DETECTION AND ISOLATION OF PRIMARY USER EMULATOR IN COGNITIVE RADIO NETWORK USING HYBRID OF ANGLE OF ARRIVAL AND RECEIVED SIGNAL STRENGTH

BY

ADEBO, Samuel Attai
(PhD/SEET/2015/800)

DEPARTMENT OF TELECOMMUNICATION ENGINEERING
FEDERAL UNIVERSITY OF TECHNOLOGY MINNA

SEPTEMBER, 2021

ABSTRACT

Cognitive Radio (CR) technology is the candidate panacea to the problem of spectrum scarcity in the wireless world. However, this emerging technology is faced with security challenges. The most severe among these security challenges is Primary User Emulation Attack (PUEA). One of the methods to detect Primary User Emulator (PUE) is via localisation, of which there are two major categories: range-free and range-based. Range-free localisation is cost effective, less computationally complex and easy to deploy. However, it is less accurate when compared with range-based category. Since accuracy is fundamental in localisation, range-based localisation scheme was adopted in this work. The range-based category is reported to be more accurate although with higher complexity. Among this category are Angle of Arrival (AOA), which utilises angular measurements to localise the PUE, and the Received Signal Strength (RSS), which employs only distance to localise the PUE. To improve performance of range-based methods, this research hybridised AOA and RSS techniques to localise PUEs in television (TV) white spaces. This scheme determines the angle at which the Primary User's (PU's) signal arrives at the Secondary Users (SUs) and the distance between the PU and SUs in the Cognitive Radio Network (CRN). Because in a TV white space, the location of PU is known, the computed AOA and the distance obtained from the RSS are therefore used to determine the position of a PU's signal transmitter. This position is compared with the location of the PU to ascertain the true source of the signal, thus detecting the PUE. Computer simulations demonstrated that the hybrid scheme estimated the position of the PUE much faster and with a much lower Root Mean Square Error (RMSE) of $5.00\text{x}10^{-3}$ after 20 iterations. This greatly outperformed RSS and AOA methods that estimated the position of PUE after 50 iterations with RMSE of $2.00\text{x}10^{-1}$ and $1.00\text{x}10^{-2}$ respectively when considered individually. Furthermore, investigation was made on the selection of the best pair of SUs to be used in the detection processes. It was discovered that a pair of SUs from the same communication environment whose RSS values are very close, detected PUE better (with RMSE of $4.7\text{x}10^{-3}$ after 20 iterations) than a pair of SUs whose RSS values are higher but in different communication environments as they localised PUE with RMSE of $6.0\text{x}10^{-3}$ after 70 iterations. The significance of this result is appreciated especially when attention is given to the fact that speed, accuracy and energy efficiency are essential in the efficient operation of cognitive radios. Energy-efficient operations are essential in the current global energy crises that wireless systems face. Moreover, by isolating the detected PUE from Cognitive Radio Network (CRN), there is availability of more spectrum holes that will accommodate newer wireless technologies for effective communication. Furthermore, Secondary Users (SUs) have more transmission time, improved quality of service (QoS), connection reliability, higher throughput and improvement in the overall general performance of the entire cognitive radio network.

TABLE OF CONTENTS

Content **Page**

LIST OF TABLES

Table **Title** **Page**

LIST OF FIGURES

ABBREVIATIONS

AOA	Angle of Arrival
AWGN	Additive White Guassian Noise
CCDA	Common Control Data Attack

CR	Cognitive Radio
CRN	Cognitive Radio Network
CSS	Cooperative Spectrum Sensing
DC	Decision Centre
DOA	Direction of Arrival
DSA	Dynamic Spectrum Access
EME	Energy with Minimum Eigenvalue
FCC	Federal Communication Commission
GPS	Global Positioning System
HLM	Hybrid Localisation Method
MAC	Medium Access Control
ML	Maximum Likelihood
MME	Maximum Minimum Eigenvalue
MSC	Mobile Switching Centre
NB	Narrow Band
OFA	Objective Function Attack
OSS	Opportunistic Spectrum Sharing
PER	Primary Exclusive Region
PU	Primary User
PUE	Primary User Emulator
PUEA	Primary User Emulation Attack
QoS	Quality of Service
RMSE	Root Mean Square Error
SBS	Secondary Base Station
SCN	Selfish Channel Negotiation

SNR	Signal-to-Noise-Ratio
SSDF	Spectrum Signal Data Falsification
SU	Secondary User
TDOA	Time Difference of Arrival
TOA	Time of Arrival
TV	Television
WB	Wide Band

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background to the Study

There is an increase in the deployment of newer wireless technologies leading to more demand for radio spectrum (Anandakumara & Umamaheswarib, 2017; Gupta & Onumanyi, 2019). The radio spectrum is referred to as the portion or band of the electromagnetic continuum that conveys radio waves. The most desired band for various wireless communications is 30MHz-3GHz (Lin *et al*., 2018; Khaliq *et al*., 2018). Initially, radio spectrum was assigned in the order of request. But with increased deployment rate of newer wireless technologies, there is an increased pressure on the available radio spectrum. This has indicated possibility of spectrum scarcity (Zeng *et al*., 2008; Zina & Noureddine, 2015; Vasanthareddy & Sanjeev, 2021).

The causes of spectrum scarcity are several as postulated in literature. One of the reasons for spectrum scarcity is emergence of newer wireless technologies (Balieiro *et al.*, 2014; Anandakumara & Umamaheswarib, 2017). Another cause of spectrum scarcity is the inept permanent frequency allocation policy (Subhedar & Birajdar, 2011; Maninder *et al*., 2016). Similarly, Jin *et al*. (2015) identified inefficient spectrum usage as potential basis for spectrum scarcity. These reasons indicate that spectrum is not scarce, but inadequately utilized as there are still licensed bands which are not fully utilized (Malik *et al*., 2010; Subhedar & Birajdar, 2011; Yuan *et al*., 2012).

Akyildiz *et al*. (2006) and Rehman, (2019) further corroborated this assertion of actual spectrum utilization as Figure 1.1shows that some portions of the licensed frequency band in the electromagnetic radio spectrum are heavily used while others either experience sparse use or medium use with less than 6% occupancy.

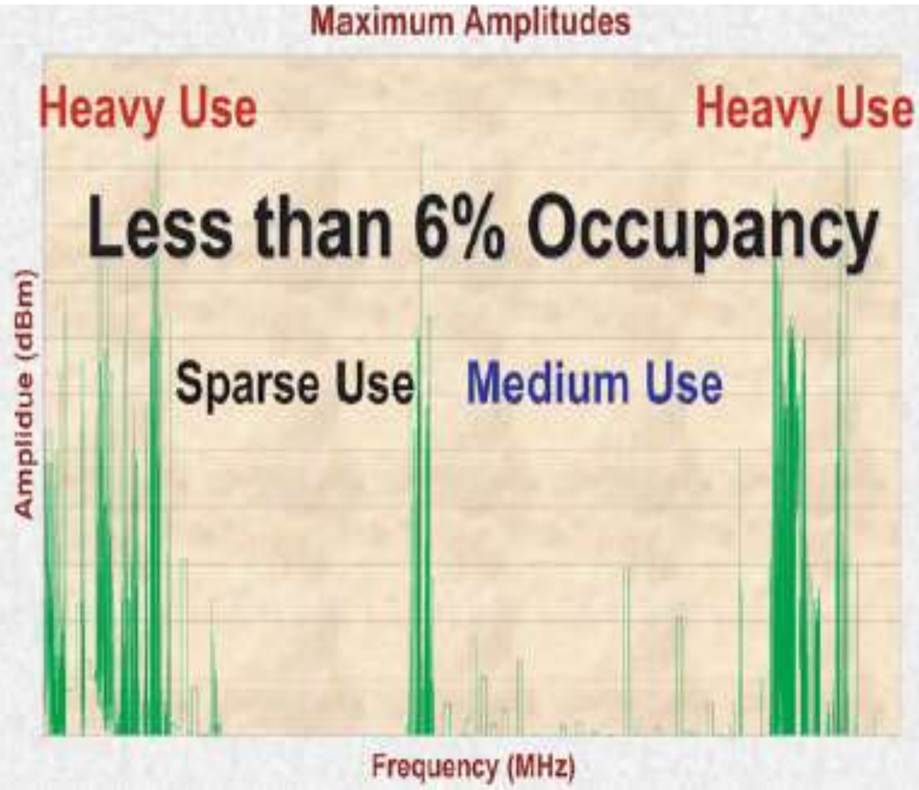


Figure 1.1: Spectrum Usage (Maninder *et al*., 2016; Rehman, 2019)

Because of underutilization of the allocated spectrum bands and the attendant difficulties in retrieving them from those allocated to, it becomes needful to develop new and dynamic methods for spectrum management and efficient utilization using cognitive radio (CR) technology (Goyal *et al*., 2016; Rharras *et al*., 2020).

CR technology is identified in literature as candidate panacea to spectrum underutilization and scarcity occasioned by static spectrum allocation (Amer *et al*., 2016; Verma *et al*., 2018; Ali *et al*., 2019). CR refers to Secondary User (SU) which is able to identify its communication environment by fine-tuning its radio parameters and opportunistically uses spectrum licensed to Primary Users (PUs) when the band is inactive without causing interference to the PU. This inactive spectrum through which CR transmits is called spectrum hole or white space (Nilesh & Patil, 2014; Sultana & Hussain, 2018). According to Arthy and Periyasamy (2015), a given radio spectrum with spectrum holes can be envisioned as depicted in Figure 1.2 where spectrum in use and spectrum holes are clearly indicated and CR dynamically accesses the spectrum holes.

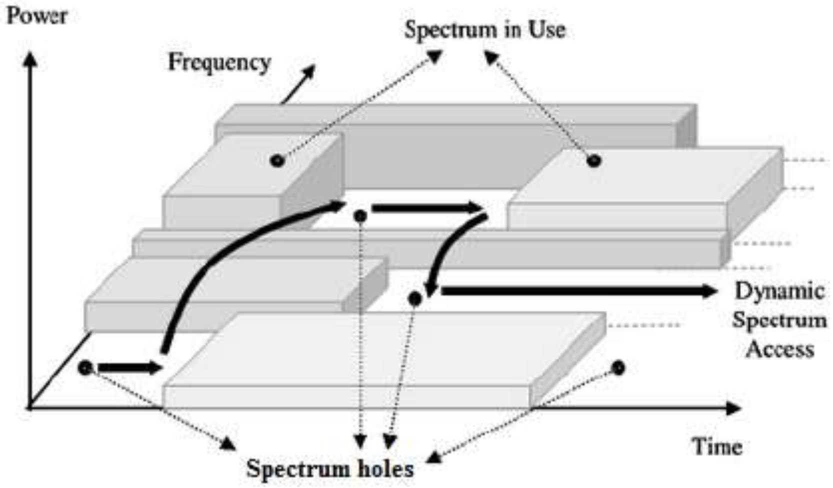


Figure 1.2: Radio spectrum with spectrum holes

(Arthy & Periyasamy, 2015)

From the foregoing, it is obvious that CR could actually enhance spectrum usage efficiency and alleviate the challenge of spectrum scarcity (Gupta *et al*., 2016; Anandakumara & Umamaheswarib, 2017; Akbari & Jamshid, 2018). Several processes are involved in the development of a cognitive radio (CR). These processes are described in the Figure 1.3

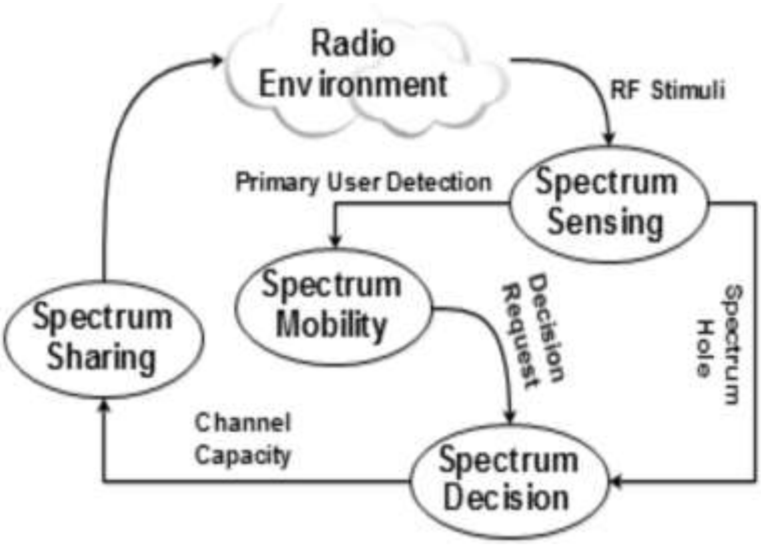


Figure 1.3: Cognitive Cycle of a Cognitive Radio (Maninder *et al*., 2016)

1.1.1 Spectrum sensing

Spectrum Sensing which is the most significant component of CR operations is the process by which a CR detects the incumbent signals (Deng *et al*., 2012; Maninder *et al*., 2016). Since CR can only utilize idle portion of the spectrum, it must observe the spectrum bands to detect unused spectrum. To ensure a trustworthy spectrum sensing process, the problem of attacks on the CRNs (which is the focus of this research) needs to be addressed by distinguishing PU signals from SU signals because uncertain, falsified or corruptly sensed data can alter the entire sensing result. Hence, the spectrum decision becomes inaccurate. This leads to false alarm and interference to PU signals (Kanti *et al*., 2015; Alhumud *et al*., 2019).

1.1.2 Spectrum decision

As soon as spectrum holes are detected, it is necessary that the CR selects the best band based on their Quality of Service (QoS) requirements. Prior information about activity of the PU is required in order to devise a spectrum decision algorithm that incorporates dynamic spectrum characteristics. As a requirement, the spectrum bands should be characterized in radio and statistical behaviours (Kanti *et al.*, 2015; Giral & Hern, 2020).

1.1.3 Spectrum sharing

Since multiple CRs in the CRN compete for available spectrum holes, there will be collision in overlapping portions of the spectrum holes. To prevent this, their transmission should be coordinated. Through spectrum sharing, spectrum resources can be opportunistically allocated to multiple CRs (Gelabert *et al.*, 2010). It also involves prevention of interference with the primary network through resource allocation. Moreover, this function enables a CR Medium Access Control (MAC) that enables the sensing control to allot sensing task among the cooperating nodes as well as spectrum access to determine transmission time (Alhumud *et al*., 2019).

1.1.4 Spectrum mobility

CR should vacate the particular portion of spectrum in use as soon as PU is detected and continues its transmission in any vacant portion of the spectrum. Therefore, spectrum mobility enables a spectrum hand off scheme to identify the link failure and shift to a new route from the current transmission or switch to a fresh spectrum band with less quality degradation. This involves collaboration of spectrum sensing, neighbour discovery in the link layer and routing protocols. Moreover, this functionality requires connection management scheme to sustain the performance of the upper layer protocols by alleviating effects of spectrum switching (Kanti *et al*., 2015; Alhumud *et al*., 2019).

Although the various operations of CR cycle in cognitive radio system are distinct, they depend on each other for the successful operations of CRN. Therefore, failure on any of the operation will lead to failure of CR operation. For example, the dynamic spectrum access (DSA) of CR will not be achieved if spectrum sensing operation fails.

CR operation is possible due to its reconfigurability and cognitive capability (Kumar & Singh, 2016; Sultana & Hussain, 2018). Reconfigurability allows a CR to adjust to its environment by regulating certain parameters like carrier frequency, bandwidth and transmission power (Liang *et al*., 2008). This becomes important because CRs must utilize the fallow bands opportunistically and vacates the bands whenever PU signal is detected. Cognitive capability of CRs (also referred to as SUs) prepares them to sense their radio environment and choose the most suitable transmission mode available in the fallow bands. This is achievable by the spectrum management process where different parameters like power, modulation type and frequency are estimated (Kaur *et al*., 2010).

1.1.5 Spectrum security

Traditional wireless communication technology faces several security threats among which are forgery, masquerading attacks and eavesdropping. These threats can easily interrupt communication during transmission (Alhakami *et al*., 2014). Although Cognitive Radio (CR) system is threatened by various security issues that traditional wireless communication system faces, it faces several other security threats among which Primary User Emulation Attack (PUEA) is the most challenging. When an impish secondary user masquerades itself as the primary user for unscrupulous reasons, PUEA is said to have occurred. Except it is addressed, PUEA can cripple the whole cognitive radio network (CRN). In order to avoid this, Primary User Emulator (PUE) should be segregated from the Cognitive Radio Network (CRN) upon detection. This will not only ensure availability of spectrum for newer wireless technologies, it will also guarantee cheaper and secured communication (Alahmadi *et al*., 2014).

1.2 Statement of the Research Problem

The task of detecting the PUEs remains a difficult process because of the lack of features to distinguish between PUEs and actual PUs (Chen *et al*., 2008a; Saeed *et al.*, 2019). Consequently, inability to localise PUEs often leads to denial of service (DoS) and inefficient use of spectrum for CR purpose. Moreover, PUEA is continuous as long as it is in CRN. If detected but left in CRN, PUE will continue to launch Primary User Emulation Attack (PUEA). Existing techniques for detecting PUEs such as Angle of Arrival, Received Signal Strength, Time of Arrival and Time Difference of Arrival, have their short comings when applied individually (Bouabdellah *et al.*, 2019). Thus, there is need to investigate the effects of a hybridised scheme for detecting PUEs in CRNs and isolate the detected PUEs from CRN. The outcome of this research work will be used for the development of economically viable and efficient method of detecting PUEs in CRN. This will lead to availability of more spectrum holes that will accommodate newer wireless technologies for effective communication.

1.3 Aim and Objectives of the Study

This research work aimed at developing an improved localisation scheme for detecting Primary User Emulator (PUE) in CRNs and isolating the detected PUE from the cognitive radio network (CRN). To achieve this aim, the objectives are to:

i. develop a hybrid of Angle of Arrival (AOA) and Received Signal Strength (RSS) schemes for localizing Primary User Emulator (PUE) in Cognitive Radio Networks (CRNs).

ii. evaluate the effects of cooperative sensing on the detection of Primary User Emulator (PUE) using the developed hybrid scheme in i.

iii. develop a technique for isolating detected Primary User Emulators (PUEs).

iv. evaluate the performance of the overall developed scheme.

1.4 Significance of the Study

Cognitive Radio Technology (CRT) is the panacea to the current spectrum scarcity posed by spectrum underutilization. However, there are many challenges to realizing its concept in practice. The most critical among the many challenges is the one posed by PUE. PUE mimics the spectral characteristics of the PU for selfish or malicious purpose. If PUEA is not dealt with, realizing CR concept remains a mirage. Hence, this study developed a technique to detecting PUE as well as eliminating it from the network for availability of more radio spectrum and efficient operation of CR devices. The outcome of this research work will benefit researchers as it will be used for the development of economically viable and efficient method of detecting PUEs in CRN. Availability of more spectrum holes will accommodate newer wireless technologies for effective communication. This without doubt leads to cheaper call and data rates, reliable connection, improved quality of service and elimination of denial of service which are beneficial to individuals and the society.

1.5 Scope of the Study

The focus of this study is on the development of a hybrid localisation method using AOA and RSS to detect the PUE and isolate it from CRN. It also investigates the effect of cooperative sensing in the localisation of PUE.

1.6 Thesis outline

The remaining chapters of this thesis are structured in this order: The review of related literatures in the domain of Cognitive Radio (CR), Primary User Emulation Attacks (PUEAs) and classifications of primary user emulators are given in chapter two. It further reviews different methods for detecting Primary User Emulator (PUE) and various spectrum sensing techniques. Chapter three presents the research methodology. It describes detection of PUE with the aid of Hybrid Localisation Method (HLM) and the effects Cooperative Spectrum Sensing (CSS) has on HLM. It further presents a method for isolating the detected PUE from the CRN. The results obtained from the developed techniques in chapter three as well as comparative analysis of the results with existing techniques are presented in chapter four while the conclusion based on the achievements of this study and the challenges encountered as well as recommendation for further work are presented in the fifth chapter.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Background to Radio Spectrum

The part of electromagnetic wave that carries radio waves is called radio spectrum. The most desired band for wireless communication is within 30MHz and 3GHz out of which only 5.2% is used on the average (Li *et al*., 2017; Lin *et al*., 2018). Initially, radio spectrum was apportioned to the newer wireless technologies in the order in which they were requested. But, with increased deployment rates of newer wireless technologies, there is an increased pressure on the available radio spectrum. This has notified policy makers on the possibility of spectrum scarcity if spectrum is not efficiently utilized. From research findings, it is clear that the problem of spectrum underutilization can be solved through opportunistic spectrum sharing using Cognitive Radio (CR) technology (Khaliq *et al*., 2018).

2.2 Cognitive Radio: A Solution to Spectrum Underutilization

Spectrum management became the focal point of Federal Communication Commission (FCC) due to an increasing request for radio spectrum caused by the upsurge in the emergence of new wireless communication technologies. Towards addressing the problem of spectrum underutilization, FCC came up with Opportunistic Spectrum Sharing (OSS). Television (TV) bands are opened up for OSS sharing because they often experience less spectrum utilization when compared to other networks.

CR also referred to as secondary user (SU) is the enabling technology for OSS (Chen *et al*., 2008b; Muñoz *et al*., 2020a). To ensure a trustworthy spectrum sensing process, the security problems on the CRNs needs to be addressed.

2.3 Spectrum Sensing in Cognitive Radio

Spectrum sensing is the ability to measure and be conscious of the parameters related to the radio channel characteristics, spectrum availability, transmit power, interference and noise, radio’s operating environment, user requirements and applications, available networks (infrastructures) and nodes, local policies and other operating restrictions. It is done across frequency, time, geographical space, code and phase. Various Spectrum sensing techniques abound and are broadly divided into three categories: non-cooperative spectrum sensing, cooperative spectrum sensing and interference-based spectrum sensing with each having its advantages and disadvantages (Dibal *et al.*, 2018).

2.4 Review of Spectrum Sensing Techniques

Spectrum sensing in cognitive radio network is achieved by using any of the spectrum sensing methods broadly classified in Figure 2.1. These spectrum sensing methods have their advantages and disadvantages (Arthy & Periyasamy, 2015)

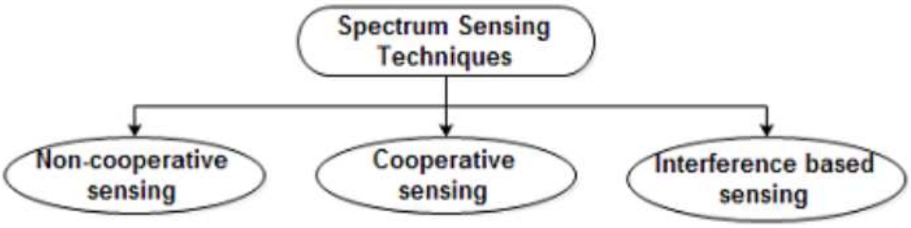
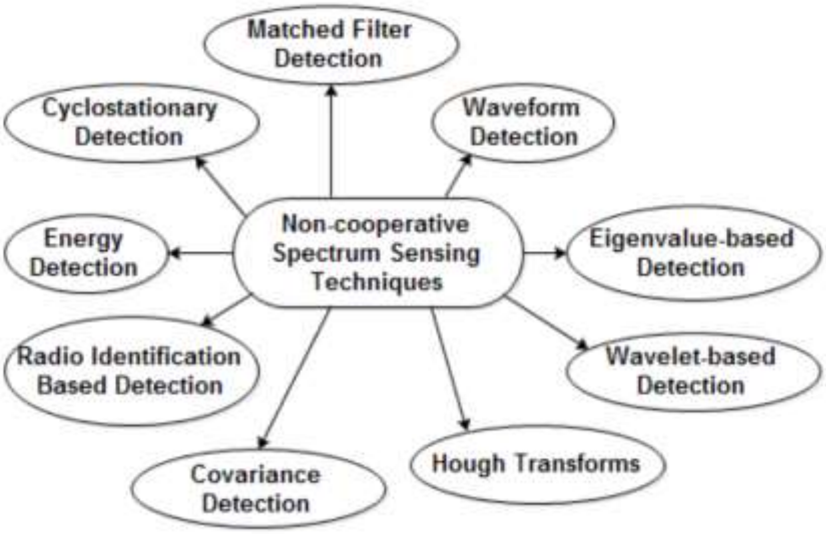


Figure 2.1: Classifications of Spectrum Sensing Methods

(Arthy & Periyasamy, 2015)

2.4.1 Non-cooperative sensing

In this technique, a cognitive radio (CR) determines the availability or non-availability of primary user (PU) in a particular spectrum space. Figure 2.2 depicts the various non-cooperative spectrum sensing techniques (Arthy& Periyasamy, 2015).



Matched Filter Detection
Cyclostationary Detection
Waveform Detection
Energy Detection
Non-cooperative Spectrum Sensing Techniques
Eigenvalue-based Detection
Radio Identification Based Detection
Wavelet-based Detection
Covariance Detection
Hough Transforms

Figure 2.2: Classification of Non-cooperative Spectrum Sensing Techniques

(Arthy & Periyasamy, 2015; Dibal *et al*., 2018)

2.4.1.1 Energy detection

Energy detection method does not require advance knowledge of primary user's characteristics. This makes energy detection accomplish spectrum sensing with low computational and implementation complexities. It also has less sensing time duration, low implementation cost and low power consumption. However, it performs poorly under low Signal-to-Noise-Ratio (SNR) but performs appreciably at high SNR. Moreover, it cannot differentiate between PU signal and noise but it can be used in narrow and wide band channels. The working principle of energy detection is presented in Figure 2.3 (Salama *et al*., 2018).

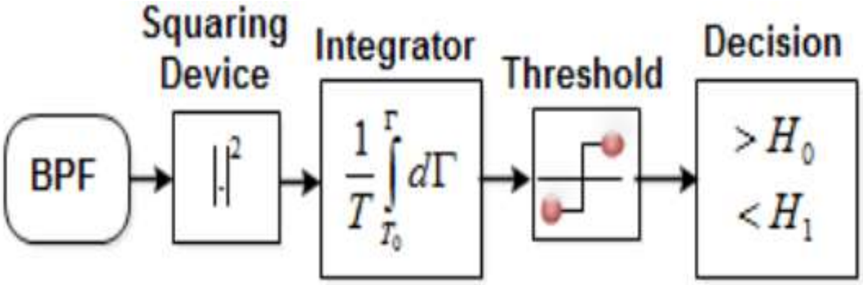


Figure 2.3: Energy Detector (Salama *et al*., 2018)

For a certain amount of samples *N*, the energy *y* can be computed as (Gupta *et al.*, 2016; Lin *et al.*, 2018):

$$y = \frac{1}{k}\sum_{k=1}^{k} | x[\mathrm{k}] |^2 \qquad (2.1)$$

where,

x[k] is the received signal.

The hypotheses of detection are given by (2.2) and (2.3):

$$P_d = P(y \geq \gamma / H_1) \qquad (2.2)$$

$$P_{fa} = P(y > \gamma / H_0) \qquad (2.3)$$

where,

P_d *is* the probability of detection *and* P_{fa} is the probability of false alarm. The receiver selects the hypothesis H_1 when y in (2.2) is equal to or greater than a predetermined threshold, γ. However if y in (2.3) is less than γ, the NULL (H_0) hypothesis is selected.

2.4.1.2 Cyclostationary detection

Cyclostationary detection technique of spectrum sensing uses the cyclostationary features of signals to detect spectrum status (Mabrook & Hussein, 2015). As shown in Figure 2.4, cyclostationary detector exploits spreading code, pulse train, sinusoidal carriers, code and other features to detect the periodicity of the signal.

