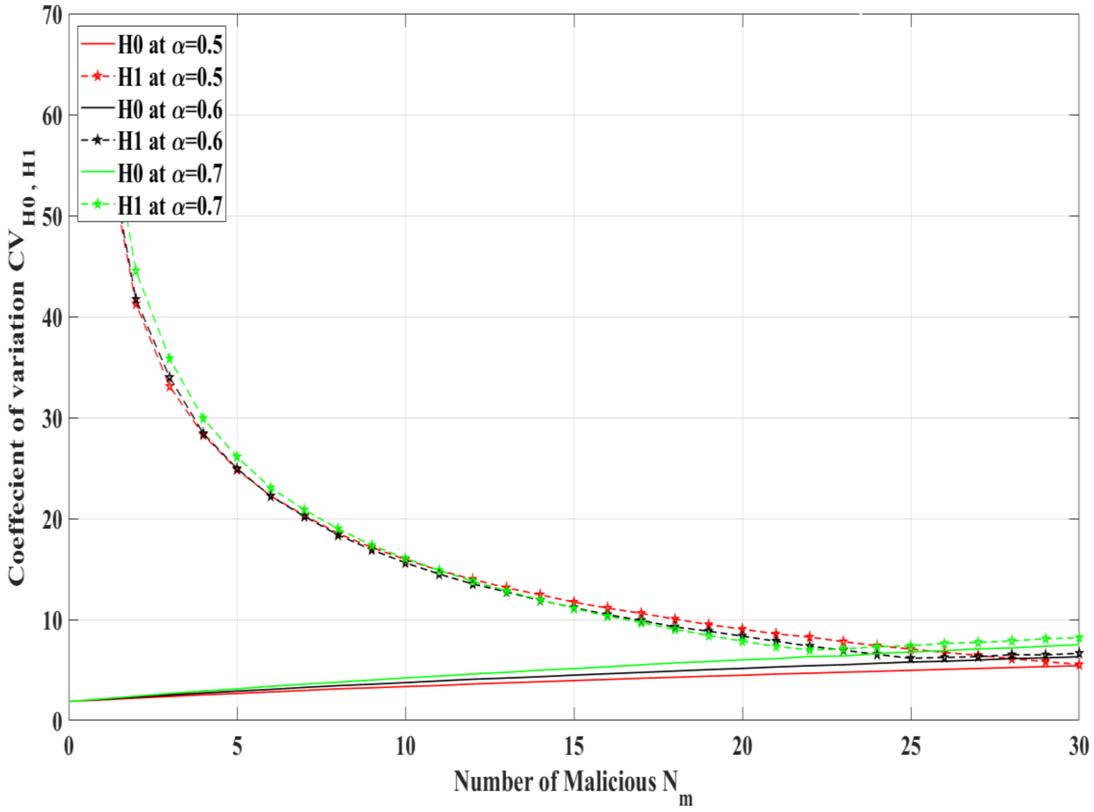


Fig.3-1 (b): Coefficient of variation for α = [0.5,0.6,0.7] as a function of number of malicious.

The relationship between various SNR values (-4 to -10 dB) and CV under H_0, H_1 when N_m = 20 at three distinct attacking probabilities is shown in Fig.3-2. It is demonstrated that the gap between H_0 and H_1 decreases with an increase in the attacking probability (the gap is largest for all SNR values at α = 0.1).

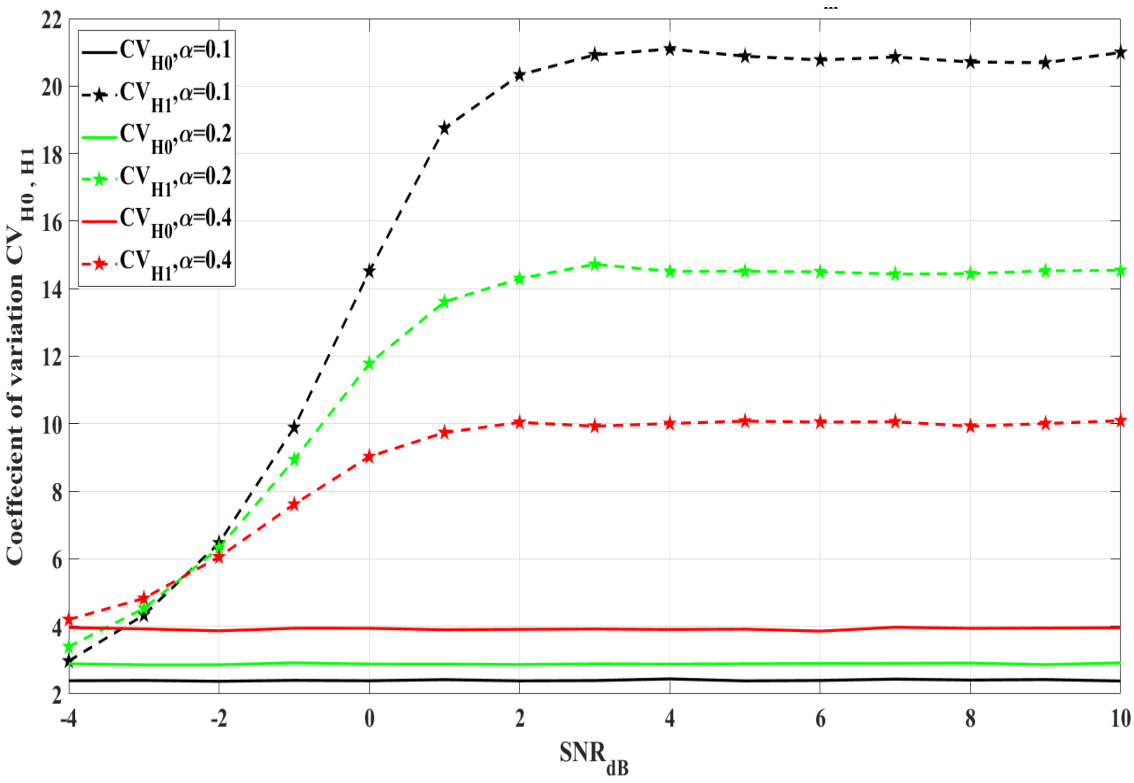


Fig.3-2: Coefficient of variation for α = [0.1,0.2,0.4] as a function of SNR when N_m =20.

Fig.3-3 shows the same result for Fig.3-2 but as N_m is decreased the gap is being less.