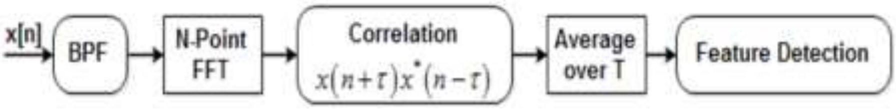


Figure 2.4: Cyclostationary Feature Detector (Mabrook & Hussein, 2015).

Aside having high computational complexity, long computational time and very high power consumption, cyclostationary detection also needs advance knowledge of the primary user's (PU's) signal's features. Conversely, it performs better at low SNR and does not require phase and frequency synchronization. Moreover, it is applicable in both narrow and wide bands. It has high sensing accuracy and high communication flexibility.

2.4.1.3 Matched filter detection

With fore knowledge of the PU signals, matched filter accurately detects PU's signals (Vadivelu *et al.*, 2014). With this method, SNR is maximized while Additive White Gaussian noise (AWGN) is present. It also has less sensing time, low cost, very high sensing accuracy, very high communication flexibility and moderate power consumption. However, it needs separate receiver for each type of PU and it is only used in narrow bands. Operation of matched filter detection is presented in Figure 2.5 (Mabrook & Hussein, 2015).

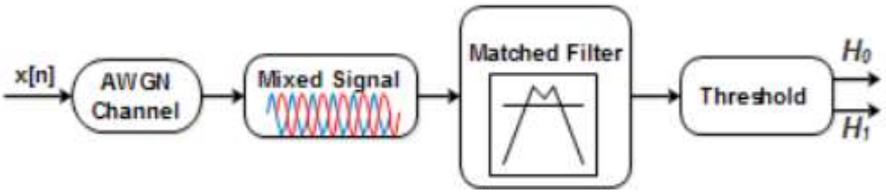


Figure 2.5: Matched Filter Detector (Mabrook & Hussein, 2015)

2.2.1.4 Waveform-based detection

Waveform spectrum sensing is usually applied for spectrum sensing only when the wave patterns of an incoming signal are known. Waveform-based detection requires these patterns for synchronization purposes. As shown in Figure 2.6, waveform spectrum sensing is achieved by comparing the received signal with the known signal.

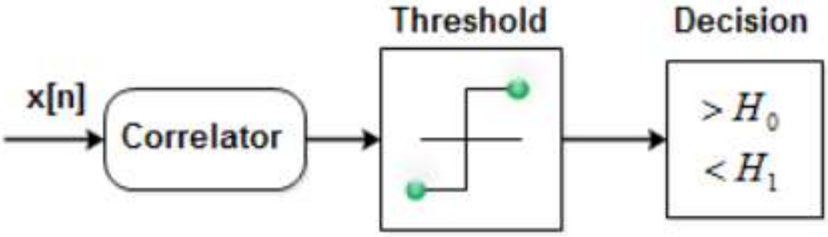


Figure 2.6: Waveform-based detection (Dibal *et al*., 2018)

Although waveform-based detection has low energy consumption, moderate deployment cost, less sensing time duration and computationally less complex, it requires advance knowledge of the PU signal, has low communication flexibility, has low sensing accuracy and finds application only in narrow bands.

2.4.1.5 Eigen value-based detection

Eigen value-based detection determines the status of the PU by calculating Eigen values related to the covariance matrix of a received signal. This technique uses Maximum-Minimum Eigen (MME) value which computes the ratio between the minimum Eigen value and the energy of the received signal. Figure 2.7 depicts Eigen value-based detection scheme.

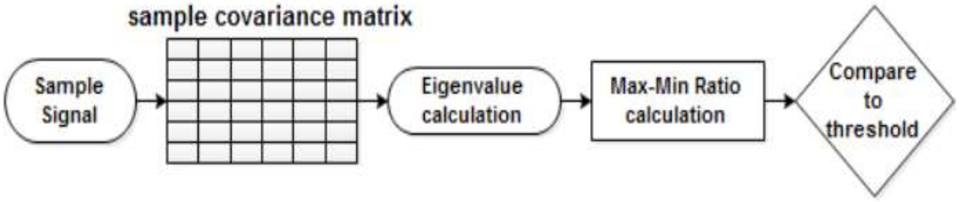


Figure 2.7: Eigen value detection (Dibal *et al.*, 2018)

Eigen value detection has very low sensing accuracy and communication flexibility as well as long computational complexity and sensing time duration. However, it has moderate implementation cost and moderate power consumption. It requires no synchronization and it is insensitive to noise uncertainty.

2.4.1.6 Covariance detection

In covariance detection, spectrum sensing is achieved by observing the disparity between autocorrelation of signal and noise. In this case, focus is on the off-diagonal elements of the covariance elements of the covariance matrix. Usually, the elements are nonzero in the presence of primary user but zero in the absence of primary user (Subhedar & Birajdar, 2011; Maninder *et al*., 2016). The block diagram of covariance detection is depicted in Figure 2.8

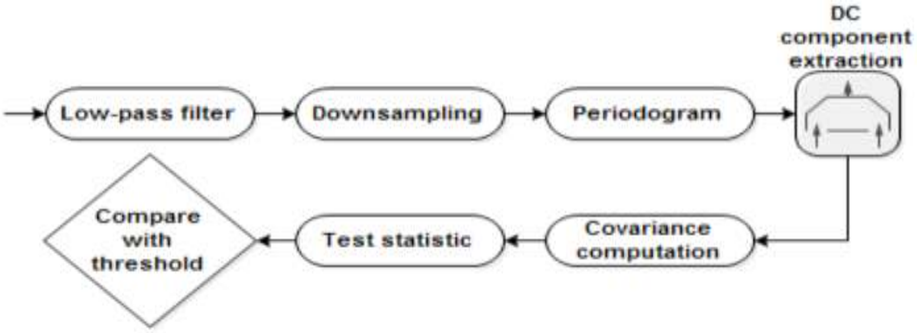


Figure 2. 8: Covariance detection (Maninder *et al.*, 2016)

2.4.1.7 Radio identification-based detection

Radio identification-based detection is applicable in the context of European Ubiquitous Terminal (TRUST) project. In this technique cognitive radio uses range and modulation to sense the spectrum (Subhedar & Birajdar, 2011; Maninder *et al*., 2016).

2.4.1.8 Hough transform

This detection technique deals with signal in the similitude of an edge detection problem. Because of the presence of noise and breakages, non-uniform illumination is experienced in the edges. Hence, edge detection algorithm with linking algorithm is followed.

2.4.1.9 Wavelet-based detection

In this technique, Wavelet is used to detect edges in the power spectral density of a signal in a communication channel. Spectrum sensing using wavelets is achieved by the disintegration of a signal into smaller non-overlapping sub-bands, which are then applied to the wavelet in order to detect the edges in Power Spectral Density (PSD).

Table 2.1 presents the summary of commonly-used non-cooperative spectrum sensing Methods.

Table 2.1: Comparison of Commonly-Used Non-Cooperative Spectrum Sensing Methods

Sensing Techniques	Narrow Band(NB)/Wide Band(WB)	Prior signal knowledge	Sensing Accuracy	Communication Flexibility	Computational complexity	Sensing time duration	Cost	Power Consumption
Energy detector	NB/WB	No	Low	Low	Low	Less	Low	Low
Cyclostati-onary based detection	NB	Yes	High	High	High	Long	High	High
Matched filter detection	NB	Yes	High	High	Low	Less	Low	Low
Waveform based detection	NB	Yes	Low	Low	Low	Low	Low	Low
Eigen value based detection	NB	Yes	Low	Low	Low	Long	Low	Low

(Subhedar & Birajdar, 2011; Maninder *et al.*, 2016).

Energy detection is chosen in this work because it does not require prior knowledge of the PU. It has very low computational complexity, very low sensing duration, very low cost, very low power consumption and finds application both in wide and narrow bands.

2.4.2 Cooperative spectrum sensing

Cooperative spectrum sensing (CSS) solves the problem of fading, shadowing, hidden node, missed detection and false alarm as CRs collaborate to achieve awareness of communication channel (Armi *et al.,* 2009; Amer *et al.*, 2016). CSS consists of two Schemes which are: Centralized spectrum sensing and distributed spectrum sensing. In centralized spectrum sensing, a central node such as base station (BS) gathers the sensing information for evaluation and decides the available channels and identifies an incumbent user. It relays this information to other CRs. In distributed spectrum sensing, each node shares its sensed information with other nodes but the final decisions are taken by individual CR node without the control of a central node (Zhang & Lili, 2017).

2.4.2.1 Merits of cooperative spectrum sensing

The following are the merits of cooperative spectrum sensing:

i. It solves the challenge of hidden node and also reduces sensing problem imposed by shadowing and fading.

ii. Unlike local sensing, cooperative sensing achieves high gain in terms of sensed spectrum.

iii. With cooperative spectrum sensing technique, detection time is reduced

2.4.2.2 Demerits of Cooperative Spectrum Sensing

The demerits of cooperative spectrum sensing include:

i. It is inefficient when different types of CRs are involved.

ii. Communicating with all CRs through the control channel is the major impediment in cooperative spectrum sensing.

Since CSS solves the problem of hidden node, shadowing, fading and achieves high gain in the capacity of sensed spectrum as well as achieving detection at reduced time duration, it was therefore selected in this work.

2.4.3 Interference-based spectrum sensing

Interference-based spectrum sensing method shown in Figure 2.8 is applicable in CR because secondary signal is not allowed to interfere with the PU signal. Since each PU has interference temperature limit that guarantees certain quality of service, CR measures the interference environment and adjusts its transmission such that the interference to PU is not above the regulatory limits. In interference-based spectrum sensing, interference takes place at the receivers but can be controlled at the transmitter through the out-of-bound emissions, radiated power and location of individual transmitters. The major drawback of the interference-based spectrum sensing is its inability to measure the interference temperature at the primary receiver (Maninder *et al.*, 2016).

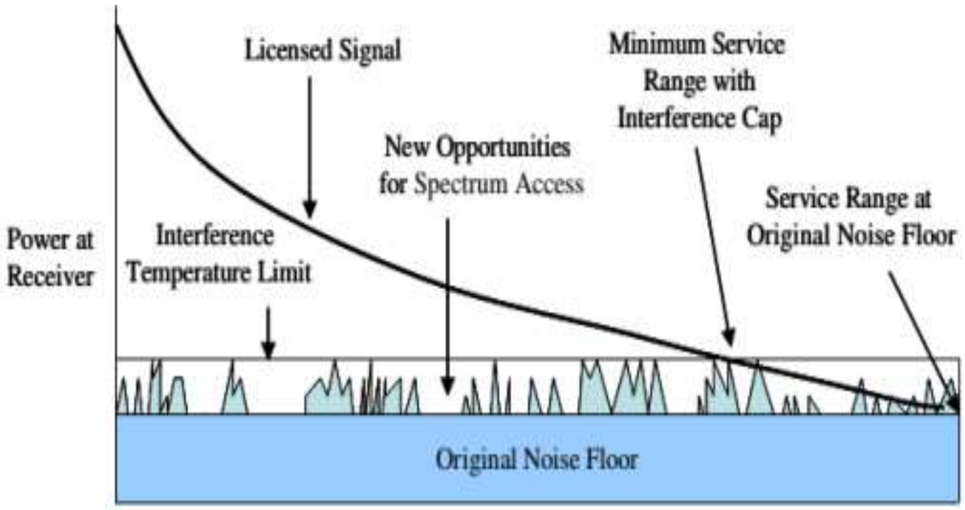

Licensed Signal
Minimum Service Range with Interference Cap
New Opportunities for Spectrum Access
Service Range at Original Noise Floor
Power at Receiver
Interference Temperature Limit
Original Noise Floor

Figure 2.9: Interference Based Spectrum Detection (Maninder *et al.*, 2016)

2.5 Background to Security Threats in Wireless Networks

Wireless networks are faced with various security issues. These security issues can be classified according to how they manifest on protocol stacks and its five layers.

2.5.1 Threats in physical layer

The attacks common to physical layer are primary user emulation attack (PUEA), objective function attack, common control data attack, and jamming. In PUEA, the PUE emulates the signal of the PU thereby making the SU to see the transmitter as the PU. In jamming, attacker continuously sends data packets to the channel, thereby making it impossible for SU to sense the channel as idle. Common control data attack prohibits channel components from sharing spectrum usage information by disturbing transmission process. It further feeds the attacker with all the information needed for spectrum sensing. In objective function attack, the attacker continuously changes its parameters so that it becomes impossible for the secondary user to adapt successfully. Physical layer attacks are the most challenging to deal with. And with particular emphasis on CR networks, PUEA is the most challenging one (Muñoz*et al*., 2020b). This attack is possible because of the flexibility enabled by software based air interface of CR.

2.5.2 Threats in link layer

The transfer of data from one node to another is done at link layer. Attacks common to this layer are three: Spectrum Signal Data Falsification (SSDF), Selfish Channel Negotiation (SCN) and Control Channel Saturation Denial of Service (CCSDoS). In SSDF (also known as byzantine attack), the malicious node sends wrongly sensed spectrum results, which leads to inaccurate decision by the fusion centre. The SCN attack occurs when malicious nodes provide wrong channel information to change the route of the node. On the other hand, CCSDoS occurs when the attacker reserves the control channel and in turn gets it saturated.

2.5.3 Threats in network layer

Two types of attacks peculiar to this layer are sink hole and Hello Flood Attack (HFA). Sink hole attack is the attack in which attacker claims to be the most appropriate route to a particular destination, with the intention that packets sent through it is discarded while malicious packets are passed on. HFA occurs when the transmitting power of the broadcast message sent to all the nodes in the network by the attacker is so convincing to the point that it can claim to be the closest neighbour in the network of those nodes.

2.5.4 Threats in transport layer

Transfer of data between two end hosts occurs in the transport layer. Two types of attacks common to this layer are lion attack, where PUEA is launched by the attacker to force the CR nodes to undergo frequency hopping among the channels so as to disturb transport control protocol (TCP). The second attack common to transport layer is jelly fish attack. Although jellyfish attack is a network layer attack, it impedes optimum operation of the transport layer.

2.5.5 Threats in application layer

The attacks related to the four preceding layers are inimical to the application layer. They all have adverse effects on application layer in various ways. Hence, attacks on various other layers of the protocol stack should be avoided for proper functioning of the application layer.

2.5.6 Security objectives for the wireless network

To be able to secure wireless network, network's resources should only be available as and when required by the individuals, as well as the devices concerned. Moreover, only authorized individuals and devices should access the networks resources. Unauthorized individuals should be denied access; otherwise, an attacker can easily manipulate SUs and successfully launch its attacks. Similarly, network data should be confidential to the point that no unauthorized user can read such network data because, if every node including the mischievous node is able to understand the network data, it can easily be attacked. In the same vein, changes in data during transmission should be known to the participating nodes. Thus, all changes (intentional/unintentional) occurring in the data during transmission must be detectable for possible avoidance.

2.6 Primary User Emulation Attack

Topmost of the security issues threatening the successful operation of CRNs is the PUEA (Sultana & Hussain, 2018; Haji *et al.*, 2020). PUEA denotes a situation whereby SU mimics a PU's signal for selfish or malicious purposes(Sharifi *et al*., 2015). PUEA is possible since CR is a highly reconfigurable device due to its software-based air interface (Lin & Wen, 2016; Fihri *et al*., 2018). One of the greatest challenges of distinguishing (PUE) from Primary user (PU) is the fact that FCC specified that *"no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum by secondary users"*(Federal Communications Commission 03-322, 2003*;*Chen & Park, 2006; Ghanem *et al*, 2016). Thus, equipping PU's signal with signature or using an interactive protocol between an incumbent signal transmitter and a verifier is not an option. FCC also ruled that there should be physical security of the PUs in primary exclusive region (Federal Communication Commission, 02-135, 2002).

2.7 Classification of Primary User Emulators

There are different types of PUEs in literature (Marinho *et al*., 2015; Yu *et al*., 2015; Fauzi & Khan, 2017) and they are classified as follows:

i. Selfish primary user emulator

ii. Malicious primary user emulator

iii. Power-fixed primary user emulator

iv. Static primary user emulator

v. Mobile primary user emulator

2.7.1 Selfish primary user emulator

Selfish PUE is often carried out by two attackers. The aim is to establish dedicated links, to transmit without allowing other SUs to have access to the same fallow spectrum bands.

2.7.2 Malicious primary user emulator

Malicious primary user emulation attack impedes the Opportunistic Spectrum Sharing (OSS) process of the SUs by preventing them from detecting and using PU's spectrum holes. A malicious PUE mimics the PU's signal features and launch a jamming signal when the PUs is not using the spectrum band. The malicious PUE transmits in idle bands during PUEA in other to deny the SUs from accessing the white space and not to interfere with the PU. Unlike the selfish PUE, the malicious PUE obstructs opportunity spectrum sharing (OSS) in several bands concurrently by using:

i. Waiting time for SU to be sure the band is vacant.

ii. During spectrum handoff

2.7.3 Power-fixed primary user emulator

A power-fixed attacker launches its attacks by using a predefined invariable power level that is independent of the PU's power. Such an attack has the capability of defeating any defensive approach that depends mainly on the power of the received signal. Since most SUs use energy detection for sensing spectrum, it becomes easy for PUE attackers to mimic power level of PU.

2.7.4 Static primary user emulator

Static attacker maintains fixed location in all rounds of attacks. Location techniques such as dedicated positioning sensors, angle of arrival or time of arrival are used to reveal this location. It can easily be detected using the difference between its location and that of PU.

2.7.5 Mobile primary user emulator

Unlike static PUE, mobile PUE is not static. This makes localizing mobile PUE more difficult when compared to static PUE. This implies that the algorithm for localizing mobile primary user emulator is more complex than that of static primary user emulator.

2.8 Conditions for Successful Primary User Emulation Attacks

The following are the conditions that make PUE attacks on CRN successful (Ammar *et al.*, 2015):

i. No primary user-to-secondary user interaction

ii. Different characteristics of PU and SU signals

iii. Channel measurement and primary signal learning

iv. Avoiding interference with the primary networks.

2.9 Impacts of Primary User Emulators on Cognitive Radio Networks

PUE is responsible for most severe security challenges faced by CRNs. The following are possible effects of PUE attacks on CRNs (Ammar *et al*., 2015; Yu *et al*., 2015; Sultana & Hussain, 2018; Srinivasan *et al*., 2019).

i. **Quality of service (QoS) Degradation:** PUEA results in discontinuity of secondary services, as a result, it causes recurrent spectrum handoff which leads to delay and jitter.

ii. **Bandwidth Wastage:** CRN was deployed to tackle the problem of spectrum underutilization caused by permanent spectrum allocation policy. However, the spectrum hole is often time stolen by PUE, which results in spectrum bandwidth waste.

iii. **Connection Unreliability:** PUEA in CRN greatly increases unreliability in the CRN connection. With the presence of PUEA, there is no guarantee of service as a result of frequent spectrum handoff, under which the SU may not find available channel.

iv. **Interference with the Primary Network:** There is a possibility of interference with the primary network if PUE fails to accurately detect the presence of PU.

v. **Denial of Service (DoS):** As a result of the high frequency with which PUE attacks occur, SUs will not find channels for their transmission. In this case, they will be denied access to the network.

2.10 Primary Exclusive Region

This is the area beyond which Secondary users must not go closer to primary transmitter. Primary exclusive region (PER) is also called keep-out-region. The keep-out-region for various TV transmitters are as shown in Table 2.2

Table 2.2: Keep-out-regions from TV Transmitter

TV Transmitter	Keep-out-region
Digital Television	132 km
Customer Premise Equipment	142 km
Base Station	155 km

Source: (Kang, 2009).

2.11 Review of Detection Schemes for Primary User Emulation Attacks

Primary user emulation attack affects successful operation of CRN. Hence, it is necessary to curb its activities on the CRN. With the specification of the FCC which states that there should be physical separation between SUs and PUs, localisation of the attacker is the best way to detect PUE. Localisation is the estimation of the spatial coordinates of a node as accurately as possible. There are two broad categories of localisation: Range-free localisation and Range-based localisation.

2.11.1 Range-free localisation scheme

This method does not make use of distance, angle estimation or other special hardware. Here, nodes communicate with each other to find out their respective distance. It is not highly accurate, but less expensive and less complex (Shakshuki *et al.*, 2019).

2.11.2 Range-based localisation schemes

Range is the distance within which something can be reached or received. Range-based localisation algorithms estimate the distance and angle between sensor nodes. The algorithms compute the distance between nodes and use the principle of geometry to calculate the location for the same nodes. These algorithms are employed to compute range metrics such as angle in Angle of Arrival (AOA) and distance in Time of Arrival (TOA), Time Difference of Arrival (TDOA) and Received Signal Strength (RSS). When implementing any localisation technique, certain parameters such as accuracy, cost, energy efficiency, and size of the hardware, should be considered as they show similarities and differences between various approaches (Kumar & Singh, 2016; Shakshuki *et al*., 2019).

2.11.3 Concepts used in range-based localisation

Several concepts are used in range-based localisation. They include triangulation, lateration, angulation, trilateration, multilateration and angulation.

Triangulation is the use of geometry of triangles to estimate the position or location of an object or a person. Triangulation is classified into lateration and angulation. Lateration is the estimation of distance between nodes. Trilateration is the estimation of the position of un-localised node by computing the distance from three nodes through intersection of three circles, which gives a single point that will eventually be the position of the un-localised node. Trilateration method is used to find the location of the sensor node when the distance is being calculated. Although this method has high accuracy, it requires more than three nodes for its location estimation and consumes a lot of power.

Typically, angulation is the means by which the location of the node is determined by considering the angle between the nodes. While triangulation is the means by which position of the un-localised node is computed by measuring at least two angles of un-localised node from two localised nodes (Khudhair *et al*., 2016).

2.11.4 Range-based localisation techniques

The different categories of Range Based techniques are:

i. Time of Arrival

ii. Time Difference of Arrival

iii. Angle of Arrival

iv. Received Signal Strength

2.11.4.1 Time of arrival

The velocity of a radio signal and the time lapse between when the signal was transmitted by the transmitter and the time it reaches the receiver is used to calculate the position of the receiver. Upon the receipt of signal by a receiver, it sends it back to the transmitter. The time lapse and the preset speed are used to compute the position of the receiver (Li *et al.*, 2016). Figure 2.10 is the typical two-dimensional localisation using time of arrival (TOA).

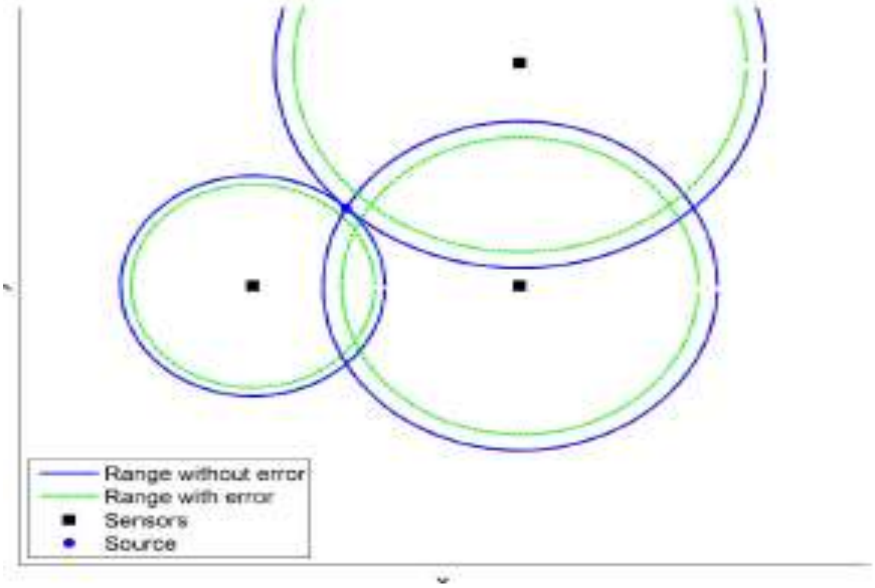


Figure 2.10: Typical two-dimensional Localisation Using Time of Arrival

A node *m* estimates its distance from its neighbour *n* by using (2.4):

$$Dis_{mn} = 2^{-1}\left(vt^{m}{}_{rec} - vt^{m}{}_{tra}\right) - \left(vt^{n}{}_{rec} - vt^{n}{}_{tra}\right) \tag{2.4}$$

where,

Dis_{mn} is the distance between *m* and *n*,t_{rec}^{m} denotes the time signal was received at node *m*, t_{tra}^{m} indicates the signal was transmitted from node *m*, t_{rec}^{n} signifies the time the signal was received at node *n* and t_{tra}^{n} is the transmission time of signal from node *n* while *v* denotes velocity of the radio signal.

The source localisation for 3D using TOA is (Li *et al*., 2016):

$$vt_{i} = \left[\left(x - x_{i}\right)^{2} + \left(y - y_{i}\right)^{2} + \left(z - z_{i}\right)^{2}\right]^{1/2} \tag{2.5}$$

where,

v is the signal propagation speed, t_i gives the signal travelling time to the receiver from the source *i*. The position of the receiver *i* in space is represented by x_i, y_i, z_i. The position of the node to be determined is *x*, *y*, *z*.

The general Linear Least Square (LLS) and Maximum Likelihood (ML) cost functions for TOA measurements are respectively given as:

$$J_{TOA} = \sum_{i=1}^{N}\left(t_{i}s - \| X - x_{i} \|\right)^{2} \tag{2.6}$$

and

$$J_{TOA} = \sum_{i=1}^{N}\frac{\left(t_{i}s - \| X - x_{i} \|\right)^{2}}{\sigma_{i}^{2}} \tag{2.7}$$

where,

J_{TOA} denotes cost function for TOA, t_i represents time of transmission and X is the position of the transmitter while x_i position of the receivers. σ_2 signifies variance i^{th} receiver whereas N is the number of receiver.

TOA has two main limitations which are:

i. Inability to match all receivers at microsecond: This problem is overcome with the application of roundtrip propagation time which computes the difference between when the signal sent from a transmitter to the receiver is sent back to the transmitter by the receiver.

ii. Internal delay by the transmitter also affects accurate computation of position of the receiver. Moreover, it is required that the node to be detected cooperates with other nodes. Therefore, TOA cannot be used to localise an attacker as it will not cooperate with other nodes.

2.11.4.2 Time difference of arrival

Time Difference of Arrival (TDOA) was developed to overcome the limitations of Time of Arrival (TOA). It computes the location of a node by using the difference of arrival time of the radio and ultrasound signals at different nodes. Each node has microphone and speaker. When anchor node sends signal to other nodes, it waits for some time lapse before generating chirps with the help of a speaker. The microphone saves the time it identifies the chirps. Unlocalised node utilizes this time information to estimate how far it is from the anchor node. Figure 2.11 is the schematic diagram of two-dimensional localisation using TDOAs.

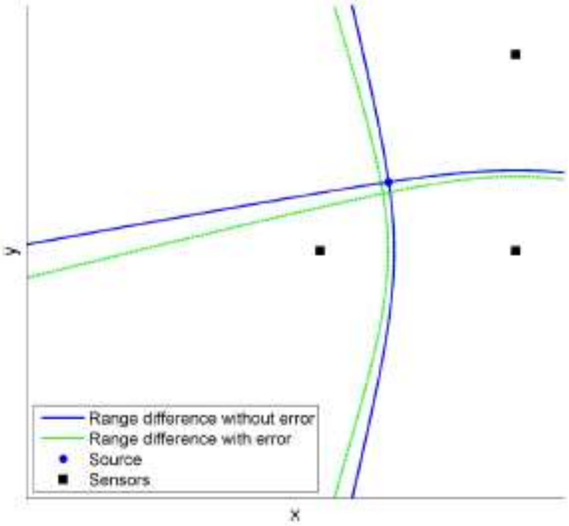


Figure 2.11: Schematic Diagram of Two-Dimensional Localisation Using TDOA

For two references, *m* and *n* the TDOA measurement can be transformed into a distance by (2.5) (Li *et al*., 2016; Ghanem *et al*., 2016):

$$Dis_{mn} = dis_{m} - dis_{n} = c(t_{m} - t_{n}) = c.t_{mn} \qquad (2.8)$$

Dis_{mn} is distance between references *m* and *n*. *c* represents the speed of sound, t_m is the time sound travels from the transmitter to the reference node *m* while t_n denotes the time signal is received at reference node *n.*

The source localisation for 3D using TDOA is (Li *et al*., 2016):

$$v\Delta t_{ij} = \left[\left(\left(x-x_i\right)^2+\left(y-y_i\right)^2+\left(z-z_i\right)^2\right)\right]^{1/2} - \left[\left(x-x_j\right)^2+\left(y-y_j\right)^2+\left(z-z_j\right)^2\right]^{1/2}, \qquad (2.9)$$

$i,j=1,2\ldots\ldots\ldots.,N$

where,

v is the signal propagation velocity, t_i is the time signal transverses between the transmitter and receiver *i*, Δt_{ij} denotes the time difference in travelling times t_i and t_j.

The location of the transmitter *i* is represented by(x_i, y_i, z_i) while that of the receiver is (x, y, z). The general Linear Least Square (LS) and Maximum Likelihood (ML) cost functions for TDOA measurements are respectively given as (Li *et al*., 2016):

$$J_{TDOA} = \sum_{i=2}^{k} \left(\left(t_i - t_j \right) s - \| X - x_i \| + \| X - x_j \| \right)^2 \qquad (2.10)$$

and

$$J_{TDOA} = \sum_{i=2}^{k} \frac{\left(\left(t_i - t_j \right) s - \| X - x_i \| + \| X - x_j \| \right)^2}{\sigma_{d,i}^2} \qquad (2.11)$$

where,

k is the number of the participating nodes $(k \geq 4)$. J_{TDOA} denotes cost function for TDOA, t_i represents time of transmission and *X* is the position of the transmitter, while x_j position of the j^{th} receivers. σ_2 signifies variance of i^{th} receiver whereas *N* is the number of receiver.

Although time difference of arrival (TDOA) localisation method has higher accuracy and precision, it requires extra hardware which makes it more complex and expensive.

2.11.4.3 Angle of arrival

As a localisation technique, Angle of arrival (AOA) utilizes angular measurements to detect a node. If orientation of the angular measurement is 0^0 and points to the north, it is absolute AOA, otherwise it is a relative AOA. Because AOA requires extra wares, it is highly expensive to deploy. However, it is highly accurate in localizing a node (Khudhair *et al*., 2016).

AOA $\theta_{k,i}$ measured from node *k* to node *i* expressed as:

$$\theta_{k,i} = \alpha_{k,i} + n_{k,i} \tag{2.12}$$

where,

$\alpha_{k,i} = \arctan\left(\frac{x_k - x_i}{y_k - y_i}\right)$ gives the actual AOA at node *i* from node *k*

$n_{k,i}$ is the noise

On gathering angular measurements from all the nodes, we have the following equation:

$$\theta = \alpha + n \tag{2.13}$$

where,

θ is a matrix showing all AOA measurements, α is the actual AOA measurement while matrix n represents the noise of the AOA measurements with variance σ^2.

2.11.4.4 Received signal strength

RSS-based localisation techniques arise from the fact that there exists a strong connection between the distance of a wireless link and RSS. If the signal travels a distance, d, its signal strength is inversely proportional to the square of the distance travelled.

$$RSSI \, \alpha \, \frac{1}{d^2} \tag{2.14}$$

This method is not very accurate due to the uncertainties of the communication channel. But it is less expensive, and easy to deploy.

Two challenges are common with RSS-based method of localisation:

i. Manipulation by rogue nodes.

ii. Inconsistency in the received signal strength.

These challenges are surmountable by carefully processing several received power. Typically, RSS value decreases as the distance between transmitter and receiver increases. As such, if a group of receivers in a large network is able to collect sufficient number of received signal strength measurements, the location with the highest value of RSS is the location of the transmitter. The advantages of this method are:

i. It prevents modifying PU's signal

ii. It allows localizing multiple transmitters that transmit signal concurrently.

iii. RSS requires no cooperation with other participating nodes to accurately detect unlocalised node.

RSS operates on three radio signal propagation models which are Log-distance model, free space propagation model and two-ray ground model (Chen *et al.*, 2008b).

i. Free Space Propagation Model

The received signal power, p_{rec}, is related to distanced$d$ (2.15):

$$p_{rec} = k_f \frac{p_{tra}}{d^2} \tag{2.15}$$

where,

P_{rec} is the received signal, k_f is a constant that depends on transceiver characteristics, P_{tra} is the transmitted power, while $d$is the distance between the transmitter and the receiver. With this model it is assumed that there is no signal attenuation in the transmission channel.

ii. Two-Ray Ground Model

Direct communication ray and reflected ray are the two rays a two-ray ground model receives. Two-ray model is given by:

$$p_{rec} = k_f \frac{p_{tra}}{d^4} \tag{2.16}$$

iii. Log-distance Model

The mathematical expression for Log-distance model is:

$$p_{rec}\alpha \frac{p_{tra}}{d^n} \tag{2.17}$$

where,

n represent loss exponent, p_{rec} is the received power and p_{tra} is transmitter signal power whereas *d* is the distance between the transmitter and the receiver.

Another formula that relates received power to distance is the case of one metre reference distance. It is given as:

$$RSS = 10.\mathrm{m}.\log_{10}(d) + B \tag{2.18}$$

where,

d is transmitter-to-receiver distance, *B* is RSS value measured by a receiver that is located one metre from a transmitter and *m* is the actual value of *RSS* measured at distance, *d.* Whereas Table 2.3 is the comparison of ranged-based localisation schemes, Table 2.4 presents suitability/unsuitability of the range-based localisation schemes for the detection of PUEs in CRNs.

Table 2.3: Comparison of Range-Based Localisation Methods

Method	Size of	Accuracy	Computational	Precision	Cost	Energy

	Hardware		Complexity			Efficiency
TOA	Large	Low	High	High	High	Low
TDOA	Large	High	High	Low	High	High
AOA	Large	High	High	High	High	Low
RSSI	Small	Low	Low	Low	Low	High

Source (Li *et al.*, 2016)

Table 2.4: Suitability of Range-Based Schemes for Localizing PUE in CRN

Scheme	Suitability	Reason
TOA	Unsuitable	- Cooperation of the attacker is required. And PUE will not cooperate with other SUs. -Synchronization problem.
TDOA	Unsuitable	-It does not require cooperation of attackers. -Inability to handle tight synchronization among participating nodes.
RSS	Suitable	-It is applicable without cooperation among the participating nodes.
AOA	Suitable	-Cooperation of other nodes is not needed.

Source: (Li *et al.*, 2016)

2.12 Review of Related Works

In the work of Chen *et al.* (2008b) PUE attacks in hostile cognitive radio (CR) environment was identified and localised but consideration was not given to mobile and low power transmitter. Hence, this technique is not applicable in mobile cognitive radio network.

Similarly, Penna and Cabric (2013) used direction of arrival of signal to detect the primary user. Each sensor was equipped with antenna that enabled higher localisation accuracy. Equipping all the sensors in the network with antenna is highly expensive.

However, optimally positioned sensors that are equipped with antennas also localise the primary users with higher accuracy but it would be less expensive.

In a related development, Chunsheng and Song (2014) used signal features such as active and idle periods of the PU to identify primary user emulation attacks (PUEAs) in CRNs without prior knowledge of primary user (PU). Although it is applicable in every type of primary user, it cannot classify Signal Activity Pattern (SAP) when multiple PUs are present in the CRN.

Advanced Encryption Standard (AES) was used in Ahmed *et al*. (2014) to detect PUE in CRNs. Since no additional hardware is required, it is financially less expensive. It is highly efficient for spectrum sharing when applied directly to today's Digital Television (DTV). However, plug-in AES chip makes it complex. The plug-in AES chip can lead to compatibility issues with other hardware components.

In the work of Ammar *et al.* (2015), distance was measured based on location coordinate and received signal strength. It successfully ensures trustworthiness among nodes in cognitive radio network by distinguishing primary and malicious users. But it failed to consider RSS of varying frequency to localise transmitters at different locations.

In Chen *et al*. (2016), density function and signal propagation was user to detect PUEA. In this technique, secondary user (SU) does not need location information of the primary user to identify the PUE. Although it has the advantage of not requiring extra hardware, it has low accuracy since each SU carried out detection independently.

In the same vein, Mrabet *et al*. (2018) used detection technique based on Kalman Filter to detect mobile primary user by measuring the received energy at the secondary node. It considered free space propagation model. Therefore, it is not applicable in a cluttered environment. It could not find the initial location of the PU and it cannot detect attackers that are very close to the PU.

Khaliq *et al*. (2018) used location verification aided mean field game approach for detection of PUE. It also allows detection of attacks by each node without additional cost. With a mean field game approach SUs autonomously make detection decision. It can detect multiple PUE and can also be applied in a distributed manner but it cannot be implemented on vehicular CR ad hoc networks. Moreover, it did not consider other game theoretic approaches.

Recently, Haji *et al*. (2020) used sparse coding through Machine learning approaches to accurately detect PUE and jammer. This scheme only outperforms energy detection-based machine learning algorithms but it finds no application in other detection techniques.

Also, Vasanthareddy & Sanjeev (2021) used received power and angle at which the power was received to accurately detect PUEA. However, Inclusion of secured Harsh Algorithm (SHA) makes the algorithm complex, expensive and unable to isolate the detected PUE from the network.

2.13 Research Gap

From appendix A, hybrid localisation method (HLM) model using AOA and RSS has not been used to localise the primary user emulator (PUE). Moreover, based on the strengths of AOA (which include high accuracy and high precision) and that of RSS (which are: low computational complexity, low cost, high energy efficiency and small hardware) over other localisation schemes (as presented in Table 2.3) and their suitability for localising PUE (as presented in Table 2.4), they are adopted for hybridisation in this work.

Existing literatures show that Cooperative Spectrum Sensing (CSS) is classified into distributed and centralized spectrum sensing (Akyildiz *et al.*, 2011; Sharma & Sharma, 2017). In centralized spectrum sensing, a decision centre (DC) computes the accurate location of the transmitter and sensing schedule of each SU over a particular channel (Yang *et al.,* 2012; Treeumnuk *et al.*, 2013; Akhtar *et al.*, 2014; Ashokan & Jacob, 2017; Shrivastava *et al.*, 2018; Akbari *et al.*, 2018). This makes it more proficient than distributed spectrum sensing (Hajiabadi *et al.*, 2017; Verma *et al.*, 2018; Souza *et al.*, 2018).

Furthermore, to the best of our understanding, there has not been any work done in the area of using Cooperative Spectrum Sensing-based Hybrid Localisation Method (CSS-HLM) to accurately detect PUEs in CRNs. Thus cooperative spectrum sensing is adopted in section 3.4 of this work.

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Background to the Methodology

In this chapter, the methods used to detect primary user emulator (PUE) and isolate the detected PUE are presented. To address the problem of detecting PUE, the problem was approached from the perspective of hybridizing RSS and AOA methods of localisation. Furthermore, a technique was developed to isolate the detected PUE from the CRN. Computer simulation using MATLAB (2009) version 7.8.0.347 tool was used to obtain the results from these developed techniques.

3.2 Materials

In this research, Laptop (HP Elite Book 8440p with Core i7 & CPU m620@ 2.67GHz, installed memory of 4.00GB, 64-bit operating system, x64-based processor) and MATLAB (2009) version 7.8.0.347 was used to carry out the simulation.

3.3 Method

PUE poses a severe security challenge to the full deployment of CR. The implication is that the activities of PUE will lead to eventual collapse of CRN. Therefore, there is need to develop a fast, accurate and energy efficient technique to detect and isolate PUE from CRN.

3.4 Hybrid Localisation Method for Detection of PUE in CRNs

In this section, special attention was paid to detecting the PUE using the blend of Angle of Arrival (AOA) and received signal strength (RSS) schemes of localisation. Sections 3.4 give full description of the system model used and how it was achieved.

3.4.1 Hybrid localisation method model

Figure 3.1 presents cognitive radio network (CRN) model, which operates in television (TV) spectrum holes. It consists of the mobile switching centre (MSC), the secondary base stations (SBSs), the primary user (PU) transmitter, the secondary users (SUs) transmitter and the primary user emulator (PUE). Federal Communications commission (FCC) regulation requires that SUs should only operate outside primary exclusive region (PER). Hence, there is physical separation between SUs and the PU receiver (Xie *et al*., 2013). Furthermore, there should be a protected band that gives the minimum distance$d_{n(\Delta)}$, of SUs from the primary receiver. This is to shield the primary transmitter from finite interference. PER and$d_{n(\Delta)}$make up the no-talk-region as shown in Figure 3.1. SU should have the capability to estimate its location (Celebi& Arslan, 2007; Vu *et al*., 2009)and this information can be shared with other SUs. Consequently, SUs are conscious of their locations, as well as that of the PU and they use the location information to compute their individual distances from each other, from the PU and the relative angular measurement between each SU and the PU (Xie *et al*., 2013).

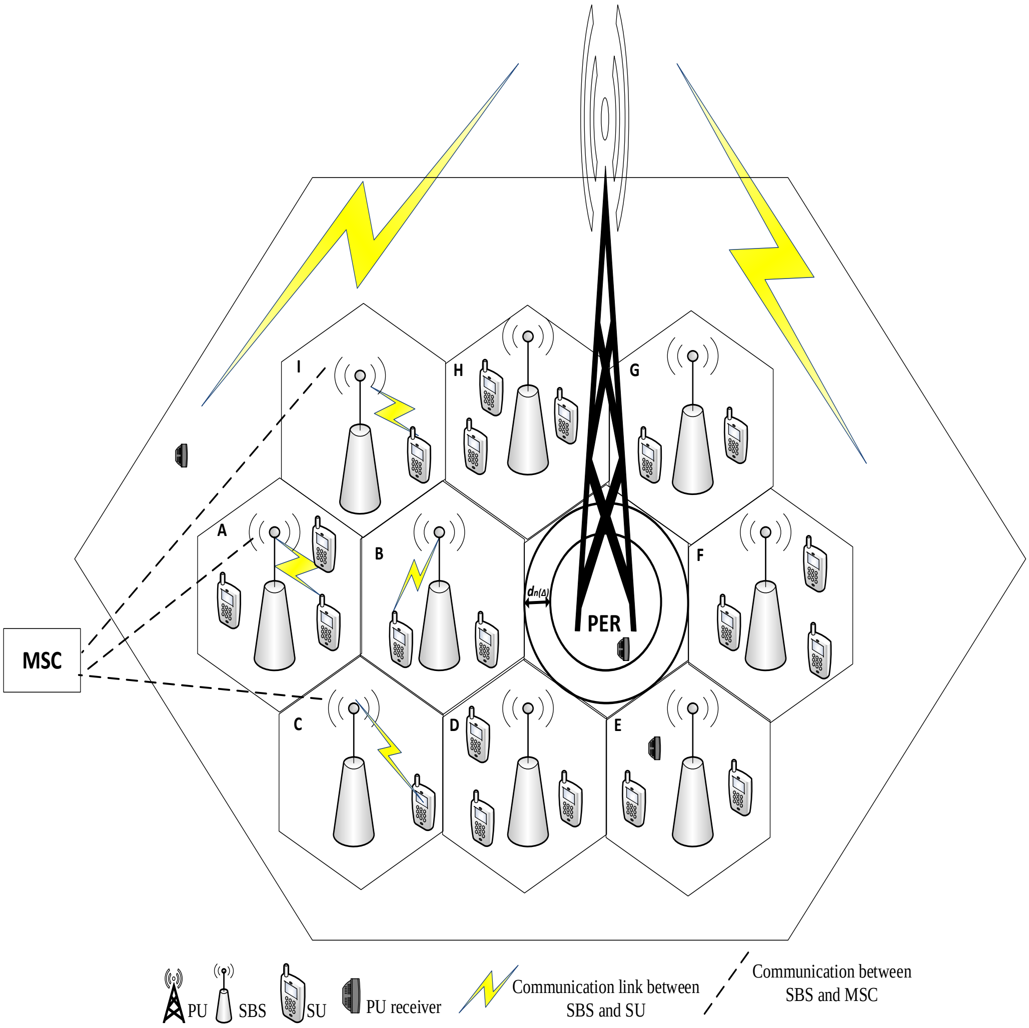

I
H
G
A
B
F
MSC
$d_{n(\Delta)}$
PER
C
D
E
PU
SBS
SU
PU receiver
Communication link between SBS and SU
Communication between SBS and MSC

Figure 3.1: Hybrid Localisation Method Model

3.4.2 No-talk region

Figure 3.2 portrays the no-talk-region, r_n. It comprises the primary exclusive region (PER)r_p, and extra safety band $d_{n(\Delta)}$ which halts SU's signal from interfering with the primary transmitter (Unnikrishnan & Veeravalli, 2008). SUs can communicate exterior of the no-talk-region given by (3.1) using (3.2) which is the equation that defines the white space (Faruk & Ayeni, 2013).

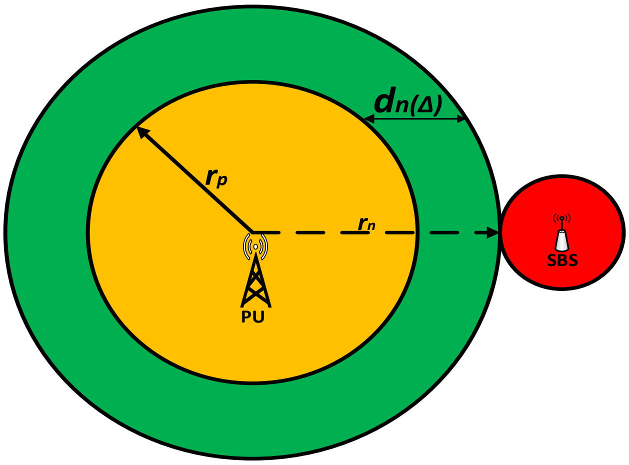


Figure 3.2: Digital Television PER and No-Talk Region

(Faruk & Ayeni, 2013)

$$r_n \in \Re \tag{3.1}$$

$$I_D : \Re \rightarrow \{0,1\} \tag{3.2}$$

(3.3) is the primary exclusive region, (3.4) is the extra safety band, and (3.5) is the no-talk-region.

$$r_p = l_p^{-1}\left(p_T + G - \psi(r) - N_0 - \lambda\right) \tag{3.3}$$

$$d_n(\Delta) = l_p^{-1}\left(p_T + G - \psi(r) - N_0 - \lambda + \Delta_i\right) \tag{3.4}$$

$$r_n(\lambda, p_T, h_t, \Delta) = r_p(\lambda, p_T, h_t) + d_n(\Delta) \tag{3.5}$$

where,

r_p represents the radius of the PER, $d_n(\Delta)$ gives additional protection from PER, the no-talk-region is denoted by r_n, Δ_i signifies the safety margin, path-loss is represented by *lp*, *Ψ(r)* indicates the fade margin, λ is wavelength, P_T, is the transmit power of the PU, N_o is the noise floor and h_t denotes antenna height while G represents antenna gain.

$$I_D\left(x, y, f, t\right) = \begin{cases} 1, & \text{if } x, y \in \Re \setminus r_n \\ 0, & \text{if } x, y \in \Re' \\ 0, & \text{if } x, y \in r_n \end{cases} \tag{3.6}$$

PUE (I_{PUE}) can communicate from the locations described by (3.7):

$$I_{PUE}\left(x, y, f, t\right) = \begin{cases} 1, & \text{if } x, y \in \Re \setminus r_n \\ 1, & \text{if } x, y \in \Re' \\ 0, & \text{if } x, y \in r_n \end{cases} \tag{3.7}$$

where,

(x, y) is the location of SU from where it transmits, *f* denotes the frequency of transmission, and *t* signifies the transmission time. I_D is the white space where SU can transmit.

3.4.3 Layout of the cognitive radio network

The layout of the CRN is shown in Figure 3.3. It consists of the no-talk region, primary user, secondary users, primary user emulators, and the coverage area of the primary user. The dimension of the layout in Figure 3.3 is 100 km x100 km.

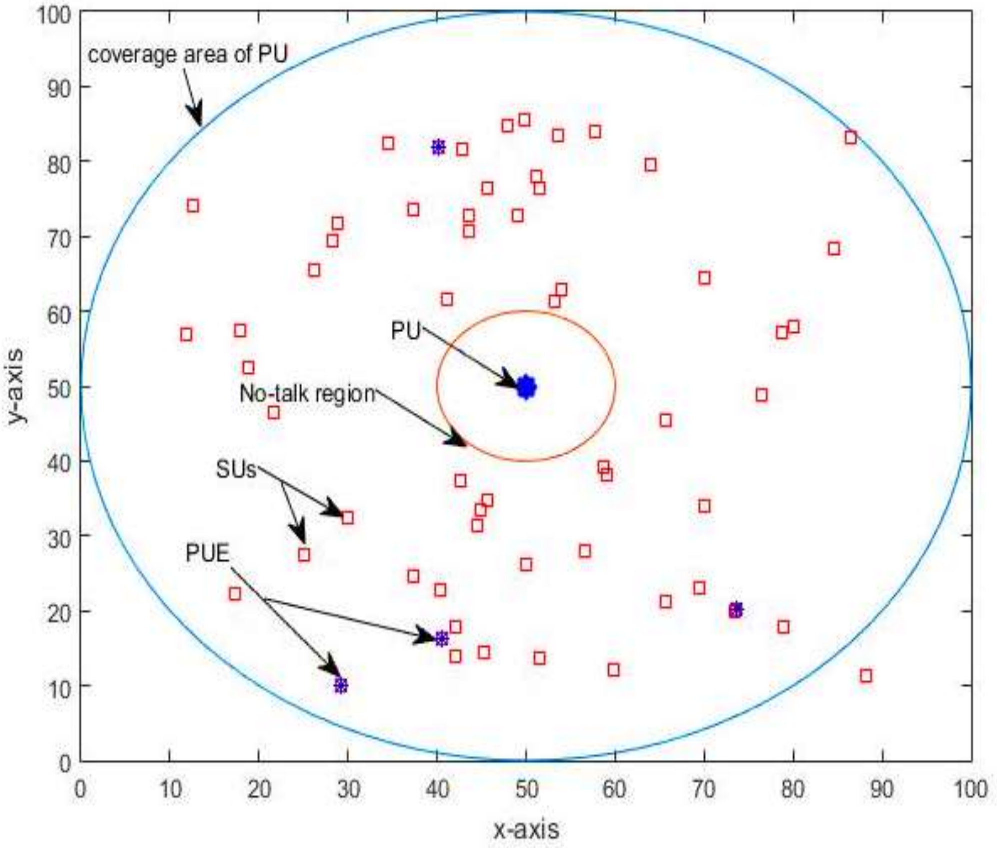


Figure 3.3: Layout of the Cognitive Radio Network

3.4.4 Hybrid localisation method model assumptions

The summary of assumptions upon which this work was based are as follows:

i. SUs are outfitted with directional antennas to calculate the AOA.

ii. The transmitter is physically separated from all SUs and the PUEs.

iii. Different received signal strengths are obtained at each SU.

iv. PUE is localised using two SU nodes.

v. Received signal strength at SU is used to estimate the Euclidean distance between the PUE and the SU.

vi. Each SU computes how far it is from PU and the angle at which it receives signal.

vii. SUs communicate among themselves via the SBS.

viii. SUs and PUEs are all non-static communication devices.

3.4.5 Hybrid localisation method model operation

When a signal is received, each SU estimates its distance and the angle at which the signal arrived from the transmitter. Each SU transmits the location information to the SBS within its cell, which then relays this information directly to the other SUs within that cell and to the SUs in other cells through their respective SBS through MSC. The estimated location of the signal transmitter is compared with the actual location of the legitimate PU and finally decides whether the transmitter is the legitimate PU or not (Leónet *al*., 2012; Piasana & Marchetti, 2014).

3.4.6 Primary user emulation attack scenario

A typical primary user emulation (PUE) attack setup is shown in Figure 3.4, where SUs in the network receive the transmitted signal from the PUE (Yadav *et al*., 2018).

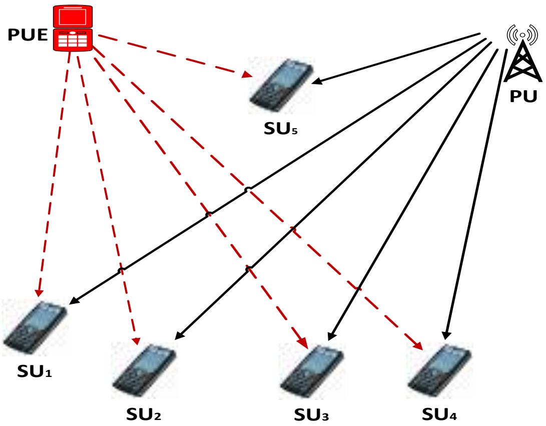


Figure 3.4: Primary User Emulation Attack Launching Scenario (Mergu, 2019)

In the localisation setup of the typical PUE shown in Figure 3.5, the locations of secondary user 1 (SU_1) is (x_1, $y_{1,}$) and that of secondary user 2 (SU_2), is (x_2, y_2). Similarly, the radius of coverage areas of SU_1 is r_1 and that of SU_2 is r_2. While (x_a, y_a)

and (x_b, y_b) represent the overlie points of the coverage areas of SU_1 and SU_2. Whereas angles ϕ and θ are the angles at which PU's signal was received at SU_1 and SU_2 respectively. PQ is the distance between the centres of SU_1 and SU_2. α_1 is the angle at which PUE's signal was received at SU_1 and α_2 is the angle at which PUE's signal was received at SU_2.