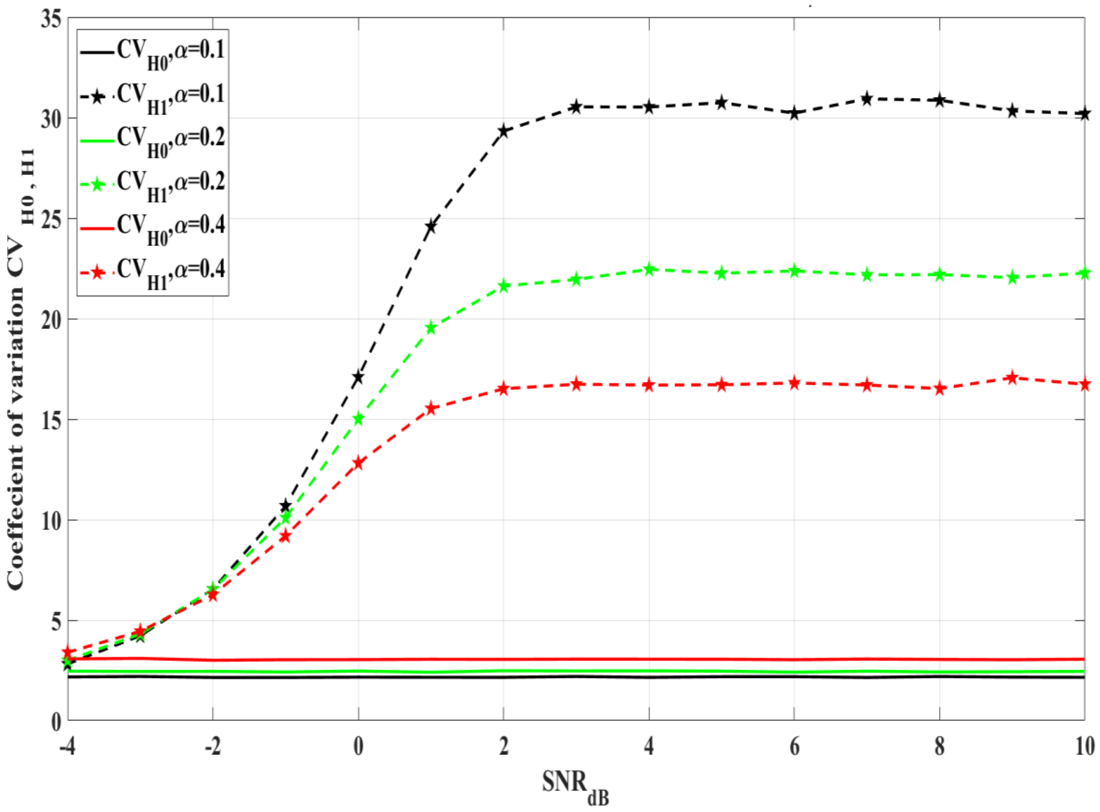


Fig.3-3: Coefficient of variation for α = [0.1,0.2,0.4] as a function of SNR when N_m =10.

So, it is concluded that SNR, attacking probability α, N_m: these parameters affected on the gap of H_0, H_1.

Fig.3-4 shows 3D figure for the relation between CV, α and the number of malicious N_m that there's a gap between H_0, H_1 what ever the N_m in the system and at all attacking probability α. Also, the gap decreases when $N_m = 30$, α more than 0.5.

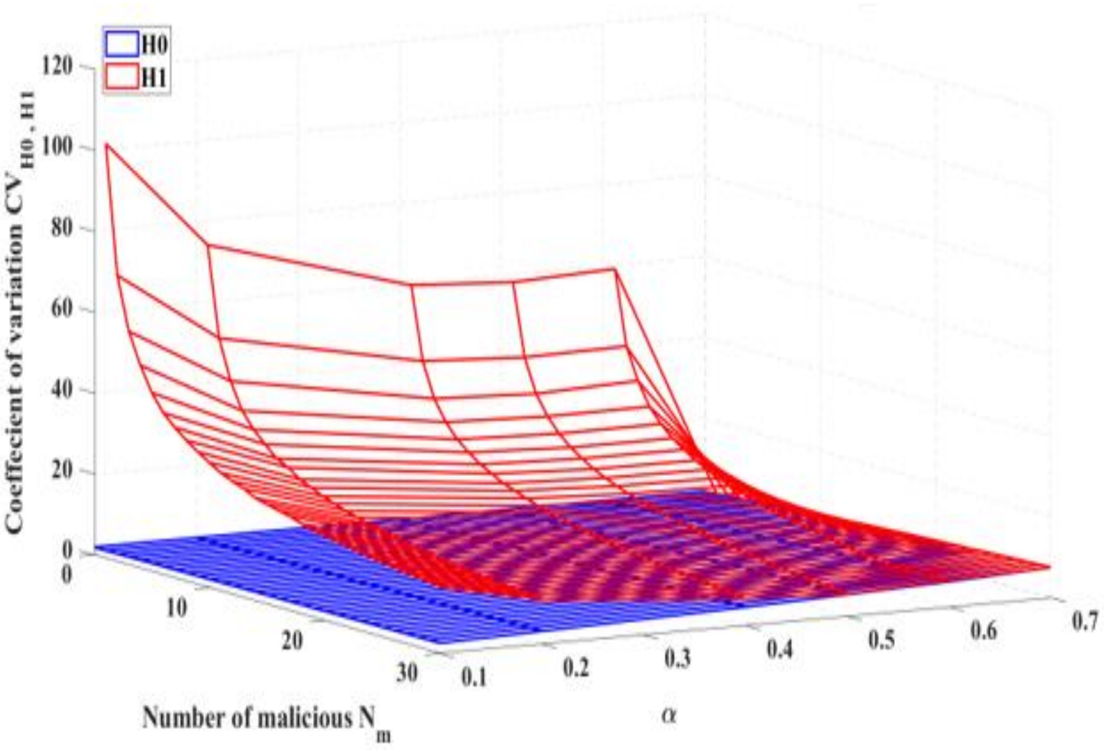


Fig.3-4: 3D of the relation between CV, α and the number of malicious.

As shown in the former figures, FC is able to determine the threshold and make a conclusion by comparing the CV values with it. In order to determine whether the PU exists with the error probability that must be acceptable for the signal to be detected at FC.

3.2.2: Parameters Effect on Error Probability

Fig.3-5 shows the relation between the error probability and the number of measurements ℓ which is in range of (4-30) in the figure. Such that, if ℓ increases P_{error} decreases. For example, at ℓ =30 the $P_{error} = 0.0002425$.