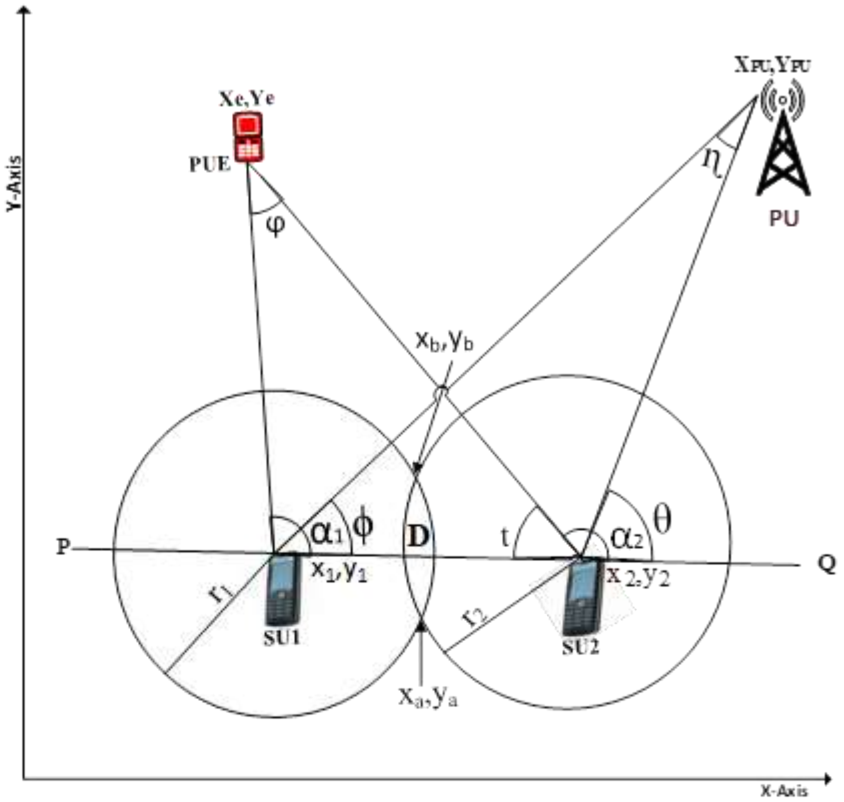


Figure 3.5: Localisation Process by Two SUs

The primary user (PU) is located at (X_{PU}, Y_{PU}), PUE is sited at point (X_e, Y_e) while SUs are(x_i, y_i) where, $i = 1, 2, \dots\dots..N$. D is the distance between the two SUs participating in the detection.

$$D = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \tag{3.8}$$

(3.9) to (3.13) give the intersection points, (x_a,y_a) and (x_b,y_b) of the two SUs that partake in localizing the PUE (Kumar & Singh, 2016).

$$X_a = \frac{x_1 + x_2}{2} + \frac{(x_2 - x_1)(\mathrm{r}_1^2 - \mathrm{r}_2^2)}{2D^2} + 2\delta(\frac{\mathrm{y}_2 - \mathrm{y}_1}{D^2}) \tag{3.9}$$

$$Y_a = \frac{y_2 + y_1}{2} + \frac{(\mathrm{y}_1 - \mathrm{y}_2)(\mathrm{r}^2{}_1 - \mathrm{r}^2{}_2)}{2D^2} - 2\delta(\frac{x_1 - x_2}{D^2}) \tag{3.10}$$

$$X_b = \frac{x_1 + x_2}{2} + \frac{(\mathrm{x}_2 - \mathrm{x}_1)(\mathrm{r}_1^2 - \mathrm{r}_2^2)}{2D^2} - 2\delta(\frac{y_2 - y_1}{D^2}) \tag{3.11}$$

$$X_b = \frac{x_1 + x_2}{2} + \frac{(\mathrm{x}_2 - \mathrm{x}_1)(\mathrm{r}_1^2 - \mathrm{r}_2^2)}{2D^2} - 2\delta(\frac{y_2 - y_1}{D^2}) \tag{3.12}$$

$$\delta = \frac{1}{4}\sqrt{(D + r_1 + r_2)(D + r_1 - r_2)(D - r_1 + r_2)(-D + r_1 + r_2)} \tag{3.13}$$

The distance, $d_{i(PU)}$ between the PU and i^{th} SU is given in (3.14)

$$d_{i(PU)} = \sqrt{(X_{PU} - x_i)^2 + (Y_{PU} - y_i)^2} \tag{3.14}$$

(3.15) gives the AOA of signal at SU$_1$ while (3.16) gives AOA of signal at SU$_2$

$$\phi = \tan^{-1}\left(\frac{Y_{PU} - y_1}{X_{PU} - x_1}\right) \tag{3.15}$$

$$\theta = \tan^{-1}\left(\frac{Y_{PU} - y_2}{X_{PU} - x_2}\right) \tag{3.16}$$

In a transmission environment with losses, the received power is estimated as

$$p_r = p_t - (\mathrm{Lo}\,ss_{shadowing} + Loss_{others}) \tag{3.17}$$

here,

$Loss_{shadowing}$ is loss due to shadowing and$Loss_{others}$is other losses in the communication environment while p_t is the transmitted power $p_r$is received power. Hence, the power received at i^{th} SU

$$\left(p_r\right)_i = p_t - p_{\mathrm{L}(d)} \tag{3.18}$$

where

$$P_L = L_{shadowing} + L_{others}$$

$$\left(p_r\right) = \begin{pmatrix} (p_r)_{1,1} & (p_r)_{1,2} & (p_r)_{1,3} & \cdots & (p_r)_{1,j} \\ (p_r)_{2,1} & (p_r)_{2,2} & (p_r)_{2,3} & \cdots & (p_r)_{2,j} \\ \vdots & \cdots & \cdots & \cdots & \ddots \\ (p_r)_{i,1} & (p_r)_{i,2} & (p_r)_{\mathrm{i},3} & \cdots & (p_r)_{i,j} \end{pmatrix} \tag{3.19}$$

But

According to Fihri *et al*.(2018) and Rappaport (2002),

$$p_{L(\mathrm{d})} = p_{L(\mathrm{d}_0)} + 10n\log_e\left(\frac{d}{d_0}\right) \tag{3.20}$$

By substituting (3.20) into (3.18), we obtain

$$d = \exp\left(\frac{p_t - p_r - p_{L(d\,0)}}{10n}\right) \tag{3.21}$$

where,

the transmit power of PUE is P_t, the received power at SU is Pr, the distance between SU and PUE is d, pathloss is denoted by $P_{L(do)}$ is the reference of 1m and loss exponent, n of 4, putting a typical urban environment into consideration.˙

Because of the dynamics of the communication environment, there are two issues that can affect the value of the received power:

Exploitation by rogue or several transmitters.

i. Inaccurate measurement of the received power.

These challenges can be tackled by averaging of several received powers.

Using (3.22), the average of multiple samples of the received power, P_r, is used to obtain a better estimate of the received power.

$$p_{r(iaverage)} = \frac{1}{N}\sum_{N=1}^{N} p_{riN} \tag{3.22}$$

Here, $P_{r(iaverage)}$ represents the average of the power received at the i^{th} SU and P_{riN} is the N^{th} sample value of the received power, P_r at the i^{th} SU in dBm. Substitute (3.22) into (3.21) to obtain (3.23):

$$d_i = \exp\left(\frac{p_t - p_{L(d0)} - p_{r(iaverage)}}{10n}\right) \tag{3.23}$$

(3.23) presents the distance separating the PUE from i^{th} SU

where,

d_i gives the distance between the transmitter and i^{th} SU, P_t represents the transmitted power from the transmitter, $P_{r(iaverage)}$ is the average power received at the i^{th} SU, n denotes the pathloss exponent which describes the propagation environment, while d_0 is the reference distance from which the line of sight propagation is assumed and $P_{L(d0)}$ typifies the pathloss at the reference distance.

In Figure 3.5, for SU_1 and SU_2 with distance D between them, the PUE is separated from SU_1 and SU_2 with distance d_1 and d_2 respectively. The angle of arrival (AOA) at SU_1 and SU_2 from PUE is expressed as:

$$\alpha_1 = arc\cos\left(\frac{D^2 + d_1{}^2 - d_2{}^2}{2Dd_1}\right) \tag{3.24}$$

$$\alpha_2 = 180 - t \tag{3.25}$$

where,

$$t = arc\cos\left(\frac{D^2 + d_2{}^2 - d_1{}^2}{2Dd_2}\right) \tag{3.26}$$

Hence,

$$\alpha_2 = 180 - \left(arc\cos\left(\frac{D^2 + d_2{}^2 - d_1{}^2}{2Dd_2} \right) \right) \tag{3.27}$$

The distance and AOA at SU$_i$ from PUE for two SUs used in the localisation of PUE, is given by

$$d_i\alpha_i = (s_i\varphi_i n_i) \tag{3.28}$$

d_i is the distance separating PUE and i^{th} SU, α_i gives the AOA of i^{th} SU from PUE and n_i is the noise in the distance, S_i and AOA, φ_i measurements.

Distance, d and AOA, α from PUE and S_i with φ_i corrupted with noise n at i^{th} position of SU are given in (3.29) and (3.30) respectively

$$d\alpha = \begin{pmatrix} (d\alpha)_{1,1} & (d\alpha)_{1,2} & (d\alpha)_{1,3} & \cdots & (d\alpha)_{1,j} \\ (d\alpha)_{2,1} & (d\alpha)_{2,2} & (d\alpha)_{2,3} & \cdots & (d\alpha)_{2,j} \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ (d\alpha)_{i,1} & (d\alpha)_{i,2} & (d\alpha)_{\mathrm{i},3} & \cdots & (d\alpha)_{i,j} \end{pmatrix} \tag{3.29}$$

$$s\varphi n = \begin{pmatrix} (s\varphi n)_{1,1} & (s\varphi n)_{1,2} & \cdots & (s\varphi n)_{1,j} \\ (s\varphi n)_{2,1} & (s\varphi n)_{2,2} & \cdots & (s\varphi n)_{2,j} \\ \vdots & \cdots & \ddots & \vdots \\ (s\varphi n)_{i,1} & (s\varphi n)_{i,2} & \cdots & (s\varphi n)_{i,j} \end{pmatrix} \tag{3.30}$$

$$Y_e - y_1 = \left(X_e - x_1\right)\tan\alpha_1 \tag{3.31}$$

$$Y_e - y_2 = \left(X_e - x_2\right)\tan\alpha_2 \tag{3.32}$$

$$X_e = \frac{x_1\tan\alpha_1 - x_2\tan\alpha_2 + y_2 - y_1}{\tan\alpha_1 - \tan\alpha_2} \tag{3.33}$$

$$Y_e = \tan\alpha_1\left(\frac{x_1\tan\alpha_1 - x_2\tan\alpha_2 + y_2 - y_1}{\tan\alpha_1 - \tan\alpha_2} \right) x_1\tan\alpha_1 + y_1 \tag{3.34}$$

Equations (3.33) and (3.34) give the location of the PUE.

The flow process of the hybrid localisation method is presented in Figure 3.6 while the algorithm for implementing the hybrid localisation scheme is presented in algorithm 3.1.

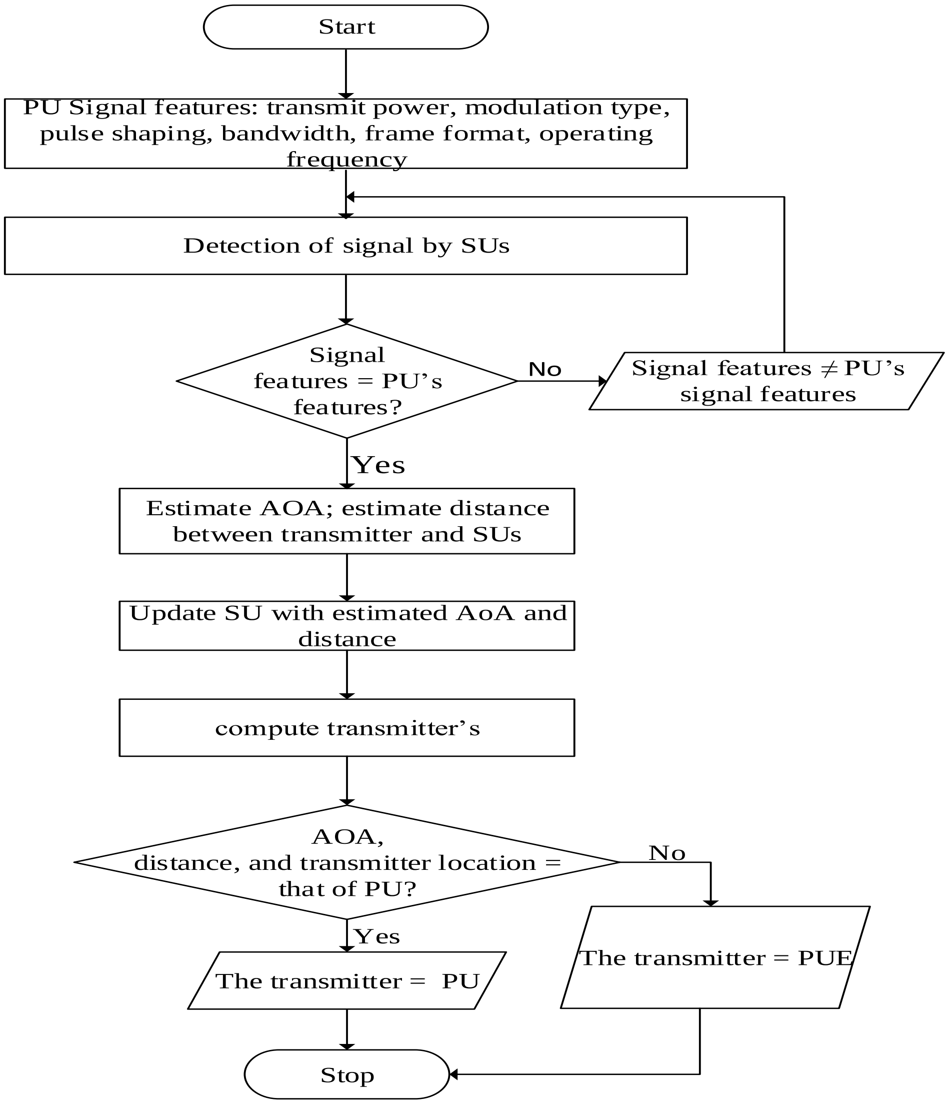

Start
PU Signal features: transmit power, modulation type, pulse shaping, bandwidth, frame format, operating frequency
Detection of signal by SUs
Signal features = PU's features?
No
Signal features ≠ PU's signal features
Yes
Estimate AOA; estimate distance between transmitter and SUs
Update SU with estimated AoA and distance
compute transmitter's
AOA, distance, and transmitter location = that of PU?
No
Yes
The transmitter = PU
The transmitter = PUE
Stop

Figure 3.6: Hybrid Localisation Flowchart

Algorithm 3.1: Hybrid Localisation

```
{
start
```

```
3   Input PU's signal characteristics = transmit power, bandwidth,
    pulse shaping, frame format, operating frequency, band
    modulation type
4   SU senses signal from unknown transmitter
5   SU extracts signal characteristics
6   If {
7         Signal characteristics ≠ PU's signal characteristics
8         transmitter ≠ PU
9   Go to step 1
10  Else
11  Go to step 12
12  Estimate $AOA_i$
13  Estimate Euclidean distance, $d_i$
14  Estimate $loc_i$
15  If {
16  $AOA_i$, $d_i$ and $loc_i$ of the transmitter = $AOA_i$, $d_i$ and $loc_i$ of the PU
17  Then
18         Transmitter = PU
19  Else
20         Transmitter = PUE
21                                                   }}
22       End
23  {
```

To evaluate the performance of the hybrid localisation scheme, comparison was made between estimated locations and the actual location of the PU using the root means square error (RMSE). Low RMSE signifies better performance.

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(\left(L_{est}\right)_i - \left(L_{real}\right)_i\right)^2} \qquad (3.35)$$

where,

L_{est} is estimated coordinate, L_{real} is the actual coordinate and N is the number of estimations.

3.4.7 Simulation of hybrid localisation method

The simulation for the hybrid method was carried out using MATLAB (2009) version 7.8.0.347. The layout of the CRN which is the simulation layout is shown in Figure 3.3.

The PU transmitter was fixed at (X,Y) (50,50) on a network area of 100km by100km, while the PUE and SUs were distributed randomly in the network. SU_1 and SU_2were respectively at initial positions of (x_1, y_1) (19, 22) and (x_2, y_2) (24, 23). The no-talk-region has radius of 10km, while coverage area of PU is 50m. PUE's transmit power was 20dBm, the loss exponent, n, was set at 4. The path loss within the reference distance, d_o, of 1m was set at 1dBm (Rappaport, 2002).

3.5 Cooperative Spectrum Sensing-Hybrid Localisation Method

PUE's detection in CRNs using fusion of RSS and AOA localisation method was achieved in section 3.4. Because localisation significantly depends on the received signals from a prospective PUE, it is tricky to accurately localise PUE as its signals have been sternly affected by various attenuation factors (Ashokan & Jacob, 2017). Consequently, to mitigate such effects, cooperative spectrum sensing (CSS) has been adopted. Here, SUs collaborate to make decisions concerning the presence or absence of PUE.

3.5.1 Cooperative spectrum sensing-hybrid localisation method model operation

The model to study the effects of cooperative sensing on the hybrid of RSS and AOA localisation schemes for the detection of PUE in CRN is depicted in Figure 3.7. It comprises the SUs, PUE, secondary base station (SBS), a building, a tree, a hill, and a car. PUE is the transmitter, SUs are the receivers. The RSS at the SUs is affected by the obstacles (building, tree, hill, and car). RSS from PUE to SU_1 is affected by the building, RSS at SU_2 is affected by the tree, and RSS at SU_3 is affected by the hill while the car affects the signal strength received at SU_6. Even though no visible obstacle exists between SU_4, SU_5 and PUE, the RSS at SU_4 and SU_5 are not the same as the transmitted power due to atmospheric condition and differences in the distance separating them from the PUE.

Moreover, an SU may not receive signal from PUE as a result of hidden node and receiver uncertainty (Fang *et al*., 2017). Hidden node problem occurs when an obstacle prevents an SU from detecting transmitted signal. To solve the problems above, centralized cooperative spectrum sensing is employed, with the SBS as the decision centre (DC) (Zhang & Lil, 2017). This model adopts parallel model of CSS which follows the three steps of local sensing, data reporting, and data fusion. DC makes the final decision from the reported data and broadcasts it to the selected pair which will participate in the localisation process. Finally, DC broadcasts localisation result to the entire SUs in the CRN after localisation is achieved. Since there is no information about the PUE signal, energy detection was adopted.

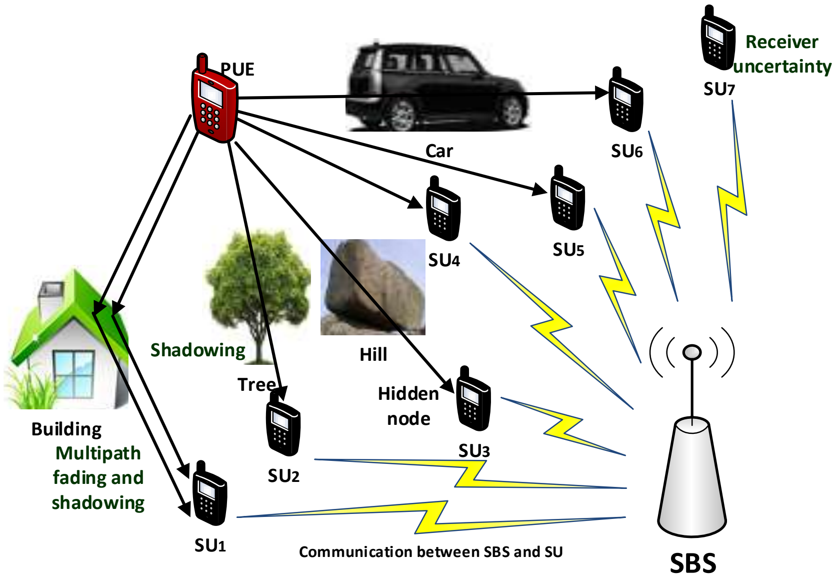


Figure 3.7: A Typical CRN with SUs, SBS and a Potential PUE

3.5.2 Application of energy detection in localizing primary user emulator

In energy detection, the test statistics *$T_i(X)$*, binary hypothesis testing *$x_i(m)$*, probability of detection, *P_{di}*, probability of false alarm (*P_{fi}*), and probability of miss detection, (*P_{mi}*) are given in (3.36) - (3.43) (Gupta *et al.*, 2016;Lin *et al.*, 2018).

$$T_i(X) = \frac{1}{k}\sum_{m=1}^{k}\left|x_i(m)\right|^2 \tag{3.36}$$

$$x_i(m) = \begin{cases} u(m) & ; H_0 \\ s(m) + u(m) & ; H_1 \end{cases} \tag{3.37}$$

m=1, 2, 3, ………*K* where *K* is the total number of received signal samples collected by SU. *$x_i(m)$* is the received signal at *i^{th}* SU. *i*= 1, 2, 3, …….*N*, while *s(m)* is the PUE signal. $s(m)$ has zero average with variance σ_s^2. The white Gaussian noise with zero mean is denoted as $u(m)$with variance of σ_n^2. *H_0* is a hypothesis describing absence of PUE and *H_1*denotes existence of PUE.

$$p_{di} = p\{T_i(X) > \lambda_i / H_1\} \tag{3.38}$$

$$p_{di} = Q\left(\frac{\lambda_i - (\sigma_s^2 + \sigma_n^2)}{\left(\sigma_s^2 + \sigma_n^2\right)/\sqrt{N/2}}\right) \tag{3.39}$$

$$p_{fi} = p\{T_i(X) > \lambda_i / H_0\} \tag{3.40}$$

$$P_{mi} = 1 - p_{di} \tag{3.41}$$

given, $Q(x)$ as general Q-function defined by (3.42)

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-\frac{t^2}{2}}dt \tag{3.42}$$

$$\lambda_i = \sigma_n^2 Q^{-1}(p_{fi}) / \sqrt{N/2} + \sigma_n^2 \tag{3.43}$$

SUs individually carry out detection of PUE and transmit their detection results to the FC with H_0indicating absence of PUE and H_1 indicating presence of PUE respectively.

3.5.3 Decision fusion

The Decision fusion (DF) plays a very crucial role in the second stage of CSS. It makes the final decision on the detection of the PUE from the detection results of the SUs in the CRN. If Λ denote the number of SUs that detect PUE, FC finally determines the presence or absence of the PUE from the report of the M participating SUs using the decision strategy γ(.) (Han *et al.*, 2010):

$$\gamma = \begin{cases} H_0, & \text{if } \Lambda < M \\ H_1, & \text{if } \Lambda \geq M \end{cases} \tag{3.44}$$

Final detection probability and final false alarm probability for different values of *M*are respectively given as:

$$p_d = \sum_{m=M}^{K} \binom{K}{m} p_d{}^m \left(1 - p_d\right)^{K-m} \tag{3.45}$$

$$p_f = \sum_{m=M}^{K} \binom{K}{m} p_f{}^m \left(1 - p_f\right)^{K-m} \tag{3.46}$$

If the cooperative function, $P = f(p)$ is the expression that the result of cooperative detection is *p*, the detection probability or false alarm probability at each SU is *P*. Combining (3.45) and (3.46) gives a uniform cooperative function given by

$$P = \sum_{m=M}^{K} \binom{K}{m} p^m \left(1 - p\right)^{K-m}$$

$$P = 1 - \sum_{m=0}^{M-1} \binom{K}{m} p^m \left(1 - p\right)^{K-m} \tag{3.47}$$

In Figure 3.8, we consider a decision centre (DC) portrayed secondary base station (SBS) that coordinates the cooperative spectrum sensing in the CRN. Sensing of PUE's signal is done by each secondary user (SU) and result is reported to the DC which fuses the data together to give final decision. The final decision is transmitted to the SUs subsequent to the conclusion of localisation with the aim to isolating the PUE. Communication between SBS and SUs during detection process is done below the noise floor of PU at very low transmit power to avoid possible interference with the PU.

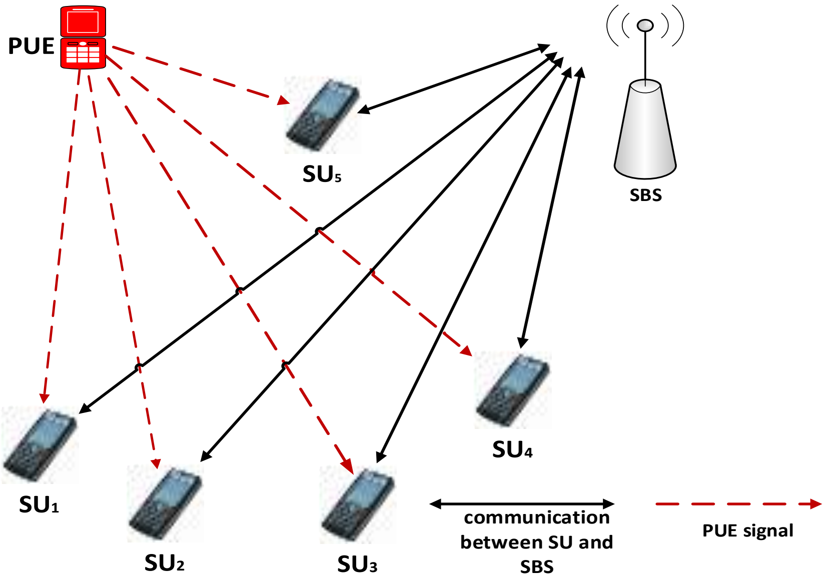
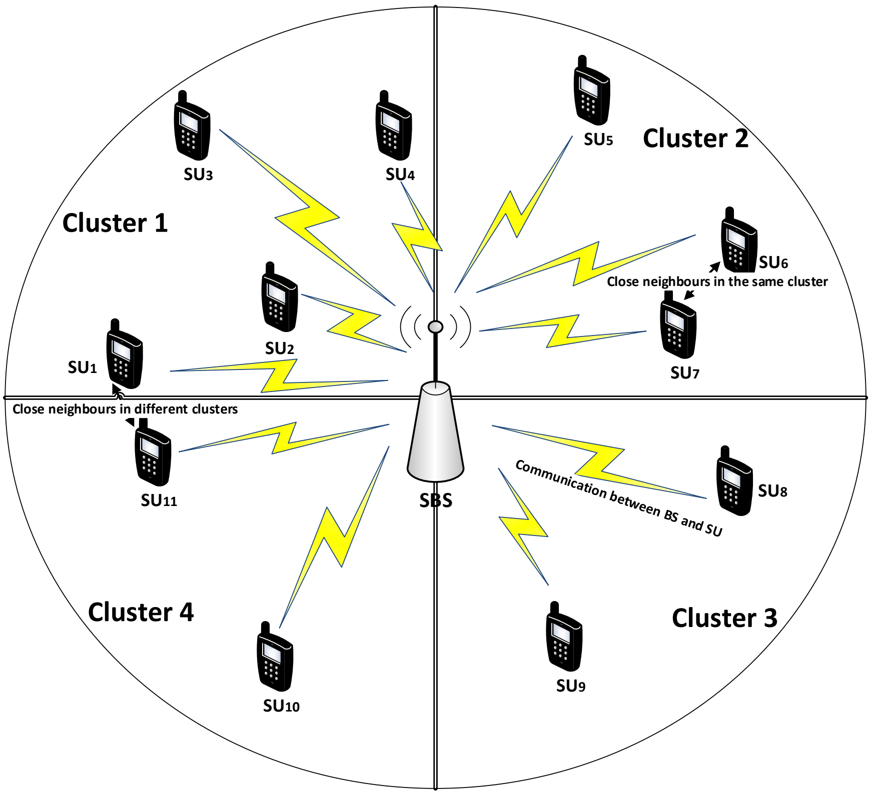


Figure 3.8: Cooperation of SUs to Detect a Potential PUE

As portrayed in Figure 3.9, the secondary base station (SBS) which is the decision centre (DC) forms four clusters where each cluster has different propagation environment. This results in SUs having similar RSS within a cluster and within close neighbouring clusters. Since distant clusters exhibit different communication environment, their SUs have variant RSS. SU_6 and SU_7 are closely related SUs within the same cluster (that is cluster 2) while SU_1 and $SU_{11}$are closely related SUs within different but neighbouring clusters (clusters 1 and 4).



SU3
SU4
SU5
Cluster 2
Cluster 1
SU6
Close neighbours in the same cluster
SU2
SU1
SU7
Close neighbours in different clusters
SU11
SBS
Communication between BS and SU
SU8
Cluster 4
Cluster 3
SU9
SU10

Figure 3.9: Cluster of SUs Around a SBS

3.5.4 Cooperative spectrum sensing-hybrid localisation method model assumptions

To realize Cooperative Spectrum Sensing-based Hybrid Localisation Method for the detection of PUEs in CRNs, the following assumptions were made:

i. Mobile cognitive radios are deployed within and around buildings, hills, cars, and other obstacles.

ii. Transmitted signal is mainly affected by scattering from surfaces or diffraction over and around buildings and other obstacles.

iii. All SUs' received power are from the same source

iv. Different values of signal strength are received at SUs

v. SUs in the same cluster experience the same environmental effects

vi. All SUs communicate directly with SBS and vice versa

vii. Communication among the SUs is via the SBS

viii. Secondary users (SUs) in the same cluster and the ones in the neighbouring clusters have closely related RSS

ix. Energy detection is used by SUs to sense the PUE's signal.

3.5.5 Cooperative spectrum sensing-hybrid localisation method model operation

RSS values are obtained at the time and point of localizing PUE. From RSS, distance between the transmitter and the SUs as well as the angle with which the signal arrives at SUs are obtained. HLM then uses distance and the measured angle to localise the primary user emulator (PUE). When they change position new pairs of SUs are selected based on their RSS to localise the PUE while discarding the former measurements. Two SUs are to be selected based on their received signal strengths (RSSs) on some received power interval [*0*, *w*] from a number, *N*, of SUs. Possible pairs to be selected are pair of SUs with maximum RSS, a pair of SUs with minimum RSS, a pair of SUs with medium RSS, a pair of SUs with one having highest RSS and the other with lowest RSS and a pair of SUs that have closely related RSS. The goal is to select the pair of SUs that enable the hybrid scheme to perform with higher accuracy, speed, and energy efficiency. Supposing all SUs received power from the same source (PUE), but they do not depend on each other, let $f(P_r)$ indicate received power density on [*0, w*] while $F(p_r)$ denote the corresponding received power distribution function. Then,

$$F(p_r) = \int_0^{p_r} f(p_r)dp_r,\ 0 \le p_r \le w \tag{3.48}$$

Because communication environment is dynamic, the average of multiple samples of the received power, P_r, is employed to acquire accurate estimate of the received power at each SU with the aid of equation (3.22).

Figure 3.10 is the flow Process for selection of SUs pairs for PUE Localisation.

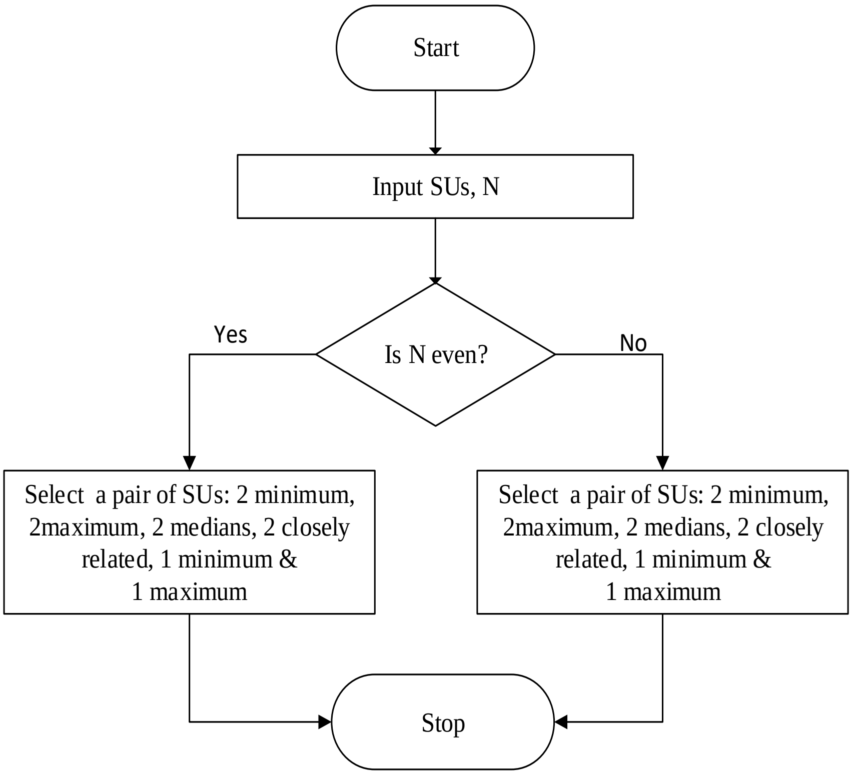

Start
Input SUs, N
Is N even?
Yes
No
Select a pair of SUs: 2 minimum, 2maximum, 2 medians, 2 closely related, 1 minimum & 1 maximum
Select a pair of SUs: 2 minimum, 2maximum, 2 medians, 2 closely related, 1 minimum & 1 maximum
Stop

Figure 3.10: Flow Process for selection of SUs pairs for PUE Localisation

3.5.6 Simulation of effects of cooperative spectrum sensing on hybrid Localisation method

MATLAB (2009) version 7.8.0.347 was used to carry out the simulation that investigated effects of cooperative spectrum sensing on the hybrid localisation method for detection PUE in CRNs. The SU_S and PUE were randomly distributed on the network area of 100 km by 100 km. The initial position of secondary user 1 is (x_1, y_1) (5, 5) and that of secondary user 2 is (x_2, y_2) (8, 8) while that of the PUE was at (X_e, Y_e) (5.9, 9.0). The transmit power of PUE was 20dBm, the path loss within the reference distance, $d_0$is 1m is 1dBm and loss exponent, n, is 4.

3.6 Isolation of Primary User Emulation in Cognitive Radio Networks

In this section, the method for the methodology for isolating is presented. It describes the system model and the operation of the system model.

3.6.1 Primary user emulator isolation model

The proposed PUE isolation model shown in Figure 3.11 comprises of the PU, SBS, SUs, and the PUE. SUs are aware of their location and that of the PU. This scheme is made up of two parts: Detection of PUE (which was accomplished in section 3.3) and isolation of PUE. The detection of PUE is established by individual sensing results of SUs. Each SU senses the transmitter and computes its distance from the transmitter and the angle at which it receives the signal. The estimated distance and the AOA are compared with the known distance and AOA of PU from SUs. If the estimated distance and AOA are the same as that from the PU, the transmitter is assumed to be the PU, otherwise, it is the PUE. SUs forward their computed locations to the SBS which finally uses the location information from SUs to compute the exact location of the transmitter and compares it with the actual location of the PU. Any deviation from the actual location of the PU shows that the transmitter is a PUE.

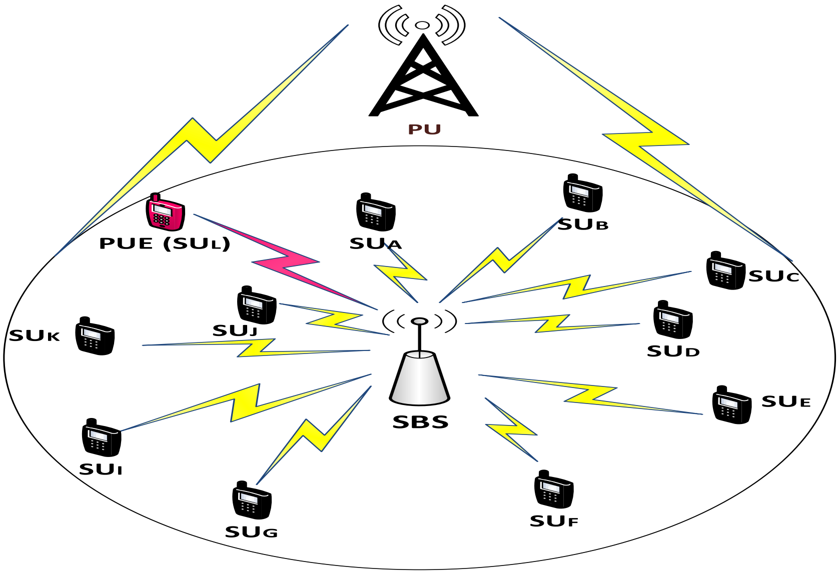


Figure 3.11: Primary User Emulator Isolation Model

Each SU is assigned an initial detection result of (0). When the SU's detection of the transmitter is consistent with the actual location of the PU, the reported detection status is said to be 1, otherwise, it is 0. Transmitter detection is given as:

$$tx \in \mathbb{Z} : \mathbb{Z} \rightarrow [1,0] \qquad (3.49)$$

Thus, the i^{th} SU's detection result can be calculated as follow:

Using (3.23) to compute distance for detection of the transmitter, the detection status is given as:

$$d_{i(tx)} = \begin{cases} 1, & \text{if } \text{tx} \in \mathbb{Z} \setminus 0 \\ 0, & \text{if } \text{tx} \in \mathbb{Z} \setminus 1 \end{cases} \qquad (3.50)$$

Similarly, (3.24) and (3.27) give AOA of the signal at SU_1 and SU_2 with the detection status given in (3.51)

$$AoA_{i(tx)} = \begin{cases} 1, & \text{if } \text{tx} \in \mathbb{Z} \setminus 0 \\ 0, & \text{if } \text{tx} \in \mathbb{Z} \setminus 1 \end{cases} \qquad (3.51)$$

Furthermore, the location of PUE is computed using (3.33) and (3.34) while the detection status is given by (3.52)

$$\mathrm{loc}_{\mathrm{i(tx)}} = \begin{cases} 1, & \text{if } \mathrm{tx} \in \mathbb{Z} \setminus 0 \\ 0, & \text{if } \mathrm{tx} \in \mathbb{Z} \setminus 1 \end{cases} \tag{3.52}$$

From the detection results of distance, AOA, and location, a fusion rule based on the AND operator is used to make final decision if the transmitter is the PU or PUE (Lin *et al.*, 2018). If computed results by the SBS are all high threshold (1s), it is the PU, otherwise, it is a PUE. For the three inputs (distance, AOA, and location), eight possible results are expected from the SBS. The final decision on the status of the transmitter is as shown in Table 3.1

Table 3.1: Detection Decision Table

Distance from SU to transmitter	Angle of arrival of signal from the transmitter	location of the transmitter	Detection result
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Based on the computation of SU detection parameter, the detection result of SU is set to be low (0) if transmitter is PUE and high (1) if transmitter is PU. Once SBS finally determines that all of the results are high, transmitter is adjudged legitimate PU. But once any of the result is low (0), the transmitter is adjudged PUE and hence isolated from CRN. The algorithm for isolating primary user emulator is as follows:

Algorithm 3.2: PUE Detection Decision

```
{ start
$d_i$ = 1, PU; $d_i$ = 0, PUE; $AOA_i$ = 1, PU; $AOA_i$ = 0,
PUE; $loc_i$ = 1,
PU; $loc_i$ = 0, PUE;
If{
$d_{i(tx)} = d_{i(PU)}$
$d_i$ =1
Else
$d_i$ = 0
If{
$AOA_{i(tx)} = AOA_{i(PU)}$
$AOA_i$= 1
Else
$AOA_i$= 0
If{
$loc_{(tx)} = loc_{(PU)}$
loc =1
Else
loc = 0
If{ $d_{i,}$ $AOA_i$, loc) =1
tx = PU
 Else
tx = PUE
 If {
tx = PU
    Cooperate
 Else
    Flag it
 }}}}
 End
```

3.6.2 Isolation process

Once it is established that a particular SU is a PUE, SBS will no longer select it to participate in the detection process. Moreover, information on the network status as well as spectrum holes will not be shared with PUE.

The two SUs to participate in detection processes are selected using (3.53) while communication with participating SUs, $\Re$ in the network is given as (3.54).

$$2SU_{(signals)} \in \Re : \Re \rightarrow \left[SU_1, SU_2, SU_3, SU_4, ...SU_N\right] \backslash PUE \qquad (3.53)$$

$$SBS \rightarrow \Re : \Re \in [SU_1, SU_2, SU_3, ...] \backslash PUE \qquad (3.54)$$

3.6.3 Isolation algorithm

The flow process for the isolation of primary user emulator (PUE) is presented in Figure 3.12

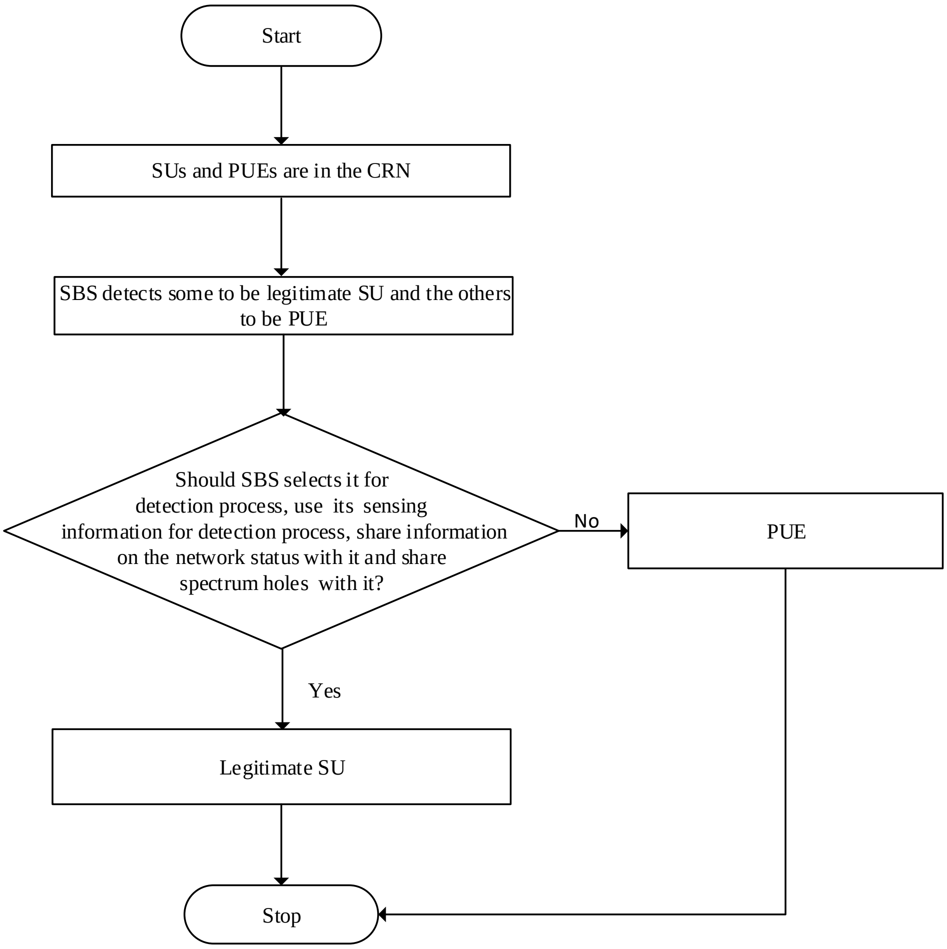

Start
SUs and PUEs are in the CRN
SBS detects some to be legitimate SU and the others to be PUE
Should SBS selects it for detection process, use its sensing information for detection process, share information on the network status with it and share spectrum holes with it?
No
PUE
Yes
Legitimate SU
Stop

Figure 3. 12: The Flow Process for the Isolation of PUE

The algorithm for isolating the primary user emulator (PUE) from the cognitive radio network is given by algorithm 3.3:

Algorithm 3. 3: Isolation of PUE

```
{Start
SBS categorizes CRs in the CRN into SUs and PUEs.
SBS separates them into SUs and PUEs
Should SBS select it for detection process, use its sensing information
for detection process, share information on the network status with it
and
share spectrum holes with it using equations (3.53) and (3.54)?
If yes
It is SU
Else
It is PUE
Stop}
```

3.6.4 Sensing and transmission times of secondary user

When SBS detects spectrum hole, it allocates it to only one SU in a time span. A time span is the epoch an SU is allowed to use the detected spectrum hole. This analysis is restricted to only one SU in one frame time or a time span, $T+T_1$, as depicted in Figure 3.13. T is the sensing time and T_1 is the transmission time. The SU transmits when the SBS correctly or wrongly decides the absence of the PU

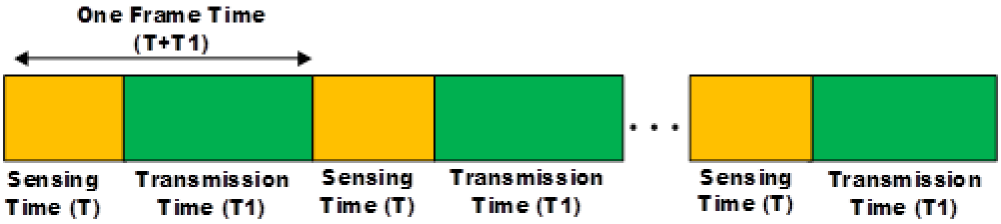


Figure 3.13: Sensing time and transmission time of SU

(Liang *et al*., 2008; Stotas & Nallanathan, 2010).

For i^{th} SU transmitting over the white space, the effective throughput G_i is given as (Liang *et al*., 2008):

$$G_i = \frac{T_1}{T+T_1}\left[C_{0i}\left(1-p_f\right)p\left(H_0\right)+C_{1i}\left(1-p_d\right)p\left(H_1\right)\right] \qquad (3.55)$$

whereC_{oi} and C_{1i} are the capacity of the normalized channel used by i^{th} SU under the hypothesis of H_0 and H_1 respectively.

Supposing the *SNR* for secondary transmission of the SU is SNR_S = 44dB. The capacity of the normalized channel used by i^{th} SU in the hypothesis of H_0 and H_1 are given by (3.56) and (3.57) respectively.

$$C_{0i} = \log_2\left(1 + SNR_S\right) = 6.66 \tag{3.56}$$

$$C_{1i} = \log_2\left(1 + \frac{SNR_S}{1 + SNR_P}\right) = 6.61 \tag{3.57}$$

SNR_S and SNR_P are signal-to-Noise-Ratio for SU and PU respectively. Since P (H_0) >P (H_1), $C_{0i} \gg C_{1i}$ and $1-P_f$>$1-P_d$ (Shrivastava *et al.*, 2018), i^{th} SU's throughput is estimated thus:

$$G_i = \frac{T_i}{T + T_i} C_{0i}\left(1 - p_f\right) p\left(H_0\right) \tag{3.58}$$

The total energy $E_{i,j}^{Tr}$ consumption of an i^{th} SU in transmission mode scenario is given by (3.59) (Saeed *et al.*, 2017).

$$E_{i,j}^{Tr} = \left(P^{TX} T_{ctr}\right) + \left(P^{cs} T_{cs}^{i,j}\right) + \left(P_{\max}^{TX} \,|\, \mathrm{h}_{i,j} \,|\, \tau_{TX}^{i,j}\right) + \left(P^{C} \tau_{TX}^{i,j}\right) \tag{3.59}$$

Where,

$E_{i,j}^{Tr}$ is the total energy consumption for i^{th} SU. P^{TX}, T_{ctr} and P^{cs} are the transmission power of the i^{th} SU, the time control message duration and circuit power of the SU respectively. The transmission duration of the i^{th} SU on channel j is given by $\tau_{TX}^{i,j}$ whereas $T_{cs}^{i,j}$ is channel switching latency. The maximum transmission power is represented by $P_{\max}^{TX}$. While $\mathrm{h}_{i,j}$ is gain of the channel.

3.6.5 Simulation and analysis for PUE isolation

By sending PU-like signal when the legitimate PU is absent, PUE decreases the performance of CRN. It is assumed that PUE knows the behaviour of the PU a priori. Therefore, in this section, we study the effect of PUE on the CRNs in the absence of PU by paying attention to the throughput of i^{th} SU in the presence of PUE. To verify analytical results of our formulation, MATLAB (2009) version 7.8.0.347 based simulation was used to investigate the effect of the PUE on the throughput of SU. The parameters used for this simulation are as follows: the sensing time is 100 milliseconds whereas the transmission time ranges between 5 milliseconds to 25 milliseconds. The normalized channel capacities (c_{oi}) of the licensed channel used by i^{th} SU under the hypothesis of H_0 is 0.2 while the probability of PU (H_0) absence is 0.8.

CHAPTER FOUR

4.0 RESULTS AND DISCUSSION

4.1 Preamble to Results and Discussion

On successful completion of detection of PUE using hybrid of AOA and RSS and successful development of technique for isolating the detected PUE in chapter three, the results obtained from the designs in chapter three are discussed in this chapter. The analyses of the results are divided into diverse sections which are sequentially arranged according to design methodology in chapter three. Therefore, in section 4.2, we analyzed the results obtained from section 3.4. Similarly, section 4.3 analyzed results obtained in section 3.5 while section 4.4 analyzed results obtain in section 3.6

4.2 Hybrid Localisation Method Results

In Figure 4.1, the distance between SU_1 and primary user (PU) is compared with the distance between SU_1 and the primary user emulator (PUE). It was observed that at different positions of SU_1, the distance between SU_1 and PU was different from the distance between SU_1 and PUE. It is worth noting that these results validate the correctness of the algebraic derivations in (3.23) and show that the computer simulation tracked the correct positions of the nodes in the cognitive radio network (CRN).

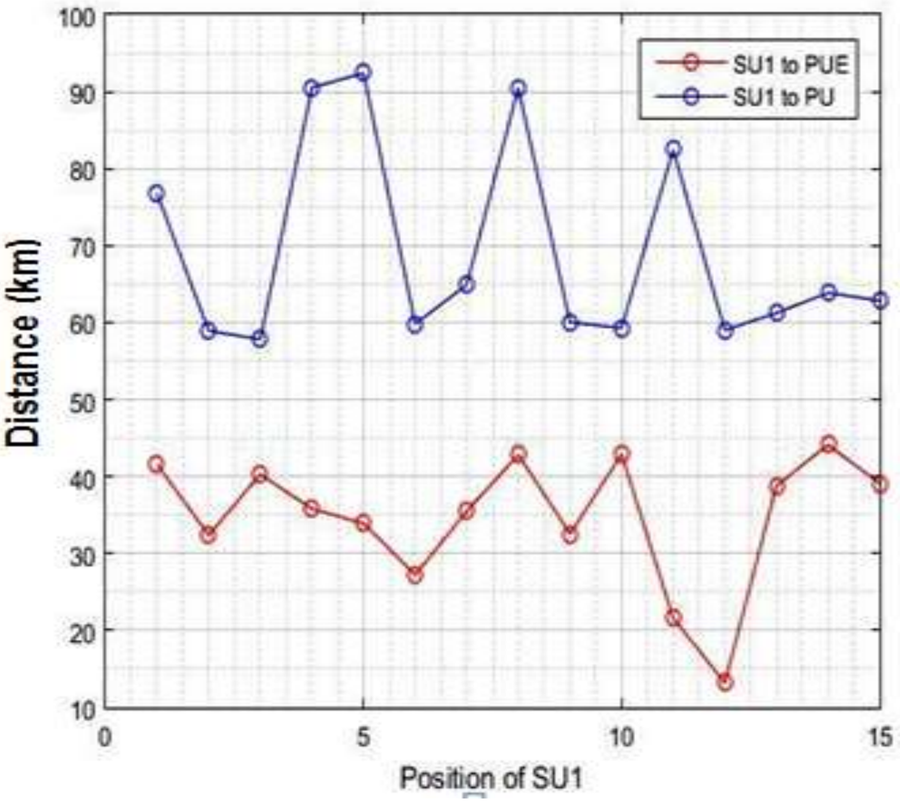


Figure 4.1: Distance between SU_1 and PU Compared with Distance between PUE and SU_1

In Figure 4.2, various locations of SU_2 were considered and the distance between $SU_2$and PU was compared with the distance between $SU_2$and PUE in each case. In each scenario, the distances from SU_2 to PU were entirely different from the distances from $SU_2$to PUE. For example, when SU_2 was at position 5, it was 39 km away from PUE and 74 km away from the PU. Likewise, at position 10, SU_2 was 45 km away from the PUE and 62.5 km away from the PU. In both cases, it is noted that PU was farther away from SU_2 than from PUE.

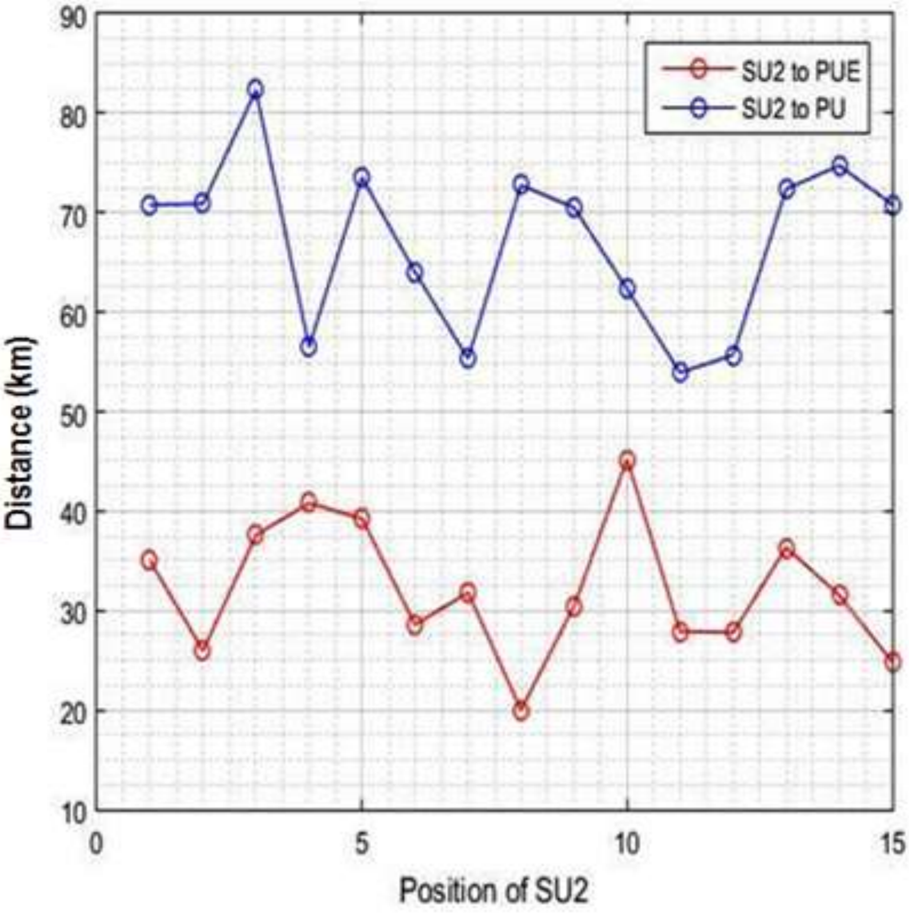


Figure 4.2: Distance between PU and SU_2 Compared with Distance between PUE and SU_2

As seen in Figure 4.3 using (3.24), at position 1, SU_1 is 45^0 from PU while it is 77^0 PUE. Similarly, at position 9, SU_1 is 25^0 from PU while it is 117^0 from PUE. Furthermore, at position 13, SU_1 is 50^0 from PU while it is 72^0 from PUE. It can be observed that at each of the fifteen different positions of SU_1, angle of arrival (AOA) of the PU's signal to SU_1 is different from that of PUE. It can thus be extrapolated that, PU and PUE are at different positions since they do not have the same AOA.