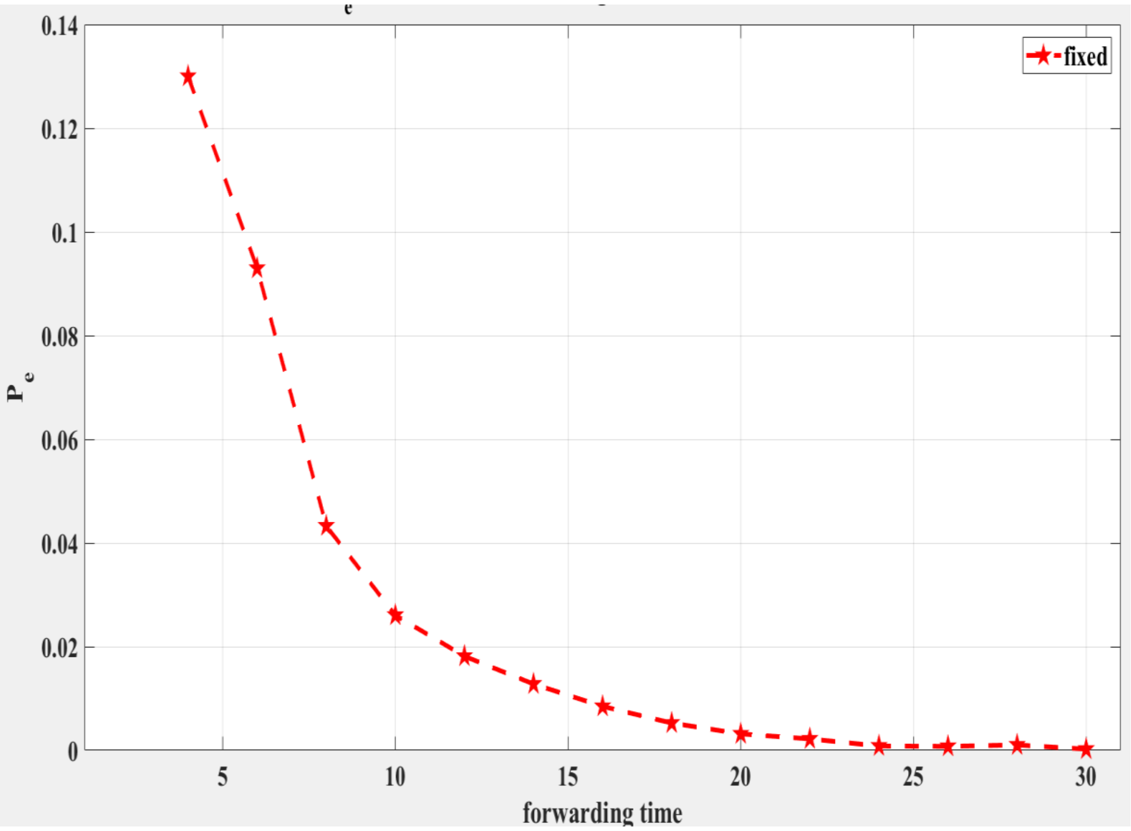


Fig.3-5: The probability of error P_{error} as a function of forwarding times ℓ at SNR=-2dB, $\alpha = 0.2$.

Fig.3-6 shows the relation between the error probability and attacking probability α at ℓ =20 and SNR= -2dB. It's clear that if α is high then the P_{error} is worse as the malicious will falsify the decision more. The worst error probability $P_{error} = 0.5\ at$ α =1.

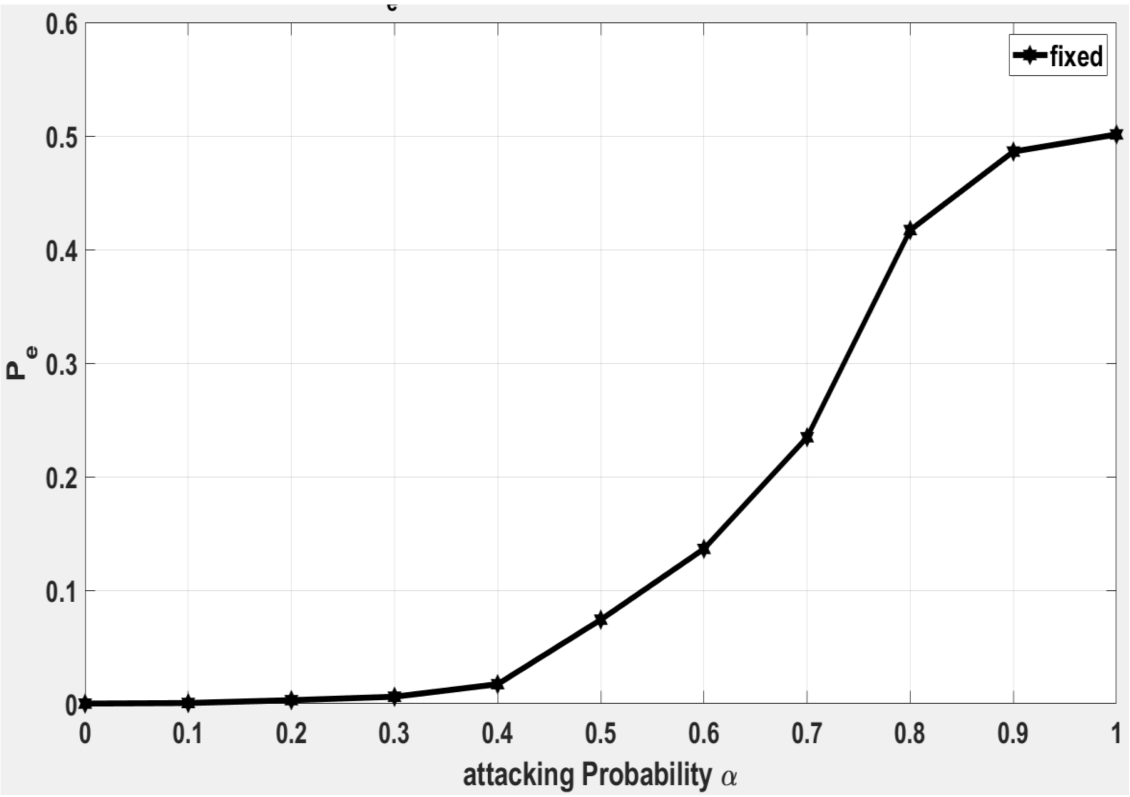


Fig.3-6: The probability of error P_{error} as a function of attacking probability α at ℓ =20 and SNR=-2dB.

Fig.3-7 shows the relation between the error probability and the percentage of malicious in the system at $\alpha = 0.5$, ℓ =20 and SNR= -2dB. It's clear if the percent of Mus increase the P_{error} increase. for example: at percent =0 which means all SUs are LUs. So, the P_{error} is less. And if the percentage =1 which means all SUs are MUs. So, the P_{error} is the worst.