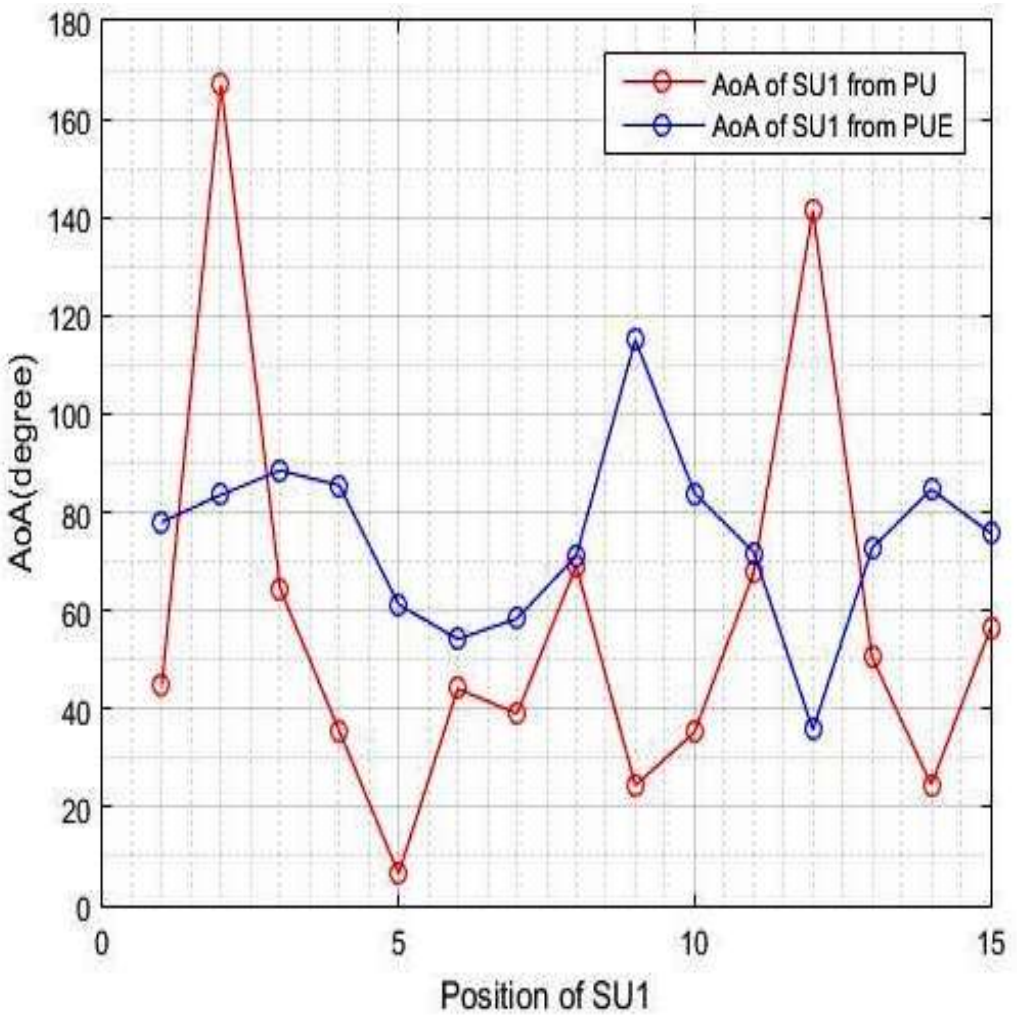


Figure 4.3: Angle of Arrival of the Signals from PUE and PU at SU_1

Using (3.27) to compare the signal received at SU_2 from PU and PUE in terms of the angle at which the signal arrived at SU_2 as pointed out in Figure 4.4, the angles at various location ofSU_2 are diverse with the exception of position 3. At position 3, the AOA of signal from both PU and PUE is 103^0. It means that in an attempt to carry out its mischievous activities, PUE can assume a position that either produces the same AOA or distance from PU to SU. This informs the need for hybridisation as both AOA and RSS cannot be compromised at the same time.

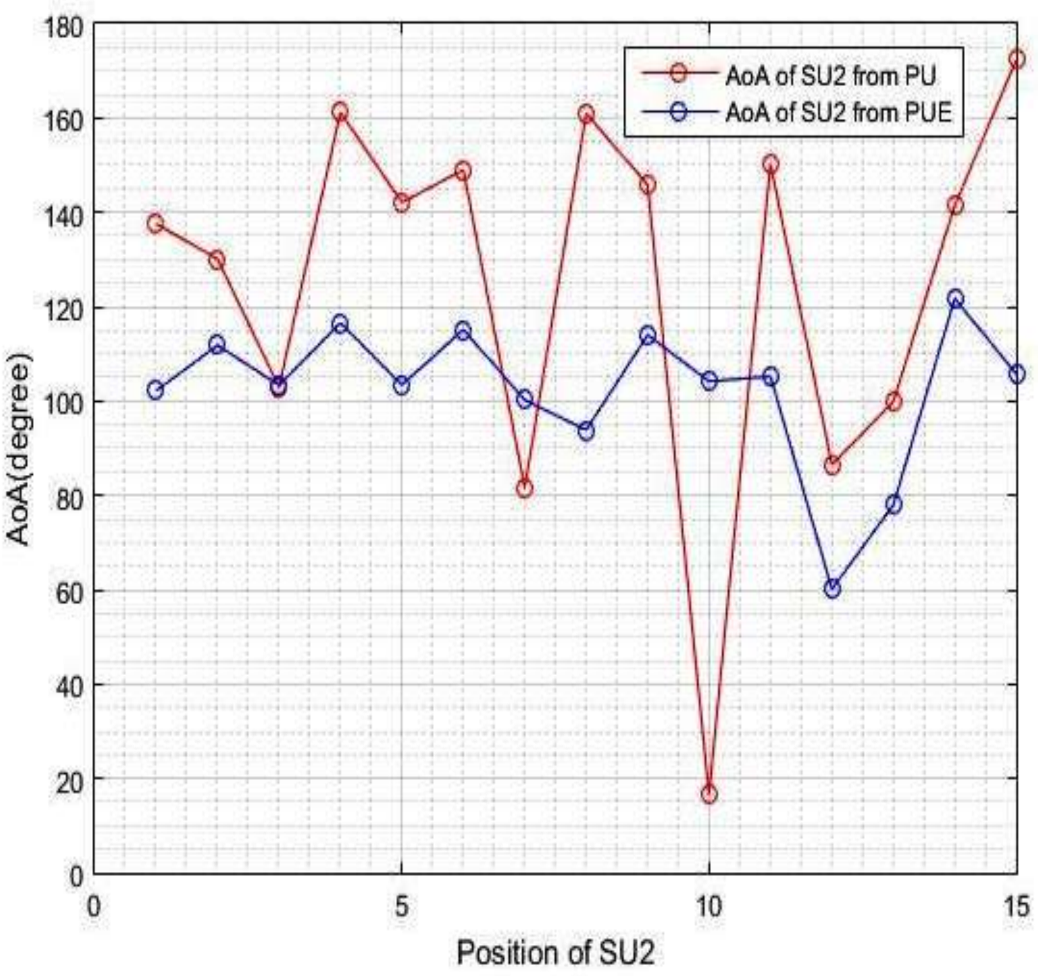


Figure 4.4: Angle of arrival of the signals from PUE and PU at SU_2

4.2.1 Performance analysis of hybrid localisation method

The performance of the HLM was carried out via RMSE (given by 3.35) as displayed in Figure 4.5. It is noticed that both RSS and AOA localisation methods converged at the 50th iteration with RMSE of 0.20 and 0.01 respectively. This means that, AOA out performed RSS in terms of speed, energy efficiency and accuracy which made it faster than RSS and AOA schemes. Similarly, HLM converged at the 20th iteration with RMSE of 0.005. Therefore, the HLM outperformed the RSS and AOA localisation schemes respectively by a good margin both in speed and accuracy. Moreover, the performance of the HLM out-performed RSS and AOA presented in (Fihri *et al.*, 2018; Penna & Cabric, 2013) and shown in Table 4.1.

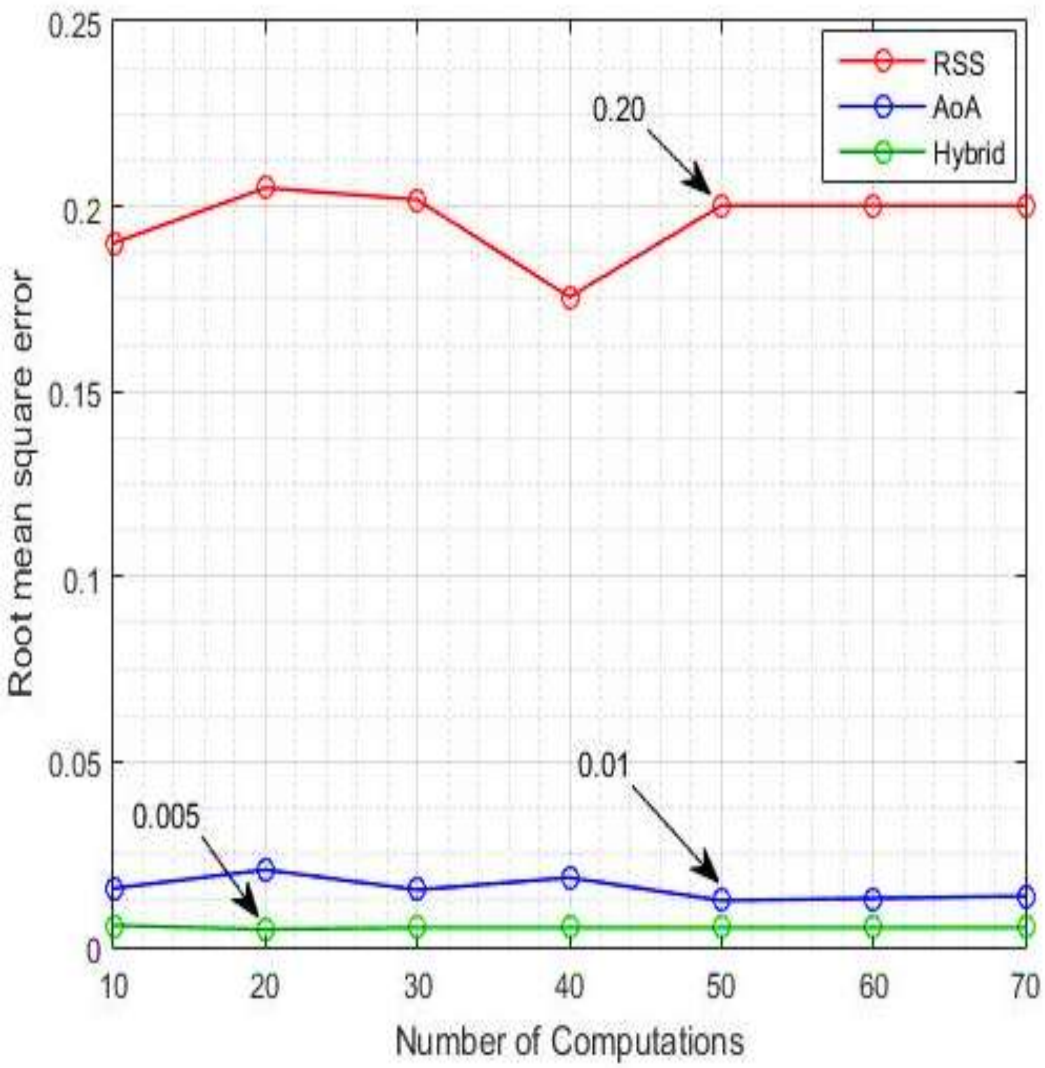


Figure 4.5: Performance of Angle of Arrival, Received Signal Strength and Hybrid Localisation Methods

4.2.2 Significance of the hybrid localisation method results

Table 4.1 displayed the comparison of hybrid localisation method with similar localisation techniques. The HLM in this workout performed better than RSS and AOA techniques by Fihri *et al*. (2018) and Penna & Cabric, (2013) respectively. Fihri *et al*. (2018) used three SUs for detection. This actually makes the algorithm complex, time consuming and expensive. However, HLM used only two SU nodes to detect PUE; hence, it is less complex, faster and less expensive. Although Penna & Cabric, (2013) achieved PUE detection faster with higher accuracy, their model is more complex and expensive because it used different multi-antenna. Conversely, our AOA which did not incorporate multi-antenna is less complex with higher accuracy. Likewise, the HLM exhibited higher accuracy with 5.00x10^{-3} RMSE. Furthermore, the HLM converged at lesser number of computations. Hence, it is faster and higher in terms of energy efficiency.

Table 4.1: Performance of Localisation Methods

Localisation Method	Amount of Iterations	RMSE
RSS (Fihri *et al*., 2018)	55	2.2x10^{-1}
AOA(Penna & Cabric, 2013)	30	1.2x10^{-2}
RSS (our algorithm)	50	2.00x10^{-1}
AOA (our algorithm)	50	1.00x10^{-2}
The Hybrid of RSS and AOA	20	5.00x10^{-3}

4.3 Effects of Cooperative Spectrum Sensing on Hybrid Localisation Method

In this section, pairs of SUs were used to localise the PUE. These pairs include: two SUs with maximum RSS values, two SUs with minimum RSS values, two SUs with one having maximum RSS value and the other having minimum RSS value, two SUs having median RSS values and two SUs with closely related RSS values. (3.28) was used for all computations in this section.

In Figure 4.6, two SUs with maximum received signal strength (RSS) were used to localise PUE using (2.23). It is interesting to know that the RMSE of 1.3X10^{-2} at the 10th iteration peaked at 1.4X10^{-2} at the 20th iteration. The reduction of the RMSE was sharper between 20th and 30th iterations but progressively reduced afterwards until it converged at the 70th iteration with RMSE of 6.0X10^{-3}.

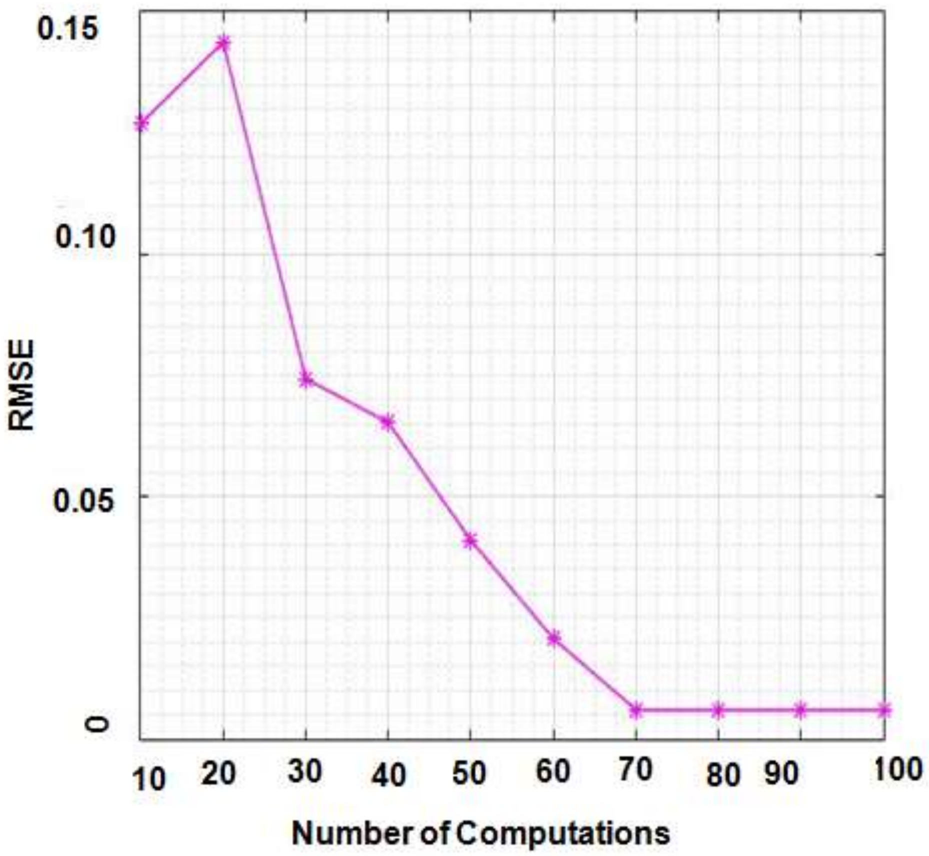


Figure 4.6: Performance of CSS-HLM using two SUs with Maximum RSS

Similarly, localisation of primary user emulator (PUE) by two secondary users (SUs) with the minimum received signal strength (RSS) was demonstrated in Figure 4.7. Using the two SUs with the minimum RSS gave a Root Mean Square Error (RMSE) of 1.9X10^{-1} at the 10th iteration but converged at the 80th iteration with the RMSE of 8.1X10^{-3}. It thus shows that if two SUs with the minimum RSS values are used for localisation, convergence can only be achieved at the 80th iteration.

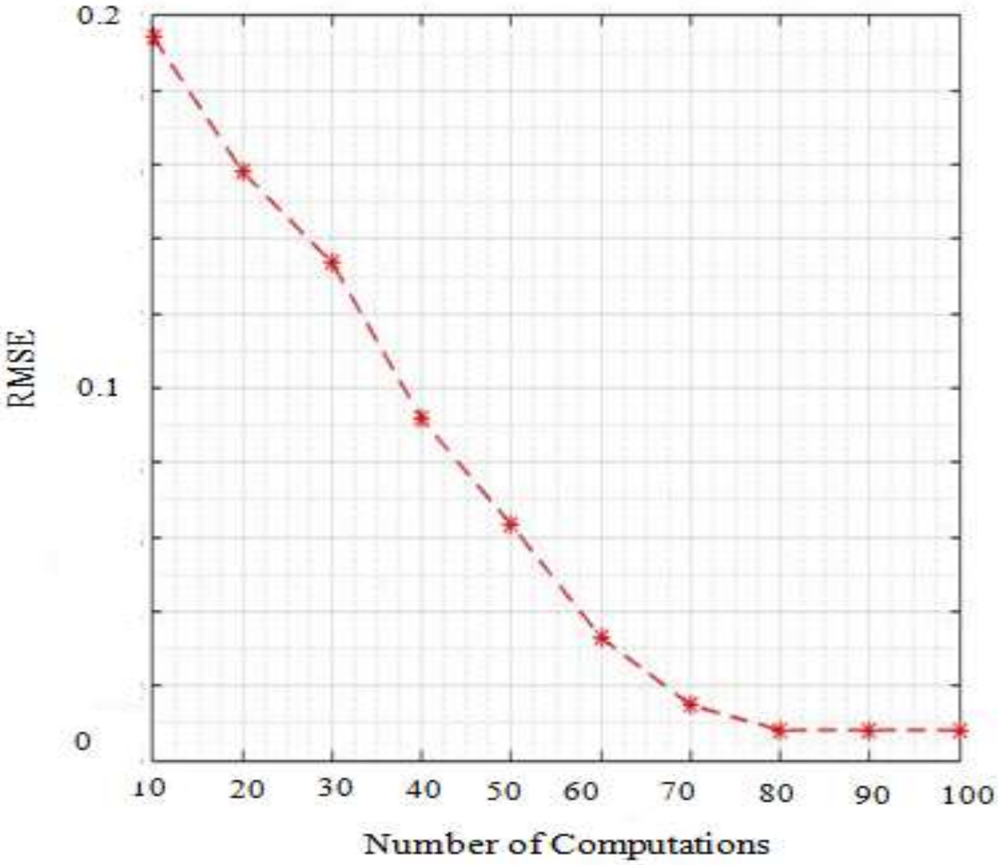


Figure 4.7: Performance of CSS-HLM using two SUs with Minimum RSS

The performance of the hybrid localisation method in the detection of PUE in CRN shown in Figure 4.8 was carried out with two SUs with median RSS. At 10th iteration, it has RMSE of as high as $1.65X10^{-1}$ but as the number of iteration increased, accuracy also increased until convergence was achieved at the 80th iteration with RMSE of $6.80X10^{-3}$.

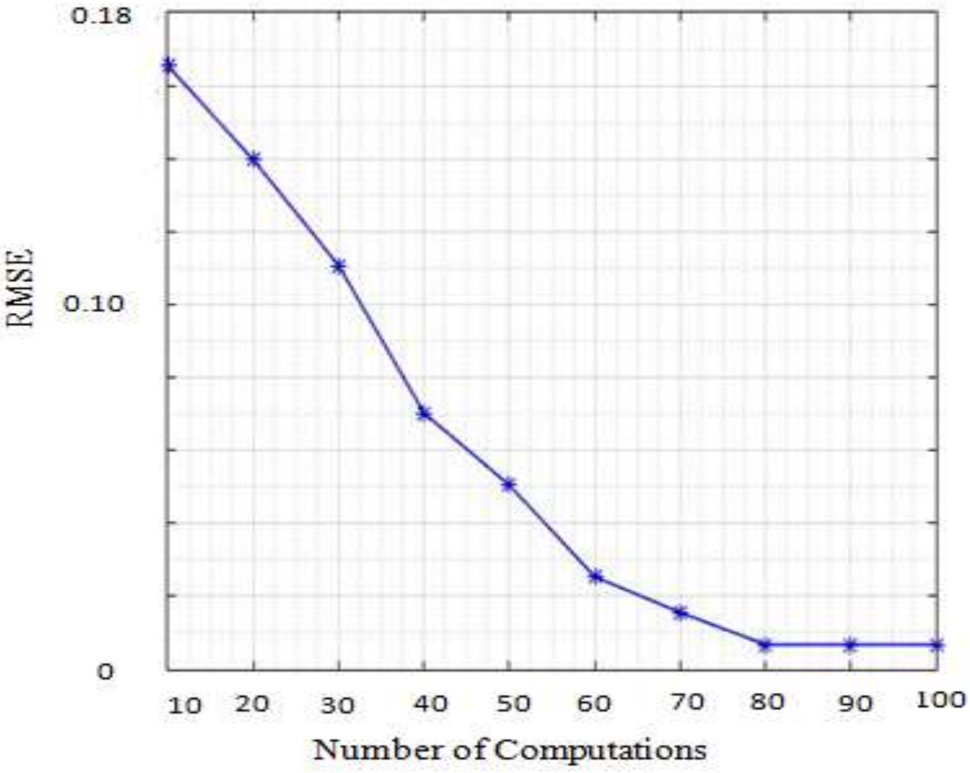


Figure 4.8: Performance of CSS-HLM using two SUs with Median RSS

In Figure 4.9, one of the two SUs that participate in the localisation of PUE has the maximum RSS whereas the other has the minimum RSS. Although the RMSE reduced with increase in the number of iterations, it never attained convergence even at 100th iteration. RMSE reduced rapidly between 10th and 20th iterations but reduced progressively until 40th iteration where convergence seemed to have been achieved. But as the number of computation increased from 50th iterations, convergence was never achieved even after the 100th. It can be deduced that using the highest and the lowest RSS, is not an ideal pair for detecting PUE in CRN.

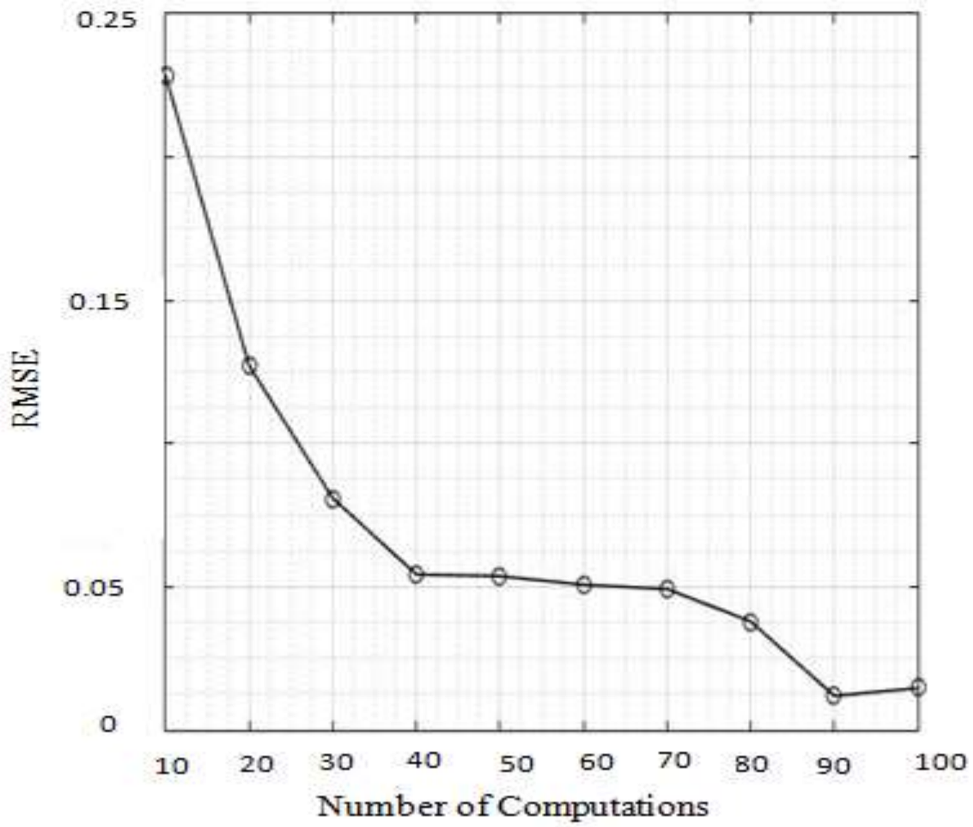


Figure 4.9: Performance of CSS-HLM with two SUs having Maximum and RSS

Figure 4.10 shows the effects cooperative spectrum sensing has on the HLM in localising PUE in CRN using two closely related RSS values is shown in Figure 4.10. Here it can be seen that at the 10th iteration, the RMSE was $1.8X10^{-1}$ but at the 20th iteration, convergence was achieved with RMSE of $4.7X10^{-3}$. Since convergence is achieved faster with this pair than any other pair, it can be extrapolated that a pair of SUs with closely related RSS values is better for detecting PUE in CRN than any other pair.

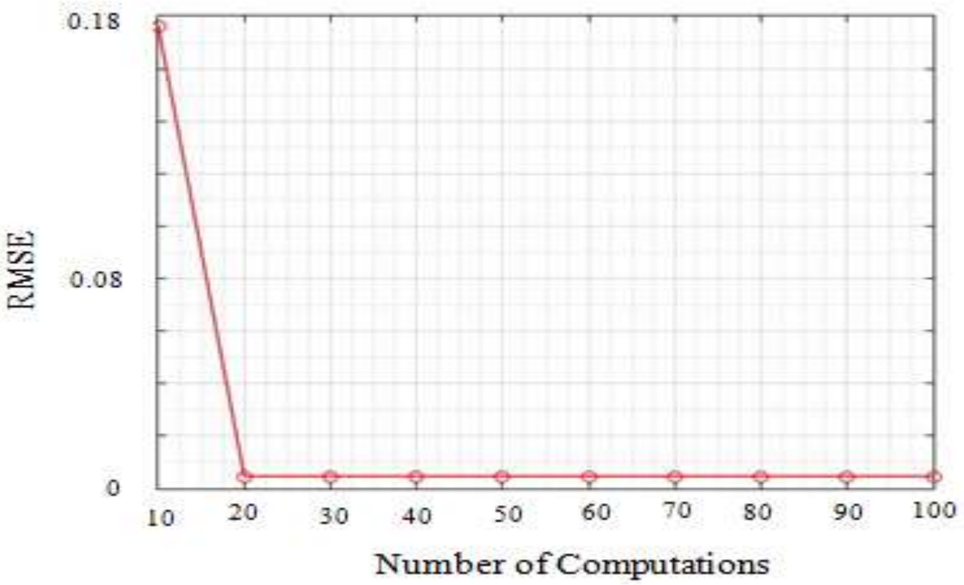


Figure 4.10: Performance CSS-HLM using two SUs with closely Related RSS

4.3.1 Performance Analysis of CSS-HLM

Figure 4.11 is the performance evaluation of the hybrid using SU pairs with closely related RSS values, minimum RSS values, maximum values, minimum and maximum RSS values and median RSS values. Clusters are differently cluttered, thus, SUs within the same cluster and neighbouring clusters have analogous signal propagation channel. This resulted in the related RSS in those clusters. But SUs in different clusters that are far apart. Thus, they experience variant signal propagation channel which leads to their variant RSS values. Consequently, different sets of SUs provided different results. It was observed that accuracy increased as the number of iterations (computations) increased in all cases. It was also observed that although two SUs with minimum RSSs and two SUs with median RSSs both converge at the 80th iteration, they have RMSE of $8.1\text{x}10^{-3}$ and $6.8\text{x}10^{-3}$ respectively. When two SUs with the maximum RSSs were used to localise the PUE, it converged at the 70th iteration with RMSE of $6.0\text{x}10^{-3}$. On the other hand, when two SUs one of which has the highest RSS and the other with the least value of RSS were used, convergence was not attained even at the 100th iteration due to the fact that their locations were far apart. But when two SUs with closely related RSSs were used to localise the PUE, it converged at the 20th iteration with RMSE of $4.7x10^{-3}$. From these discoveries and as shown in Figure 4.11, it is extrapolated that, the HLM for detecting PUE in CRNs performs better when two SUs with closely related RSS are used to detect the PUE while the worse combination is SUs with maximum and minimum RSS values.

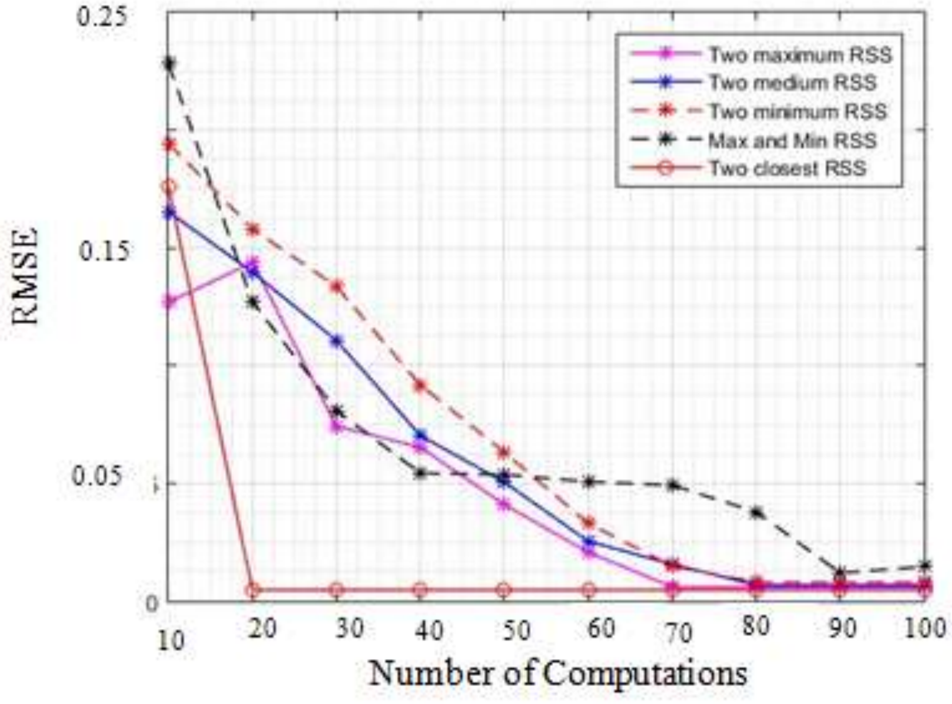


Figure 4.11: Performance of CSS-HLM with two SUs having varying RSS

4.3.2 Significance of the results

The comparison of PUE detection using different pairs of SUs is shown in Table 4.2. Shows that the pair of SU that are closely related detects PUE faster with higher accuracy as convergence was attained after the 20th iteration with RMSE of $4.7x10^{-3}$.

Furthermore, Figure 4.12 presents the total energy consumed by each pair of SUs as given by (3.59) over the convergence time and their respective RMSE values. It was discovered that SUs with closely-related pair of RSS converged fastest to its minimum RMSE value. Thus, it consumed the least energy. Basically, Figure 4.12 presents two interesting observations: the CSS-HLM can be used with or without clustering approach. In the clustering approach, it is suggested that SU pairs with closely related values of RSS should be selected from the same cluster or neighbouring clusters as this produces improved performance. However, in a non-clustered CRN, it is advised that SU pairs with maximum RSS values should be adopted for the best performance.

Table 4.2: Comparison of PUE detection using different pairs of SUs

Combination of SUs	RMSE	Number of Iterations
Minimum and maximum RSS	$1.5\text{x}10^{-2}$	150
Minimum RSS	$8.1\text{x}10^{-3}$	80
Median RSS	$6.8\text{x}10^{-3}$	80
Maximum RSS	$6.0\text{x}10^{-3}$	70
Closely related RSS	$4.7\text{x}10^{-3}$	20

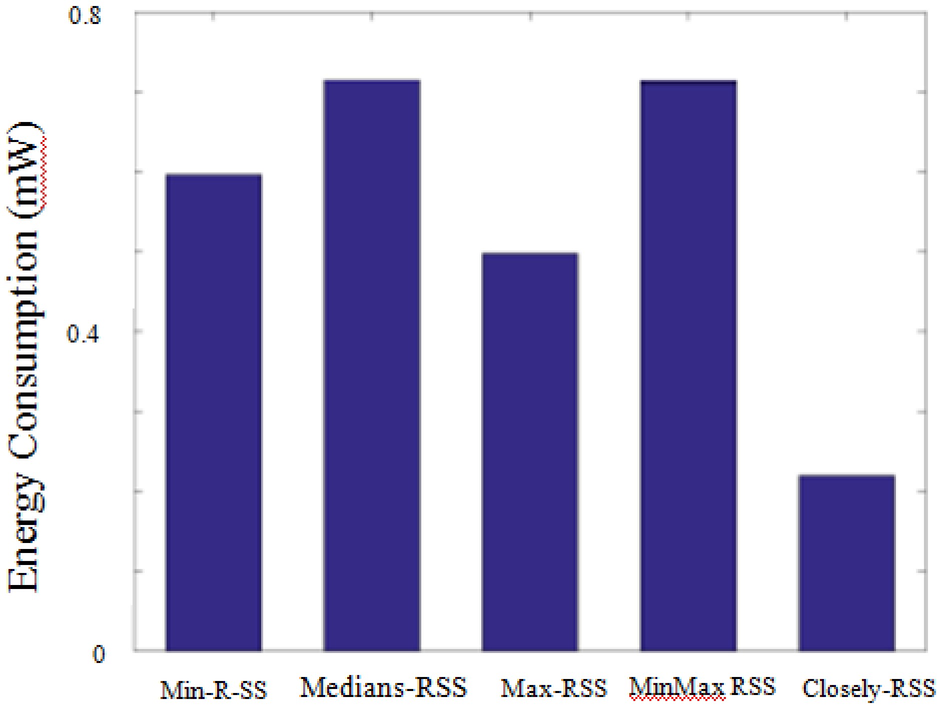


Figure 4.12: Energy Consumption of the CSS-HLM with a Pair of SUs Having Minimum, Median, Closely Related and Maximum RSS

4.4 Isolation of Primary User Emulator

In the absence of PUE, SU transmits for longer time leading to high throughput. But throughput of an SU will be less when PUE comes in with PU-like signal and SU breaks its transmission. As displayed in Figure 4.13, on transmitting for 25 milliseconds, SU was expected to have a throughput of $104x10^{-2}$. Howbeit, if at any time SU quitted the spectrum for PUE with the assumption that PUE was the PU, its throughput dropped. For example, with the presence of PUE, SU's throughput dropped at 25 milliseconds to $84x10^{-2}$. Similarly, when SU transmitted for 15 milliseconds but PUE took over the spectrum and transmitted for the remaining time, SU's throughput would be $56x10^{-2}$ as against $7x10^{-1}$ when PUE was not present. In the same way, when PUE took over spectrum after 20 milliseconds of SU's transmission, throughput dropped to $7x10^{-1}$ as against $9x10^{-1}$ when PUE was absent.

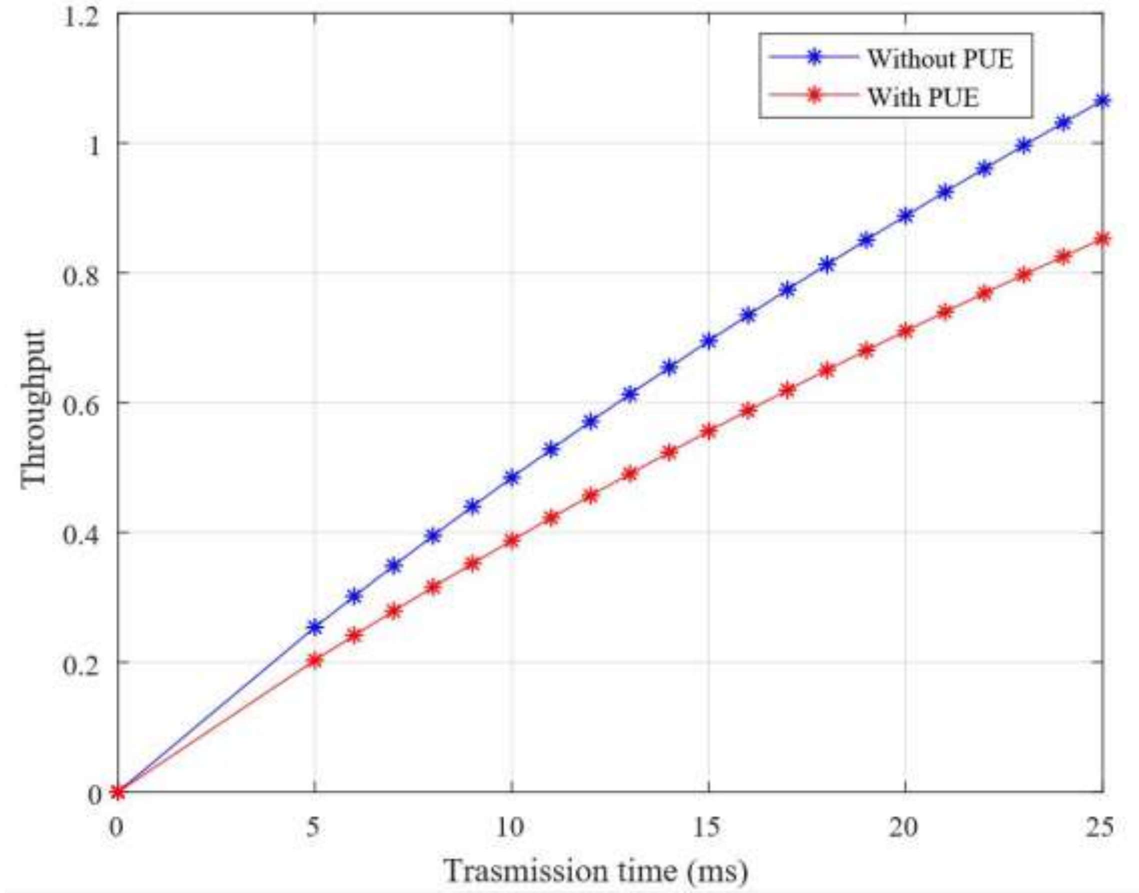


Figure 4.13: Throughput versus transmission time.

Effect of false alarm on the throughput is portrayed in Figure 4.14. Here it was observed that when probability of false alarm was 0.0, it means PUE is not present and so, throughput was 25x10^{-2}. But when probability of false alarm was 0.2, throughput dropped to 2x10^{-1}. Similarly, when false alarm probability increased to 0.4, throughput became 15x10^{-2}. But when false alarm probability was 1, throughput was 0. This shows that, at the point when the probability of false alarm is 1, it is certain that the PUE has taken over the spectrum and so, throughput of the SU at that point equals 0. Thus, higher probability of false alarm invariably leads to lower throughput and vice versa.

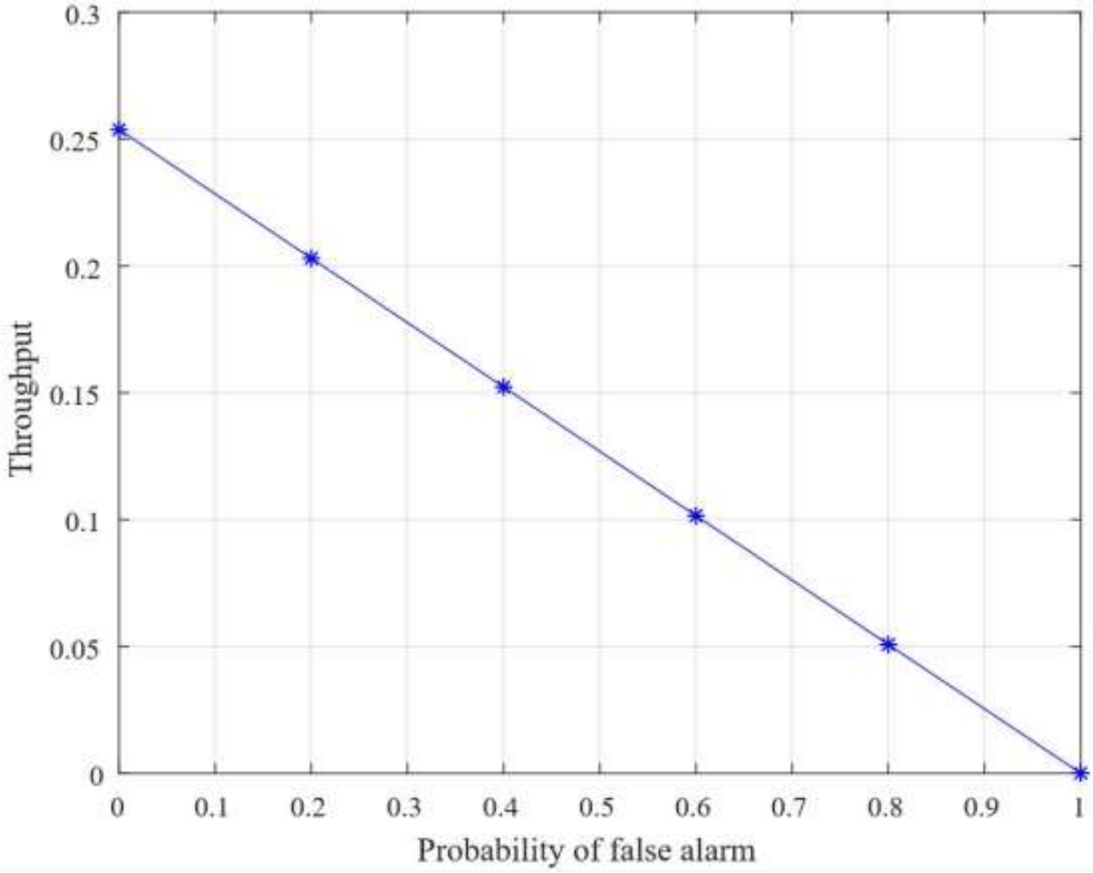


Figure 4.14: Throughput versus false alarm

CHAPTER FIVE

5.0 CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

A hybrid localisation method to accurately detect PUE in cognitive radio network (CRN) was developed in this research work. This is in contrast to the range-based localisation methods which are financially expensive and complex to deploy. The hybrid method uses just a pair of SUs to estimate the position of the PUE and validated the developed hybrid localisation method in section 3.4 via computer simulations. The simulations substantiate that the hybrid method localises PUE accurately and faster (Table 4.1).

Moreover, while two SUs can be used to detect a PUE in CRNs, shadowing, fading, path loss and hidden node problems pose a fundamental challenge of uncertainty in the value of RSS at the SUs. This challenge affects accurate detection of PUE in CRN thereby leading to inefficient operation of CRN. To overcome this challenge, the best SUs (that are closely related in RSS values) were used in the detection procedure. To overcome channel impairment and mobility issues of centralized cooperative sensing, cluster-based centralized CSS was developed to select the right SUs for the hybrid localisation scheme. Computer simulations were then used to demonstrate cluster-based centralized cooperative sensing by means of two suitable SUs to localise the PUE. The simulation results ratify that SUs pair with closely related received signal strength (RSS) localises PUE more accurately (with RMSE of $4.7\text{x}10^{-3}$), faster (with 20 iterations), and has an added advantage of being more energy efficient than any combination of SUs as it converged faster than any pair. The results further demonstrate that the combination of maximum (or highest) and minimum (or least) RSS values give the worse localisation result with a RMSE of $1.5\text{x}10^{-2}$.

Moreover, since PUE parades itself as the legitimate PU, it causes SU to quit using the spectrum while transmitting. This results in denial of service, connection unreliability, low throughput, bandwidth waste, degraded quality of service and eventual collapse of the CRNs if PUE is left in the network. To prevent this and perk up the general performance of CRNs, an algorithm for isolating PUE from a CRN upon detection was developed.

5.2 Recommendations

Based on the discoveries of this study, we recommend that further research is made on localisation of PUE with a view to designing a hybrid scheme that will utilise geographical poles to localise PUE from a CRN in which primary user, secondary user and primary user emulator are all mobile devices. We equally recommend that further research is made in the application of OR gate in isolating PUE for optimal operation of CRN.

5.3 Contributions to Knowledge

The following contributions were made at the end of this study:

i. A hybridised technique of localizing PUE in CRN was developed

ii. An efficient approach for selecting a pair of SUs for detecting PUE was developed.

iii. An approach for isolating the detected PUE in CRN was developed.

REFERENCES

Ahmed, A., Mai A., Jian R.,& Tongtong, L. (2014). Throughput analysis and routing security discussions of mobile access coordinated wireless sensor networks. *2014*

IEEE Global Communications Conference (pp.772–781). Austine USA: IEEE. doi: 10.1109/glocom.2014.7037536

Akbari, K.,& Jamshid, A. (2018). Signal classification for detecting primary user emulation attack in centralized cognitive radio networks. *Iranian Conference on Electrical Engineering* (pp.342–347). Iran: IEEE. https://doi.org/ 10.1109/ ICEE. 20 18.8472515

Akhtar, S., Shahzad, M., & Imran, M. (2014). A weighted linear combining scheme for cooperative spectrum sensing. *Procedia Computer Science* (pp.149–157). Hasselt, Belgium: Elsevier Masson SAS. https://doi.org/10.1016/j.procs.2014.05.409

Akyildiz, I. F., Lo, B. F., & Balakrishnan, R. (2011). Cooperative spectrum sensing in cognitive radio networks : A survey. *Physical Communication*, *4*(1), 40–62. https://doi.org/10.1016/j.phycom.2010.12.003

Akyildiz I. F., Won-Yeol L., Mehmet, C. V.,& S. M. (2006). Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks, 50*(13), 2127–2159. https://doi.org/10.1016/j.comnet.2006.05.001

Alahmadi, A., Abdelhakim, M., Ren, J., & Li, T. (2014). Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. *IEEE Transactions on Information Forensics and Security*, *9*(5), 772–781.doi: 10.1109/TIFS.2014.2310355.

Alhakami, W., Mansour, A., & Safdar, G. A. (2014). Spectrum sharing security and attacks in CRNs : A review. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *5*(1), 76–87. http://dio.org/10.14569/IJACSA.2014.05 0111

Alhumud, H., Zohdy, M., Debnath, D., & Olawoyin, R. (2019). Cooperative spectrum sensing for cognitive radio-wireless sensors network based on OR rule decision to enhance energy consumption in greenhouses. *Wireless Sensor Network*, 2019(*11)*, 1–11. https://doi.org/10.4236/wsn.2019.111001

Ali, A., Abbas, L., Shafiq, M., Bashir, A. L., Afzal, M. K., Liaqat, H. B., Siddiqi, M. H.,& Kwak, K. S. (2019). Hybrid fuzzy logic scheme for efficient channel utilization in cognitive radio networks. *IEEE Access, 7(2019)*, 24463–24476. https://doi.org/10.1109/ACCESS.2019.2900233

Amer, R., El-sherif, A. A., Ebrahim, H., & Mokhtar, A. (2016). Cooperation and underlay mode selection in cognitive radio network. *Fifth International Conference on Future Generation Communication Technologies* (pp. 36–41) Bedfordshire, Luton, UK. IEEE. https//:dx.doi.10.1109/FGCT.2016.7605066

Ammar, M., Riley, N., Mehdawi, M., Fanan, A., & Zolfaghari, M. (2015). Detection threats and mitigation techniques in cognitive radio based on localisation of signal source and trustworthiness. *4th International Conference on Advances in Engineering Sciences & Applied Mathematics* (pp.77–83). Kuala Lumpur, Malaysia: *ICAESAM*. https://doi.org/http://dx.doi.org/10.15242/IIE.E1215070

Anandakumara, H. & Umamaheswarib, K. (2017). An efficient optimized handover in cognitive radio networksusing cooperative spectrum sensing. *Journal of Intelligent Automation & SoftComputing,* 2017(9), 1–9. https://doi.org/10.1080/10798587. 20 17.1364931

Armi, N., Saad, N. M., & Arshad, M. (2009). Hard decision fusion based cooperative spectrum sensing in cognitive radio system. *ITB Journal of ICT, 3*(2), 109–122. https://doi.org/http/:dx.doi.org/10.5614%2Fitbj.ict.2009.3.2.3

Arthy, A. & Periyasamy, P. (2015). A review on spectrum sensing techniques in cognitive radio network. *Proceedings of UGC Sponsored National Conference on Advanced Networking and Applications* (pp. 80–83). Amravati, India: Springer

Ashokan, A., & Jacob, L. (2017). Distributed cooperative spectrum sensing with multiple coalitions and non-ideal reporting channel. *IEEE SPICES 2017* (pp. 1–6). Kollam, Kerala, India: IEEE. DOI:10.1109/SPICES.2017.8091340

Balieiro, A., Yoshioka, P., Dias, K., Cavalcanti, D., &Cordeiro, C. (2014). A multi-objective genetic optimization for spectrum sensing in cognitive radio. *Journal of Expert Systems With Applications*, *41*(8), 3640–3650. https://doi.org/10.1016/ j. es wa.2013.12.010

Bouabdellah, M., Ghribi, E., & Kaabouch, N. (2019). RSS-based localisation with maximum likelihood estimation for pue attacker detection in cognitive radio networks. *2019 IEEE International Conference on Electro Information Technology (EIT 2019)* (pp. 1–16). Brookings, SD, USA:IEEE. doi: 10.1109/EIT.2019.8834095

Celebi, H & Arslan, H. (2007). Utilization of location information in cognitive wireless networks. *IEEE Journal of Wireless Communication*, *14*(4), 6–13. https://doi. org/10.1109/MWC.2007.4300977

Chen, R., & Park, J. (2006). Ensuring trustworthy spectrum sensing in cognitive radio networks. *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks* (pp. 110–119). Reston, VA,USA: IEEE.

Chen, R., Park, J., & Hou, Y. T. (2008a). Towardssecure distributed spectrum sensing in cognitive radio networks. *IEEE Communication Magazine*, 4(4), 50–55.

Chen, R., Park, J., & Reed, J. H. (2008b). Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, *26*(1), 25–37. https://doi.org/10.1109/JSAC.2008.080104

Chen, Y., Liuqing Y., &Shuaishuai M. (2016). Detecting primary user emulation attacks based on PDF-BP algorithm in cognitive radio networks. *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 660–666). Chengdu, China: IEEE. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.144

Chunsheng, X., & Song, M. (2014). Detection of PUE attacks in cognitive radio networks based on signal activity pattern. *IEEE Transaction on Mobile Computing, 13*(5), 1022–1034. https://doi.org/10.1109/TMC.2013.121

Deng, R., Chen, J., Yuen, C., Cheng, P., & Sun, Y. (2012). Energy-efficient cooperative spectrum sensing by optimal scheduling in sensor-aided cognitive radio networks. *IEEE Transactions on Vehicular Technology*, *61*(2), 716–725. DOI: 10.1109 / TVT.2011.2179323

Dibal, P. Y., Onwuka, E. N., Agajo, J., & Alenoghena, C. O. (2018). Application of wavelet transform in spectrum sensing for cognitive radio : A survey. *Physical Communication*, *28*(2018), 45–57. https://doi.org/10.1016/j.phycom.2018.03.004

Fang, Y., Xun, Z., &Yibing, L. C. T. (2017). Faithworthy collaborative spectrum sensing based on credibility and evidence theory for cognitive. *MDPI Symmetry*, *9*(36), 1–16. https://doi.org/10.3390/sym9030036

Faruk, N., & Ayeni, A. A. (2013). DTV coverage and protection contour estimation for spatial white space. *2013 IEEE International Conference on Emerging & Sustainable Technologies for Power & ICT in a Developing Society (NIGERCON)* (pp. 96–100). Owerri, Nigeria: IEEE. DOI: 10.1109/NIGERCON.2013.6715643

Fauzi, A. H., & Khan, A. S. (2017). Threats advancement in primary user emulation attack and spectrum sensing data falsificationattack in cognitive radio network for 5G wireless network environment. *Journal of Telecommunication, Electronic and Computer Engineering*, *9*(2), 179–183.

Federal Communications Commission 03-322, F. (2002). *Spectrum policy task force report*. *Tech. Rep. ET Docket No. 02- 135*. Columbia, SC, USA, Tech.

Federal Communications Commission 03-322, F. (2003). *Notice of proposed rule making and order, ET docket No. 03-108*. Washington, D.C. 20554. USA

Fihri, W. F., Arjoune, Y., Ghazi, H. El, Kaabouch, N., Abou, B., & Majd, E. (2018). A particle swarm optimization based algorithm for primary user emulation attack detection. *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 823–827). Las Vegas, USA.: IEEE. DOI: 10.1109/CC WC.2018.8301616

Gelabert, X., Sallent, O., Pérez-romero, J., & Agustí, R. (2010). Spectrum sharing in cognitive radio networks with imperfect sensing : A discrete-time Markov model. *Journal of Computer and CommunicationsComputer Networks*, *54*(14), 2519–2536. https://doi.org/10.1016/j.comnet.2010.04.005

Ghanem, W. R. & Shokair, M. D. (2016). An improved primary user emulation attack detection in cognitive radio networks based on firefly optimization algorithm. *National Radio Science Conference* (pp. 178–187). Aswan, Egypt: IEEE.doi: 10.1109/NRSC.2016.7450851

Giral, D., & Hern, C. (2020). Spectrum decision-making in collaborative cognitive radio networks. *MDPI Journal of Applied Sciences*, *10*(6786), 1–23. https://doi.org/doi: 10.3390/app10196786

Goyal, P., Buttar, A. S., & Goyal, M. (2016). An efficient spectrum hole utilization for transmission in cognitive radio networks. *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 322–327). Noida, India: IEEE. DOI**:** 10.1109/SPIN.2016.7566712

Gupta, A. & Onumanyi, A. J. (2019). Performance analysis of dynamic threshold estimation techniques based on the one-tier cognitive radio network. *Journal of Computer and Communications*, *7*(2), 31–46. https://doi.org/ 10.4236/ jcc.2019. 7 2003

Gupta, M., Verma, G., & Dubey, R. K. (2016). Cooperative spectrum sensing for cognitive radio based on adaptive threshold. 2nd *International Conference on Computational Intelligence & Communication Technology* (pp. 444–448). Ghaziabad, India: IEEE. https://doi.org/10.1109/CICT.2016.94

Haji, M. F. Mehmet, A. A. Mahmoud, N. & Hüseyin, A. (2020). Primary user emulation and jamming attack detection in cognitive radio via sparse coding. *EURASIP Journal on Wireless Communications and Networking, 2020*(141), 1–19. https://doi.org/https://doi.org/10.1186/s13638-020-01736-y

Hajiabadi, M., Khoshbin, H., & Hodtani, G. A. (2017). Cooperative spectrum estimation over large scale cognitive radio networks. *IET Signal Processing, 11*(8), 1006–1014. https://doi.org/10.1049/iet-spr.2016.0727

Han, W., Li, J., Tian, Z., & Zhang, Y. (2010). Efficient cooperative spectrum sensing with minimum overhead in cognitive radio. *IEEE Transactions on Wireless Communications*, *9*(10), 3006–3011.doi:10.1109/twc.2010.080610.100317

Jin, F., Varadharajan, V., & Tupakula, U. (2015). Improved detection of primary user emulation attacks in cognitive radio networks. *2015 International Telecommunication Networks and Applications Conference (ITNAC)* (pp.274–279). Sydney, Australia: IEEE.https://doi.org/10.1109/ATNAC.2015.7366825

Kang, B. (2009). Spectrum sensing issues in cognitive radio networks. *International Symposium on Communications and Information Technologies (ISCIT 2009)* (pp. 824–828). Incheon, Korea: IEEE.