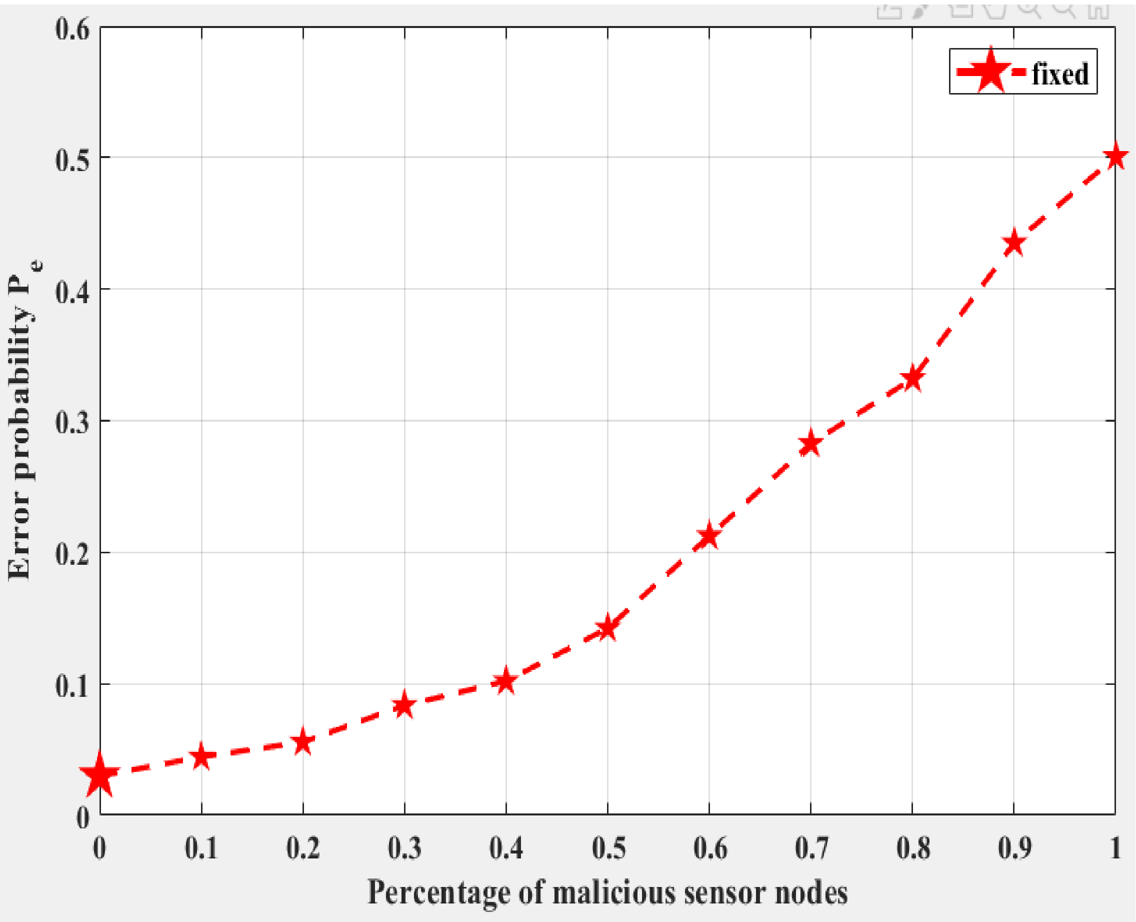


Fig.3-7: The probability of error P_{error} as a function of percentage of malicious users at SNR=-2dB, $\alpha = 0.5$.

3.2.3: Comparing the Analytical and Numerical Forms for the CV

Fig.3-8 shows the relation between CV and number of malicious N_m under constant SNR and attacking probability α that there's a gap between H_0, H_1 what ever the N_m in the system. Also, the gap decreases when $N_m = 30$, α more than 0.5. Also, There's a matching between the CV values under H_0, H_1 which mean the results are satisfying at the same SNR, N_m, α, P_d and P_{fa}.

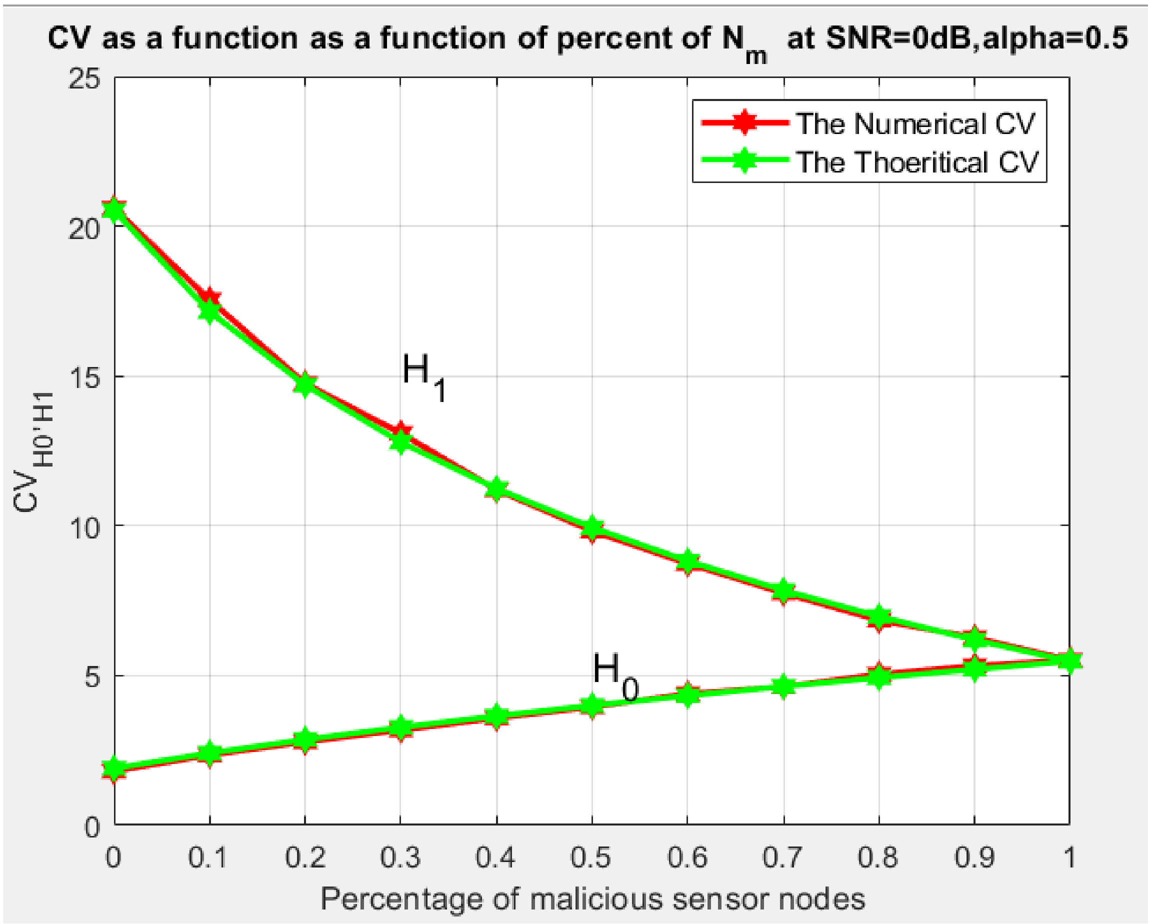


Fig.3-8: Coefficient of variation as a function of number of malicious when $\alpha = 0.5, \mathrm{SNR} = 0\mathrm{dB}$, ℓ=1000.

Table 3-1 shows the calculations of CV values for some samples when $\alpha = 0.5, \mathrm{SNR} = 0\mathrm{dB}$, ℓ=1000, it is confirmed that the values of CV numerically and theoretically are almost the same with acceptable error whatever the α in the system which mean the results are satisfying at the same SNR, $N_m, \alpha,\ P_d$ and P_{fa}.

Table 3-1: Sample calculation of Fig.3-8.

Percentage of malicious	0.2	0.4	0.6	0.7	0.8	1
Numerical CV *under* H_0	2.786038	3.582563	4.39146	4.626305	5.04092	5.512781
Theoretical CV *under* H_0	2.864093	3.651093	4.329249	4.638409	4.931447	5.477226
Numerical CV *under* H_1	14.74559	11.19825	8.735671	7.753623	6.844421	5.510248
Theoretical CV *under* H_1	14.69184	11.23778	8.821133	7.842541	6.97242	5.477226

Fig.3-9 shows the relation between CV and attacking probability α that there's a gap between H_0, H_1 whatever the α in the system and there's a matching between the CV values under H_0, H_1 which mean the results are satisfying at the same SNR, N_m, α, P_d and P_{fa}.

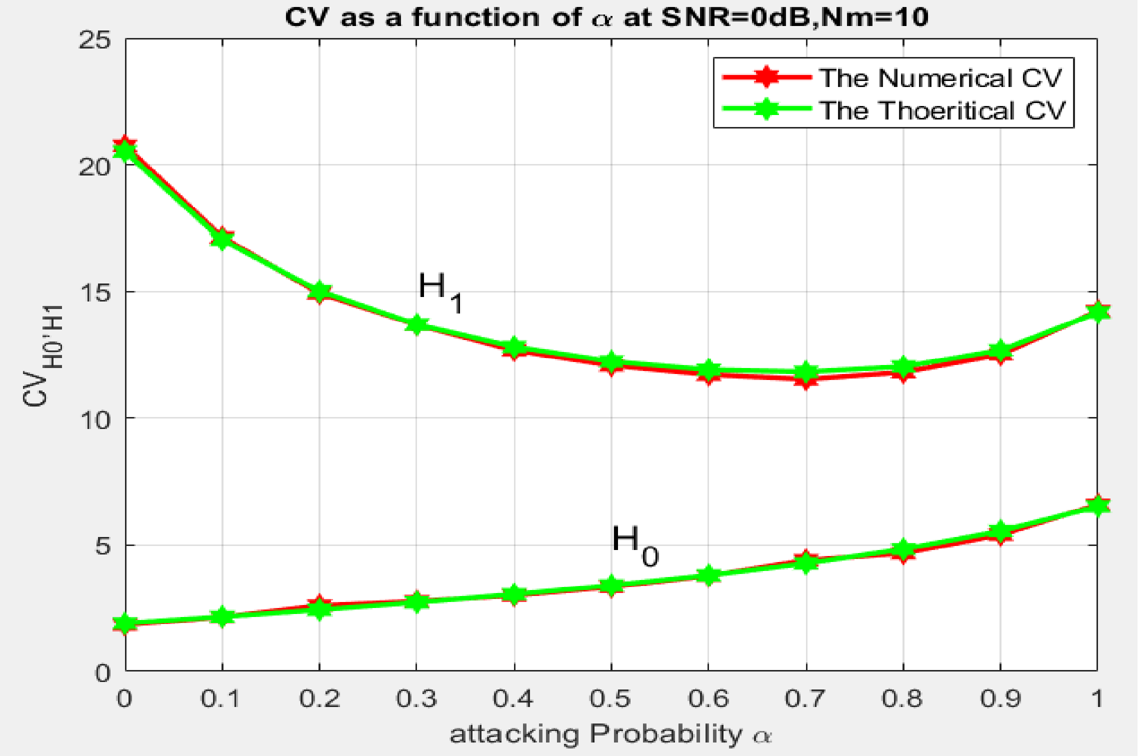
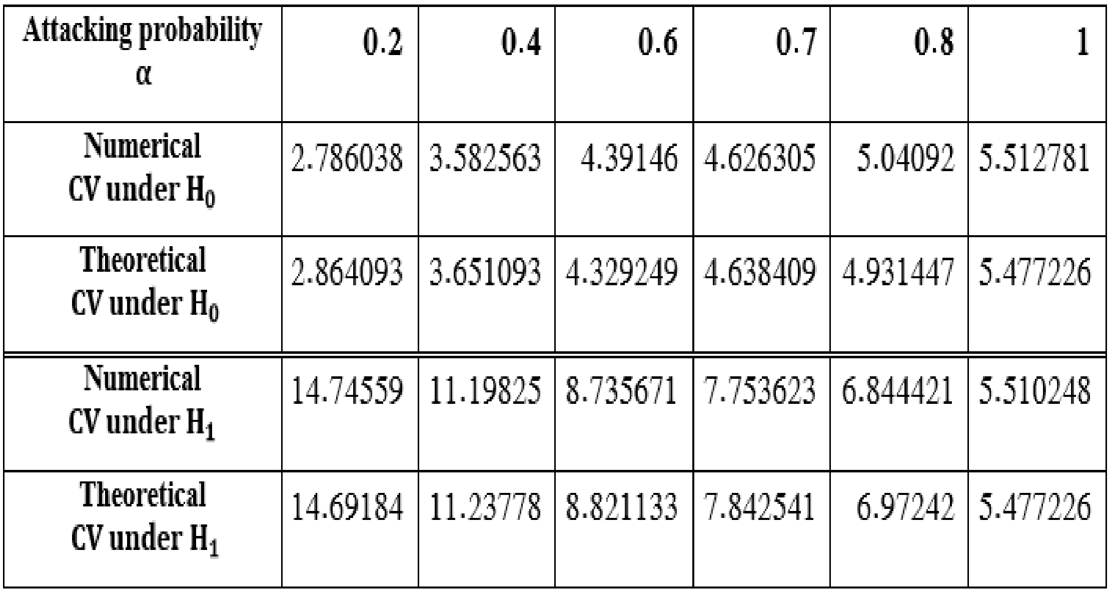


Fig.3-9: Coefficient of variation as a function of α when N_m =10, SNR=0dB, ℓ=1000.

Table 3-2 shows the calculations of CV values for some samples when N_m =10, SNR=0dB, ℓ=1000, it is confirmed that the values of CV numerically and theoretically are almost the same with acceptable error whatever the α in the system which mean the results are satisfying at the same SNR, N_m, α, P_d and P_{fa}.

Table 3-2: Sample calculation of Fig.3-9



Attacking probability α	0.2	0.4	0.6	0.7	0.8	1
Numerical CV under H_0	2.786038	3.582563	4.39146	4.626305	5.04092	5.512781
Theoretical CV under H_0	2.864093	3.651093	4.329249	4.638409	4.931447	5.477226
Numerical CV under H_1	14.74559	11.19825	8.735671	7.753623	6.844421	5.510248
Theoretical CV under H_1	14.69184	11.23778	8.821133	7.842541	6.97242	5.477226

3.2.4: Comparing Error Probability between the Majority Rule and the Fixed Proposed Algorithm

Fig.3-10 shows the relation between the probability of error P_{error} and the percentage of malicious users at SNR=0dB, $\alpha = 0.5$. it is appeared that there’s an matching in both methods at these values and that when all the system is malicious the P_{error} =0.5. It is confirmed that the fixed algorithm is suboptimal of the majority rule.

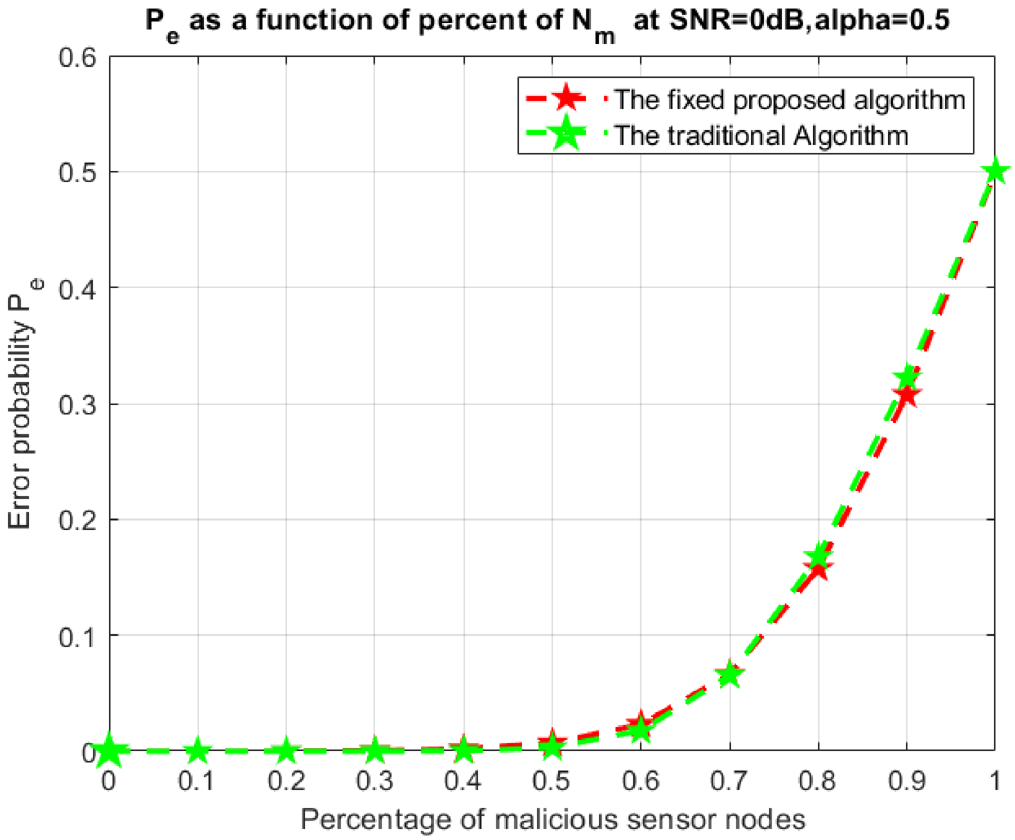


Fig.3-10: Probability of error P_{error} as a function of number of malicious when α =0.5, SNR=0dB, ℓ=1000.

3.2.5: Comparing the Number of Measurements ℓ Between the Sequential Method and the Fixed Proposed Algorithm

The sequential method uses the same argument as in chapter two to treat the sum of the hard decisions as a Gaussian approximation because of CLT. We get two sets of measurements and calculate the $P_{D_{FC}}$, $P_{FA_{FC}}$ for a given value of the false alarm probability. When the target P_{fa} is equal to the value of the $P_{FA_{FC}}$, the system stops working. If not, it will measure again until the target value is reached.

Fig.3-11 shows the relation between the number of measurements ℓ and the attacking probability α at SNR= -2dB, $N_m = 10$ to obtain a fixed value of P_{fa} for example 0.1 for both proposed algorithms (fixed and sequential). It is appeared that in both methods when α increase the number of measurements need to achieve P_{fa} =0.1 increase as the effect of malicious is increased in the system. Moreover, it is confirmed that the sequential method reduced the overhead in the system (reduce the required ℓ values) as it's need less values of ℓ than fixed algorithm to obtain the same P_{fa} at the FC. The fixed method make decision used all ℓ arrived to FC. But the sequential one used in maximum 0.6 of ℓ measurement's. it is appeared that at high α the sequential method is better than the fixed one.

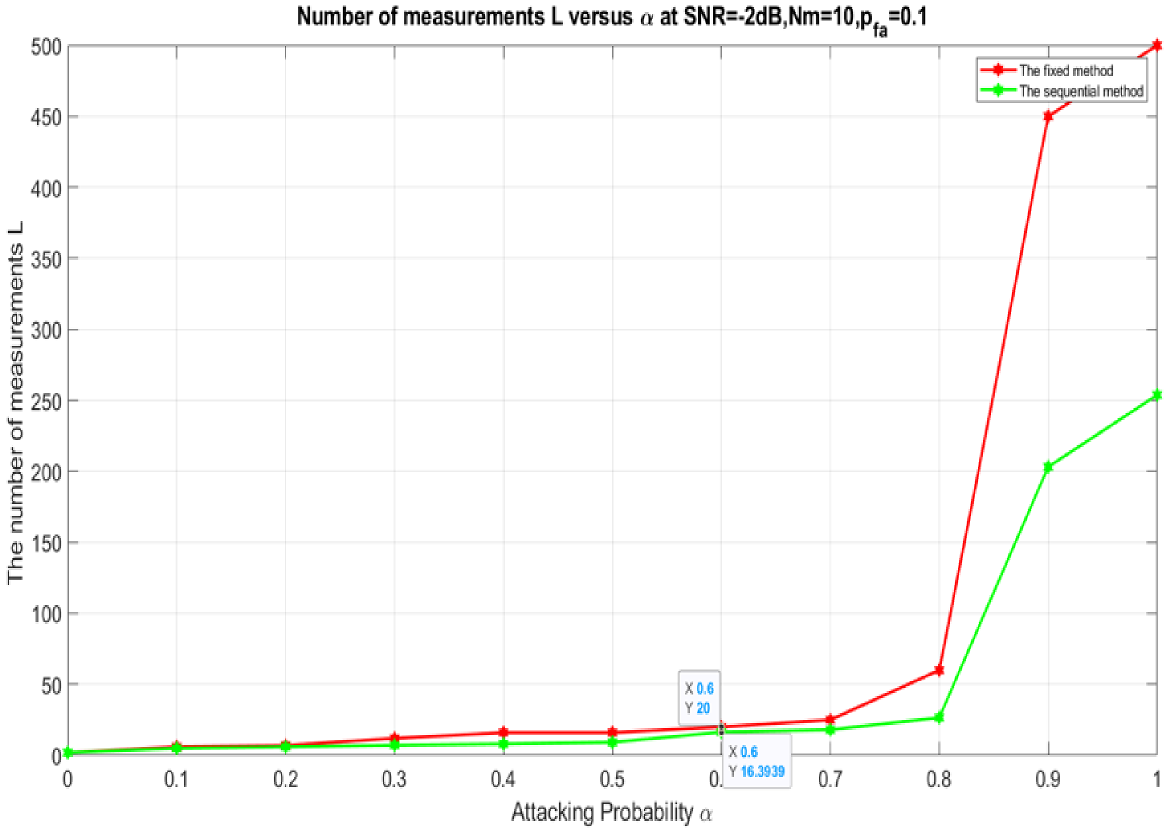


Fig.3-11: The number of measurements ℓ as a function of attacking probability α at SNR= -2dB , P_{fa}=0.1, $N_m = 10$.

Table 3-3 shows the calculations of the forwarding time required for the both algorithms (fixed and sequential)values at all attacking probability α values (0-1) when SNR= 2dB , P_{fa}=0.1, N_m = 10 and it is appeared that when **α** increase, the number of measurements need to achieve P_{fa} =0.1 increase. Also, the sequential method reduced the overhead in the system for example at α=0.9, the sequential needs 203 measurements but the fixed need 450 to obtain the same P_{fa} at the FC which mean approximately half of the measurements.

Table 3-3: Forwarding Time calculation of Fig.3-11.

Attacking Probability α	Forwarding Time Fixed	Forwarding Time Sequential
0	2	2
0.1	6	5
0.2	7	6
0.3	12	7
0.4	16	8
0.5	18	9
0.6	20	16
0.7	25	18
0.8	60	26
0.9	450	203
1	500	253

Chapter 4

Conclusion

4.1 Conclusion

The benefits of using collaboration among SUs are reduced by the presence of MUs in a CSS environment. In a CSS environment, effective and prompt PU detection is required to prevent the FC from making incorrect conclusions about the PU status. This thesis focuses on improving the performance of CSS using CV tool. The FC is taking sensing information from all cooperating SUs, including LUs and MUs, and combining them for a more precise and concrete decision about the licensed user spectrum. The Simulations reflect the superiority and authenticity of the proposed scheme in producing an accurate and reliable decision in CSS at the FC. Also, the algorithm can restrict a user's inappropriate behavior in the CR network and avoid privacy violations and improve the detection probability.

The main results obtained by this thesis are:

- When the number of MUs in the system varies between 0 and 30, there is always a gap between the CV under H_0 and H_1, which can be used at this time to make a decision at FC.

- The CV is investigated for the number of measurements ℓ, attacking probability α, and the percentage of malicious user effects, and the error probability is determined as follow:
  - When the percentage of MUs increase the P_{error} increase as the gap decrease.
  - When the attacking probability α increase the P_{error} increase as the gap decrease.
  - When the number of measurements ℓ increase the P_{error} decrease.

- The fixed proposed algorithm is compared with the traditional majority rule in terms of the error probability.

- The sequential proposed method is compared to the fixed in terms of the number of measurement, it is confirmed that sequential method reduces the overhead in the system.

Bibliography

[1] W. B. Tesfay, T. Booth and K. Andersson, "Reputation Based Security Model for Android Applications," *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, UK, 2012, pp. 896-901, doi: 10.1109/TrustCom.2012.236.

[2] A. Salcedo and E. Martinez, "Analysis of the Electromagnetic Spectrum under the Extremely Low Frequency Band: Frequency Sub-Bands Classification," *2017 International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE)*, Cuernavaca, Mexico, 2017, pp. 157-162, doi: 10.1109/ICMEAE.2017.15.

[3 S. Haykin, D. J. Thomson and J. H. Reed, "Spectrum Sensing for Cognitive Radio," in *Proceedings of the IEEE*, vol. 97, no. 5, pp. 849-877, May 2009, doi: 10.1109/JPROC.2009.2015711.

[4] M. Falih and H. Abdullah, "A Combined Spectrum Sensing Method Based DCT for Cognitive Radio System" ,International Journal of Electrical and Computer Engineering (IJECE). , vol. 10, no. 2, pp. 1935- 1942, 2020.

[5] M. I. Khalaf, D. Al- jumeily, and A. L. Eds, "Applied Computing to Support Industry", vol. 2. Springer International Publishing, 2019.

[6] D. Bhargavi and C. R. Murthy, "Performance comparison of energy, matched-filter and cyclostationarity-based spectrum sensing," *2010 IEEE 11th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Marrakech, Morocco, 2010, pp. 1-5, doi: 10.1109/SPAWC.2010.5670882.

[7] D. Cabric, S. M. Mishra and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.*, Pacific Grove, CA, USA, 2004, pp. 772-776 Vol.1, doi: 10.1109/ACSSC.2004.1399240.

[8] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, Baltimore, MD, USA, 2005, pp. 124-130, doi: 10.1109/DYSPAN.2005.1542626.

[9] H. Sun, A. Nallanathan, C. -X. Wang and Y. Chen, "Wideband spectrum sensing for cognitive radio networks: a survey," in *IEEE Wireless Communications*, vol. 20, no. 2, pp. 74-81, April 2013, doi: 10.1109/MWC.2013.6507397.

[10] S. Chatterjee, S. P. Maity and T. Acharya, "Energy Efficient Cognitive Radio System for Joint Spectrum Sensing and Data Transmission," in *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 4, no. 3, pp. 292-300, Sept. 2014, doi: 10.1109/JETCAS.2014.2337191.

[11] I. Sobron, P. S. R. Diniz, W. A. Martins and M. Velez, "Energy Detection Technique for Adaptive Spectrum Sensing," in *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 617-627, March 2015, doi: 10.1109/TCOMM.2015.2394436.

[12] R. Tandra and A. Sahai, "SNR Walls for Signal Detection," in *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 4-17, Feb. 2008, doi: 10.1109/JSTSP.2007.914879.

[13] S. S. Kalamkar, A. Banerjee and A. K. Gupta, "SNR wall for generalized energy detection under noise uncertainty in cognitive radio," *2013 19th Asia-Pacific Conference on Communications (APCC)*, Denpasar, Indonesia, 2013, pp. 375-380, doi: 10.1109/APCC.2013.6765974.

[14] A. Polydoros and I. Dagres, "Estimation-based noise-robust sensing," *2012 7th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, Stockholm, Sweden, 2012, pp. 362-366, doi: 10.4108/icst.crowncom.2012.248723.

[15] K.kockaya and I. Develi, ,"Spectrum sensing in cognitive radio networks: threshold optimization and analysis.," J Wireless Com Network 2020, 255 ,2020. https://doi.org/10.1186/s13638-020-01870-7.

[16] S. Yuan, L. Li and C. Chigan, "On MMD-Based Secure Fusion Strategy for Robust Cooperative Spectrum Sensing," in *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 504-516, Sept. 2019, doi: 10.1109/TCCN.2019.2906236.

[17] A. Kumar, S. Saha and R. Bhattacharya, "Wavelet Transform Based Novel Edge Detection Algorithms for Wideband Spectrum Sensing in CRNs" , AEU - Int. J. Electron. Commun. , vol. 84, no. November 2017, pp. 100- 110, 2018, doi: 10.1016/ j. aeue. 2017. 11. 024.

[18] S. V. R. K. Rao and G. Singh, "Wavelet Based Spectrum Sensing Techniques in Cognitive Radio" , Procedia Eng. , vol. 38, pp. 880- 888, 2012, doi: 10. 1016/ j. proeng. 2012. 06. 111.

[19] K. Divakaran , N. Manikandan and S. Hari, "Wavelet Based Spectrum Sensing Techniques for Cognitive Radio- A Survey" , International Journal of Computer Science & Information Technology (IJCSIT), Vol. 3, No. 2, April 2011.

[20] H. Ziboon and A. Thabit, "A New Proposed Adaptive Cognitive Radio detection system Based on MLP Neural Network for Different Modulation Schemes" , ARPN J. Eng. Appl. Sci., vol. 12, no. 2, pp. 521- 527, 2017.

[21] E. Salman *et al*., "On the energy detection performance based Welch's DCT algorithm in cognitive radio systems," *2018 1st International Scientific Conference of Engineering Sciences - 3rd Scientific Conference of Engineering Science (ISCES)*, Diyala, Iraq, 2018, pp. 135-139, doi: 10.1109/ISCES.2018.8340542.

[22] M. Falih and H. Abdullah, “DWT Based Energy Detection Spectrum Sensing Method for Cognitive Radio System.,” Iraqi Journal of Information and communications Technology 3(3):1-11,2020. https://doi.org/10.31987/ijict.3.3.99.

[23] I. Akyildiz, B. Lo and R. Balakrishnan, “Cooperative spectrum sensing in cognitive radio networks: A survey,” Physical Communication, vol. 4 no. 1 pp. 40-62, 2011. Elsevier https://doi.org/10.1016/j.phycom.2010.12.003

[24] I. Harjula, A. Hekkala, M. Matinmikko and M. Mustonen, "Performance Evaluation of Spectrum Sensing Using Welch Periodogram for OFDM Signals," *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, Budapest, Hungary, 2011, pp. 1-5, doi: 10.1109/VETECS.2011.5956246.

[25] J. Lehtomaki, “Analysis of energy-based signal detection,” A Doctoral Dissertation, University of Oulu, 2005. Available online, http://herkules.oulu.fi/isbn9514279255.

[26] C. Sun, W. Zhang and K. Ben Letaief, "Cooperative Spectrum Sensing for Cognitive Radios under Bandwidth Constraints," *2007 IEEE Wireless Communications and Networking Conference*, Hong Kong, China, 2007, pp. 1-5, doi: 10.1109/WCNC.2007.6.

[27] M. Alijani and A. Osman, “Calculate the optimum threshold for double energy detection technique in cognitive radio networks (CRNs)”,2022.

[28] W. Zhang, X. Jing and J. Li, "An Energy Detection Based on Coefficient of Variation for Spectrum Sensing in Cognitive Radio”, Lect. Notes Electr. Eng., vol. 473, pp. 87- 94, 2018, doi: 10.1007/ 978- 981- 10- 7521- 6- 11.

[29] X. Luo, "Secure Cooperative Spectrum Sensing Strategy Based on Reputation Mechanism for Cognitive Wireless Sensor Networks," in *IEEE Access*, vol. 8, pp. 131361-131369, 2020, doi: 10.1109/ACCESS.2020.3009466.

[30] X. Ni, H. Chen, L. Xie and K. Wang, "Reputation-based hierarchically cooperative spectrum sensing scheme in cognitive radio networks," *2013 IEEE/CIC International Conference on Communications in China (ICCC),* Xi'an, China, 2013, pp. 397-402, doi: 10.1109/ICCChina.2013.6671149.

[31] R. Wan, L. Ding, N. Xiong and X. Zhou, "Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks, " International Journal of Distributed Sensor Networks, vol. 15, no. 9, p. 1550147719870645, 2019. https://doi.org/10.1177/1550147719870645

[32] V. Brinda and M. Bhuvaneshwari, "Identifying Malicious Secondary User Presence Within Primary User Range in Cognitive Radio Networks, " Wireless Pers Commun 122, 2687–2699 ,2022. https://doi.org/10.1007/s11277-021-09025-7.

[33] K.-C. Chen and R. Prasad, " Cognitive Radio Networks, " Wiley, 2009.

[34] M. Grissa, B. Hamdaoui and A. A. Yavuz, "Location Privacy in Cognitive Radio Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1726-1760, thirdquarter 2017, doi: 10.1109/COMST.2017.2693965.

[35] H. Vu-Van and I. Koo, "A robust cooperative spectrum sensing based on Kullback-Leibler divergence, " IEICE Transactions on Communications, vol. E95–B, no. 4, pp. 1286–1290, 2012.

[36] N. Gul, A. Naveed, A. Elahi, T. SaleemKhattak and I. M. Qureshi, "A combination of double sided neighbor distance and Genetic Algorithm in cooperative spectrum sensing against malicious users," 2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 2017, pp. 746-753, doi: 10.1109/IBCAST.2017.7868137.

[37] S. Swati et al. , "Energy Detection Spectrum Sensing in Cognitive Radio, " 2017.

[38] M. Abdo-Tuko, " Performance Evaluation and Comparison of Different Transmitter Detection Techniques for Application in Cognitive Radio, " International Journal of Networks and Communications, 2015, p-ISSN: 2168-4936, e-ISSN: 2168-4944.

[39] J. G. Proakis, "Digital communications, fourth ed. McGraw-Hill, " 2001.

[40] S. M. Kay, " Fundamentals of statistical signal Processing, " Vol. II, Detection theory. Prentice-Hall International Editions, Upper Saddle River, NJ, 1998.

[41] A. Kumar, , P. Thakur, S. Pandit, et al., " Analysis of optimal threshold selection for spectrum sensing in a cognitive radio network: an energy detection approach," Wireless Netw 25, 3917–3931 , 2019.

[42] L. As-Sayid-Ahmad, N. Mansour and D. Dahlhaus, "Robust Cooperative Primary User Detection in Malicious Cognitive Radio Networks," *2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, Sofia, Bulgaria, 2022, pp. 65-71, doi: 10.1109/BlackSeaCom54372.2022.9858285.