Kanti, M., Barma, D., Singh, H., Roy, S., &Sen, S. K. (2015). Augmented spectrum sensing in cognitive radio networks. *International Journal of Computer Science and Network*, *4*(6), 838–846.

Kaur, M. J., Uddin, M., & Verma, H. K. (2010). Performance evaluation of QoS parameters in cognitive radio using genetic algorithm. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *4*(10), 1592–1597.

Khaliq, S. B. A., Amjad, M. F., Abbas, H., Shafqat, N., &Afzal, H. (2018). Defence against PUE attacks in adhoc cognitive radio networks : Amean field game approach.*JournalofTelecommunicationSystems*,*29(5)*, 1–18. https://doi.org/ 10. 1007/s11235-018-0472-y

Khudhair, A. A., Jabbar, S. Q., Sulttan, M. Q., & Wang, D. (2016). Wireless indoor localisation systems and techniques: Survey and comparative study. *Indonesian Journal of Electrical Engineering and ComputerScience*,*3*(2), 392–409. https://doi.org/10.11591/ijeecs.v3.i2.pp392-409

Kumar, A., & Singh, A. K. (2016). Range-based primary user localisation in cognitive radio networks. *Procedia Computer Science* (pp.199–206). Cochin, India: Elsevier Masson SAS. https://doi.org/10.1016/j.procs.2016.07.201

León, O., Hernández-serrano, J., & Soriano, M. (2012). Cooperative detection of primary user emulation attacks in CRNs. *Journal of Computer Networks*, *56*(56), 3374–3384. https://doi.org/10.1016/j.comnet.2012.05.008

Li, X., Deng, Z. D., Rauchenstein, L. T., Carlson, T. J.,& Deng, Z. D. (2016). Contributed review : Source-localisation algorithms and applications using time of arrival and time difference of arrival measurements. *Review of Scientific Instruments*, *87*(41502), 1–12. https://doi.org/10.1063/1.4947001

Li, Y., Pateromichelakis, E., Vucic, N., Luo, J., Xu, W., & Caire, G. (2017). *Radio Resource Management Considerations for 5G Millimeter Wave Backhaul andAccessNetworks*, *2017*(6), 86-92. https://doi.org/10.1109/ MCOM. 2017.1601118

Liang, Y., Member, S., Zeng, Y., Member, S., Peh, E. C. Y., & Hoang, A. T. (2008). Sensing-throughput tradeoff for cognitive radio networks. *IEEE Trasanctions on Wireless Communications*, *7*(4), 1326–1337.

Lin, P., Chen, Y., Chang, P., & Jeng, S. (2018). Cooperative spectrum sensing and optimization on multi-antenna energy detection in rayleigh fading channel. *27th Wireless and Optical Communications Conference (WOCC2018)* (pp. 13–17). Taiwan, China: IEEE.doi: 10.1109/WOCC.2018.8372735.

Lin, S., & Wen, C. (2016). A device-based secure scheme against PUEA attacks in cognitive radio sensor networks. *International Journal of Communications, 1*(1), 117–126.

Mabrook, M. M. &, Hussein, A. I. (2015). Major spectrum sensing techniques for cognitive radio networks : A survey. *International Journal of Engineering and Innovative Technology (IJEIT), 5*(3), 24–37.

Malik, S. A., Shah, M. A., Dar, A. H., Haq, A., Ullah, A., & Javed, T. (2010). Comparative analysis of primary transmitter detection based spectrum sensing techniques in cognitive radio systems. *Australian Journal of Basic and Applied Sciences, 4*(9), 4522–4531.

Maninder, S., Pradeep K., &Anusheetal D. (2016). Techniques for Spectrum sensing in cognitive radio networks : Issues and challenges. *International Research Journal of Engineering and Technology (IRJET),3*(5), 153–159.

Marinho, J., Granjal, J., & Monteiro, E. (2015). A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. *EURASIPJournal-on-Information-Security, 2015*(4),1–14. https://doi.org/ 10. 1186/s13635-015-0021-0

Mergu, K. (2019). Combating PUE attack in cognitive radio networks using RSSI based EKFandUKF.*InternationalJournal of Engineering and Advanced Technology (IJEAT), 9*(2), 5108–5114. https://doi.org/10.35940/ijeat.B3886.129219

Mrabet, Z. El, Arjoune, Y., Ghazi, H. El, Abou, B., & Majd, A. (2018). Primary user emulation attacks : A detection technique based on kalman filter. MDPI *Journal of Sensor and Actuator Networks*, 7(26), 1–14. https://doi.org/10.3390/jsan7030026

Muñoz, E. C., Fernando, L., Mart, P., Eduardo, J., & Triviño, O. (2020a). Detection of malicious primary user emulation based on a support vector machine for a mobile cognitive radio network using software-defined radio. *Journal of MDPI Journal of Electronics, 9*(1282), 1–17. https://doi.org/doi:10.3390/electronics9081282

Muñoz, E. C., Rodriguez-colina, E., Pedraza, L. F., & Paez, I. P. (2020b). Detection of dynamic location primary user emulation on mobile cognitive radio networks using USRP. *EURASIP Journal on Wireless Communications and Networking*, *2020*(53). https://doi.org/https://doi.org/10.1186/s13638-020-1657-0

Nilesh, R. C. & Patil, Y. M. (2014). Attacks and detection in cognitive radio system. *International Journal of Emerging Engineering Research and Technology*, *2*(4), 223–233.

Penna, F., & Cabric, D. (2013). Cooperative DoA-only localisation of primary users in cognitive radio networks. *EURASIP Journal on Wireless Communications and Networking,2013*(107),1–14. https://doi.org/10.1186/1687-1499-2013-107

Piasana, F,. &Marchetti N. (2014). Radar, TV, Cellular bands: Which Spectrum access techniques fro which bands. *IEEE Communication Surveys and Tutorials*, *13*(3), 1193–1220. https://doi.org/10.1109/SURV.2014031914.00078

Rappaport, T. S. (2002). *Wireless Communication Principles and Practice*. USA: Person Education Limited.

Rehman, A. (2019). Detection of primary user emulation attack in cognitive radio networks based on TDOA using grey wolf optimizer. *International Journal of ComputerSciences and Engineering.*7(2), 332–337. https://doi.org/ 10. 64 38 /ijcse/v7i2.332337

Rharras, A., Saber, M., Chehri, A., Saadane, R., Hakem N.,& Jeon, G.R. (2020). Optimization of spectrum utilization parameters in cognitive radio using genetic algorithm radio. *Procedia Computer Science* (pp. 2466–2475). Verona

Italy: Elsevier B.V. https://doi.org/10.1016/ j.procs. 2020. 09.328

Saeed A., Young D. L., Seung H. H., & Insoo K. (2017). A cognitive radio-based energy-efficient system for power transmission line monitoring in smart grids . *Hindawi Journal of Sensors*, 2017(1), 1-12. https: //doi.org/ 10.1155/ 2017/ 3 8 62375

Saeed, N., Nam, H., Al-naffouri, T. Y., & Alouini, M. (2019). Primary user localisation and its error analysis in 5G cognitive radio networks. *MDPI Journal of Sensor Networks*, 19(2035), 1–12. https://doi.org/10.3390/s19092035

Salama, U., Sarker, P. L., & Chakrabarty, A. (2018). Enhanced energy detection using matched filter for spectrum sensing in cognitive radio networks. *2018 Joint 7th International Conference on Informatics, Electronics & Vision (ICIEV) and 2018 2nd International Conference on Imaging, Vision &Pattern Recognition (icIVPR)* (pp.185–190). Japan: IEEE. https://doi.org/10.1109/ICIEV.2018.8641079

Shakshuki, E., Abu, A., Nemer, I., & Adam, M. (2019). Comparative study on range free localisation algorithms. *Procedia Computer Science* (pp. 501–510). Leuven, Belgium: Elsevier B.V. https://doi.org/10.1016/j.procs.2019.04.068.

Sharifi, A. A., Sharifi, M., & Niya, M. J. M. (2015). Secure collaborative spectrum sensing in the presence of primary user emulation attack in cognitive radio networks. *Amirkabir International Journal of Science & Research (Electrical and Electronics Engineering)*,*47*(2), 1–8.https://www.sid.ir/en/journal/ View Paper .asx?id=543042

Sharma, G., & Sharma, R. (2017). Distributed cooperative spectrum sensing over different fading channels in cognitive radio. *17th International Conference on Computer, Communications and Electronics (Comptelix)* (pp. 107–111). Jaipur, India: IEEE.

Shrivastava, S., Rajesh, A.,&Bora, P. K. (2018). Defense against primary user emulation attacks from the secondary user throughput perspective. *International Journal of Electronics Communication. (AEÜ)*, *84*(11), 131–143. https://doi. org/ 10.1016/j.aeue.2017.11.012

Souza, P. H. C., Guimar, D. A., & Aquino, G. P. (2018). Efficient fusion of spectrum sensing information under parameter uncertainty and impulsive noise. *Journal of Communication and Information Systems*, *33*(1), 37–45. doi: 10.1109/98.788210.

Srinivasan, S., Shivakumar, K. B., & Mohammad, M. (2019). Semi-supervised machine learning for primary user emulation attack detection and prevention through core-based analytics for cognitive radio networks. *International Journal of Distributed Sensor Networks*, *15*(9), 1–12. https://doi.org/10.1177/1550147719860365

Stotas, S., & Nallanathan, A. (2010). On the throughput maximization of spectrum sharing cognitive radio networks. In *IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings* (pp. 0–4). IEEE.

Subhedar, M., & Birajdar, G. (2011). Spectrum sensing techniques in cognitive radio networks: A survey. *International Journal of Next-Generation Networks (IJNGN), 3*(2), 37–51. https://doi.org/10.5121/ijngn.2011.3203

Sultana, R., & Hussain, M. (2018). Mitigating primary user emulation attack in cognitive radio network using localisation and variance detection. *Proceedings of First International Conference on Smart System, Innovations and Computing, Smart Innovation, Systems and Technologies* (pp. 433–444). Singapore: Springer Nature.

Treeumnuk, D., Macdonald, S. L., & Popescu, D. C. (2013). Optimizing performance of cooperative sensing for increased spectrum utilization in dynamic cognitive radio systems. In *IEEE ICC 2013 - Signal Processing for Communications Symposium Optimizing* (pp. 4656–4660). Budapest, Hungary: IEEE.

Unnikrishnan, J. & Veeravalli, V. (2008). Cooperative sensing for primary detection in cognitive radio. *IEEE Journal of Selectied Topics In Signal Processing*, *2*(1), 18–27.https://*doi*.org/10.1109/JSTSP.2007.914880.

Vadivelu, R., Sankaranarayanan, K., & Vijayakumari, V. (2014). Matched filter based spectrum sensing for cognitive radio at low signal to noise ratio. *Journal of Theoretical and Applied Information Technology*, *62*(1), 107–113.

Vasanthareddy, R. M. & Sanjeev, C. L. (2021). Detection and prevention of primary user emulation attack in cognitive radio networks using secure hash algorithm. *International Journal of Intelligent Engineering and Systems*, *14*(2), 136–146. https://doi.org/10.22266/ijies2021.0430.12

Verma, G., Dhage, V., & Chauhan, S. S. (2018). Analysis of combined data-decision fusion scheme for cognitive radio networks. *2018 2nd International Conference on Inventive Systems and Control (ICISC),* 1324–1327.http://dx. doi. org/ 10. 1109 /ICISC.2018.8399021

Vu, M., Devroye, N., & Tarokh, V. (2009). On the primary exclusive region in cognitive networks. *IEEE Transactions on Wireless Communications*, 8(7), 3380–3385).doi: 10.1109/TWC.2009.080454.

Xie, X., Wang, W., & Charlotte, U. N. C. (2013). Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding. In *Procedia - Procedia Computer Science* (Vol. 21, pp. 430–435). Ontario, Canada: Elsevier Masson SAS. https://doi.org/10.1016/j.procs.2013.09.057

Yadav, K., Sanjay R. D., & Kundu, S. (2018). Total error reduction in presence of malicious user in a cognitive radio network. In *2nd International Conference on Electronics, Materials Engineering and Nano-Technology (IEMEMTech)* (pp. 4–7). Kolkata, India: IEEE. https://doi.org/10.1109/IEMENTECH.2018.8465260

Yang, L., Song, S. H., & Letaief, K. B. (2012). Optimizing spectrum sensing efficiency in cognitive radio networks. In *Proc. of IEEE Computing, Communication and Applications Conference* (pp. 262–266). Budapest, Hungary: IEEE.

https://doi.org/10.1109/ComComAp.2012.6154854

Yu, R., Yan, Z., Liu, Y., Gjessing, S.,& Guizani, M. (2015). Securing cognitive radio networks against primary user emulation attacks. *IEEE Network*, *29*(4), 68–74.doi: 10.1109/MNET.2015.7166193.

Yuan, Z., Niyato, D., Li, H., Song, J. Bin, & Han, Z. (2012). Detecting primary user emulation attacks using belief propagation in cognitive radio networks. *IEEE Journal on Selected Areas in Communication*, *30*(10), 1850–1860.doi: 10.1109/JSAC.2012.121102.

Zeng, Y., Liang, Y., & Zhang, R. (2008). Blindly combined energy detection for spectrum sensing in cognitive radio. *IEEE Signal Processing Letters*, *15*(2008), 649–652.doi:10.1109/lsp.2008.2002711

Zhang, J., & Lili, C. S. (2017). Malicious cognitive user identification algorithm in centralized spectrum sensing system. *Future Internet*, *9*(79), 1–13. https:// doi. org/ 10.3390/fi9040079

Zina, C. & Noureddine, H. (2015). A survey on spectrum management in cognitive radio networks. *International Journal of Wireless and Mobile Computing*, *8*(2), 153–165.https://doi.org/10.1504/IJWMC.2015.068618

APPENDICES

Appendix A: Summary of Related Works on Primary User Emulator

S/N	Title	Author(s)	Metrics	Strength	Weakness
1.	Defense against Primary User Emulation Attacks in Cognitive Radio Networks	Chen *et al.*, (2008)	Received power	It identifies PUE attacks in hostile CR environment and localises it	It did not consider localizing mobile and low power transmitter.
2.	Cooperative DoA-only localisation of primary users in cognitive radio networks	Penna & Cabric, (2013)	Direction of arrival of signal	It does not depend on distance. It has antenna on all the sensors. This enables higher localisation accuracy.	Equipping all the sensor in the network is highly expensive. Using fewer sensors-equipped antenna that are optimally position will be less expensive
3.	Detection of PUE Attacks in Cognitive Radio Networks Based on Signal Activity Pattern	Chunsheng & Song, (2014)	Signal features	Advance information about the PU is not required. It is applicable to both static and mobile PU.	It can only detect single PU. But cannot detect multiple PU.
4.	Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard	Ahmed *et al.*, (2014)	Received Signal Strength	It is less financially expensive as no additional hardware is required. When applied directly to today's DTV, it is highly efficient for spectrum sharing.	It requires plug-in Advanced Encryption Standard (AES) chip. This makes it complex. The plug-in AES chip can lead to compatibility issues with other hardware components
5.	Detection Threats and Mitigation	Ammar *et al.* (2015)	Measured distance based on	It successfully ensures trustworthiness	It did not consider RSS of varying frequency to

	Techniques in Cognitive Radio based on Localisation of Signal Source and trustworthiness		location coordinates and received signal strength	among nodes in cognitive radio network by distinguishing primary and malicious users.	localise transmitters at different locations
6.	Detecting primary user emulation attacks based on PDF-BP algorithm in cognitive radio networks	Chen*et al.* (2016)	Density function and signal propagation	Secondary user (SU) does not need location information of the PU for its detection process. It does not require extra hardware.	Detection is inaccurate since each SU carries out detection independently.
7.	Primary User Emulation Attacks: A Detection Technique Based on Kalman Filter	Mrabet *et al.*, (2018)	Measured Received Signal Strength	It uses Kalman filter frame work to track the position mobile PU. It is able to detect PUE attacks on non-stationary PU	It considered free space propagation model. It difficult to be applied in a cluttered environment. It could not find the initial coordinates of the PU. It cannot detect attackers that are very close to the PU.
8.	Defence against PUE attacks in adhoc cognitive radio networks: a mean field game approach	(Khaliq *et al.*, 2018)	Transmitter location	It allows detection of attacks by each node without additional cost. With a mean field game approach. It also detects multiple PUE and applicable in distributed manner	It cannot be implemented on vehicular CR ad hoc networks. It did not consider other game theoretic approaches.
9.	Primary user emulation and jamming attack detection in cognitive radio via sparse	Haji, *et al*, (2020)	Received signal	Accurately detected PUE.	Only outperforms energy detection-based Machine learning techniques. Not applicable in other detection

	coding				techniques.
10.	Detection and Prevention of Primary User Emulation Attack in Cognitive Radio Networks Using Secure Hash Algorithm	VasanthaReddy & Sanjeev, (2021)	Received power	Accurate detection	Inclusion of secured Harsh Algorithm (SHA) makes the algorithm complex and expensive. Unable to isolate the detected PUE from the network

Appendix B: List of Published and On-Going Papers from Thesis

A number of papers have been published from this research. We present in the table below, a list of the papers published.

S/N	Paper Title	Paper Type	Status	Place of Publication	Rating
1	A Survey of Range-Based Techniques for Localizing Primary User Emulators in Cognitive Radio Network	Conference	Published	Proceeding on Big Data Analytics & Innovation vol.1, pp192-198	
2	A Hybrid Scheme for Localizing Rogue Secondary User in a Mobile Cognitive Radio Network	Conference	Published	2nd International Engineering Conference (IEC2017), Federal University of Technology, Minna, Nigeria pp 266-270	-
3	A Hybrid Localisation Scheme for Detection of Primary User Emulator in Cognitive Radio Networks	Journal	Published	International Journal of Computing and Digital Systems ISSN (2210-142X) Int. J. Com. Dig. Sys. 8, No.3 (May-2019) http://dx.doi.org/10.12785/ijcds/080302.	Q2
4	Cooperative-hybrid Detection of Primary User Emulators in Cognitive Radio Networks	Journal	Published	International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No.3, June 2020, pp. 1 – 9 ISSN: 2088-8708 DOI :http://DOi.org/10.11591/ijece.v10i3	Q2
5	Isolation of Primary User Emulator in Cognitive Radio Network	Journal	In progress		
6	Hybrid Localisation of Mobile Primary User in Cognitive Radio Network	Journal	In progress	-	

Appendix C: Codes for Hybrid of AOA and RSS Schemes for Localising PUE in CRNS

```
close all;
clear all;
clc
z=15
for v=1:z

t1=1; u1=4;
t2=1; u2=9;

t3=4; u3=6;
t4=1; u4=4;

t5=6; u5=9;
t6=1; u6=9;

t7=4; u7=6;
t8=6; u8=9;

x1=t1+(u1-t1)*rand(1,1)
 y1=t2+(u2-t2)*rand(1,1)

 xc2=t3+(u3-t3)*rand(1,1)
 yc2=t4+(u4-t4)*rand(1,1)

 xc3=t5+(u5-t5)*rand(1,1)
 yc3=t6+(u6-t6)*rand(1,1)

 xc4=t7+(u7-t7)*rand(1,1)
 yc4=t8+(u8-t8)*rand(1,1)


 x2=t1+(u1-t1)*rand(1,1)
 y2=t2+(u2-t2)*rand(1,1)
 p1(:,v)=x1;
 p2(:,v)=y1;


 p3(:,v)=xc2;
 p4(:,v)=yc2;

 p5(:,v)=xc3;
 p6(:,v)=yc3;

 p7(:,v)=xc4;
 p8(:,v)=yc4;

X=5; Y=5; %position of the PU
%Position of SU1 and SU2 respectively
k=20;%Number of samples of RSS taken
pt=80; %Transmit power of PU
pt_pue=50; %Transmit power of PUE
Ploss_do=1;%pathloss within the reference distance
n1=3; n2=4%loss exponent
```

```
a=15; b=25;%Received power is between 60dB and 75dB
r=20;% radius of PER in metres
R=70; %Radius of coverage of PU in metres
l=100;% length of design space
j=20;% Number of RSS sampled

%x1_arr = zeros(150,1);
%%Zy1_arr = zeros(150,1);
%y2_arr = zeros(150,1);
s1=abs(sqrt((X-x1)^2+(Y-y1)^2));% Distance between SU1 and PU
s2=abs(sqrt((X-x2)^2+(Y-y2)^2));% Distance between SU2 and PU
D=abs(sqrt((x2-x1)^2+(y2-y1)^2))%Distance between SU1 and SU2



k=20;
for q=1:k
    pr1(:,q)=a+(b-a)*rand(1,1);%RSS of SU1 from PUE
end
    m1=(1/k).*sum(pr1);%mean of the RSS of SU1 from PUE

for p=1:k
    pr2(:,p)=a+(b-a)*rand(1,1);%RSS
end
     m2=(1/k).*sum(pr2);%mean of the RSS RSS of SU2 from PUE

for p=1:k
    pr3(:,p)=a+(b-a)*rand(1,1);%RSS
end
     m3=(1/k).*sum(pr3);

for p=1:k
    pr4(:,p)=a+(b-a)*rand(1,1);%RSS
end
     m4=(1/k).*sum(pr4);

for p=1:k
    pr5(:,p)=a+(b-a)*rand(1,1);%RSS
end
     m5=(1/k).*sum(pr5);

for p=1:k
    pr6(:,p)=a+(b-a)*rand(1,1);%RSS
end
     m6=(1/k).*sum(pr6);

     rss_su1(:,v)=m1%a set of received powers from of SU1 from PUE
     rss_su2(:,v)=m2%a set of received powers from of SU2 from PUE
     rss_su3(:,v)=m3%a set of received powers from of SU3 from PUE
     rss_su4(:,v)=m4%a set of received powers from of SU4 from PUE
     rss_su5(:,v)=m5%a set of received powers from of SU5 from PUE
     rss_su6(:,v)=m6%a set of received powers from of SU6 from PUE

     n=n1+(n2-n1)*rand(1,1);%loss exponent
d1=10^((pt_pue-m1-Ploss_do)/(10*n))%Distance between SU1 and PUE
d2=10^((pt_pue-m2-Ploss_do)/(10*n))%Distance between SU2 and PUE

X1(:,v)=x1
Y1(:,v)=y1
X2(:,v)=x2
```

```
Y2(:,v)=y2

pu_su1_set(:,v)=s1 % a set of distances between PU and SU1
pu_su2_set(:,v)=s2 % a set of distances between PU and SU1
dis_su1_pue(:,v)=d1
dis_su2_pue(:,v)=d2
dis_su1_su2(:,v)=D

phi(:,v)=acosd((s1^2+D^2-s2^2)./(2*s1*D));%angle between su1 and pu
theta(:,v)=180-acosd((s2^2+D^2-s1^2)./(2*s2*D))%angle between su2 and
pu
alpha1=acosd((d1^2+D^2-d2^2)./(2*d1*D));%angle between su1 and PUE
beta1=180-acosd((d2^2+D^2-d1^2)./(2*d2*D));
xe=(x1*tan(alpha1)-x2*tan(beta1)-y1+y2)/(tan(alpha1)-tan(beta1));
ye=tan(alpha1)*xe-x1*tan(alpha1)+y1;
Xe(:,v)=xe
Ye(:,v)=ye
alp(:,v)=alpha1
bet(:,v)=beta1%angle between su2 and PUE

%m_d2=sum(dis_su2_pue)/z;
%ms_d2(:,v)=(m_d2-d2)^2
%m_alpha=sum(alpha)/z;
%ms_alpha(:,v)=(m_alpha-alpha)^2;
%m_beta=sum(beta)/z;
%ms_beta(:,v)=(m_beta-beta)^2;

%phi=atan((Y-yi)./(X-xi));%AoA of RSS at ith SU from PU
%theta=atan((Y-yi)./(X-xi));%AoA of RSS at ith SU from PU
%d=NaN(1:2);



%alpa=acos((d1)^2)+((D)^2)-((d2)^2)/(2*d1*d2);% AoA of RSS at SU2 from
PUE
%t=acos((d2)^2)+((D)^2)-((d1)^2)/(2*D*d2);% AoA between d2 and D
%beta=180-t;%AoA of RSS at SU2 from PUE
%Xe=(x1*tan(phi)-x2*tan(theta)+(y2-y1)/(x1*tan(phi)));%X-coordinate of
PUE
%Ye=(tan(phi)*((x1*tan(phi)-x2*tan(theta)+(y2-y1))/(x1*tan(phi)-
tan(theta))))-(x1*tan(phi)+y1);%Y-coordinate of PUE
%Emulator=[Xe Ye];
p=(l/2)-r;%lower boundary
s=(R/2)-r;%upper boundary

%for j=j+1
% SU1loc=p+(s-p)*rand(j,1);
%SU2loc=p+(s-p)*rand(j,1);
end
m_d1=sum(dis_su1_pue)/z;
m_d1_mat(1,1:z)=m_d1;
m_diff_d1=(m_d1_mat-dis_su1_pue);
squ_d1=m_diff_d1.^2;
var_d1=sum(squ_d1)/z
std_d1=sqrt(var_d1)

m_d2=sum(dis_su2_pue)/z;
m_d2_mat(1,1:z)=m_d2;
m_diff_d2=(m_d2_mat-dis_su2_pue);
squ_d2=m_diff_d2.^2;
```

```
var_d2=sum(squ_d2)/z
std_d2=sqrt(var_d2)

m_alpha=sum(alp)/z;
m_alpha_mat(1,1:z)=m_alpha;
m_diff_alpha=(m_alpha_mat-alp);
squ_alpha=m_diff_alpha.^2;
var_alpha=sum(squ_alpha)/z
std_alpha=sqrt(var_alpha)

m_beta=sum(bet)/z;
m_beta_mat(1,1:z)=m_beta;
m_diff_beta=(m_beta_mat-bet);
squ_beta=m_diff_beta.^2;
var_beta=sum(squ_beta)/z
std_beta=sqrt(var_beta)


%plot(pu_su1_set,su1_pr_pue);
figure;
th= 0:pi/50:2*pi;
r=5;
x=r*cos(th)+r;
y=r*sin(th)+r;
%subplot(2,2,1)
plot(x,y)
xlabel('x-axis');
ylabel('y-axis');
hold
th= 0:pi/100:2*pi ;
r=1;
x=r*cos(th)+5;
y=r*sin(th)+5;

plot(x,y);
hold on
plot(p1,p2,'rs');
hold on
plot(p3,p4,'rs');
hold on
plot(p5,p6,'rs');
hold on
plot(p7,p8,'rs');
hold on
plot(5,5,'k*');


xlswrite('Result_PhD.xlsx',transpose(X1),'Sheet1','A2')
xlswrite('Result_PhD.xlsx',transpose(Y1),'Sheet1','B2')
xlswrite('Result_PhD.xlsx',transpose(X2),'Sheet1','C2')
xlswrite('Result_PhD.xlsx',transpose(Y2),'Sheet1','D2')
xlswrite('Result_PhD.xlsx',transpose(dis_su1_su2),'Sheet1','E2')
xlswrite('Result_PhD.xlsx',transpose(rss_su1),'Sheet1','F2')
xlswrite('Result_PhD.xlsx',transpose(rss_su2),'Sheet1','G2')
xlswrite('Result_PhD.xlsx',transpose(pu_su1_set),'Sheet1','H2')
xlswrite('Result_PhD.xlsx',transpose(pu_su2_set),'Sheet1','I2')
xlswrite('Result_PhD.xlsx',transpose(dis_su1_pue),'Sheet1','J2')
xlswrite('Result_PhD.xlsx',transpose(dis_su2_pue),'Sheet1','K2')
xlswrite('Result_PhD.xlsx',transpose(phi),'Sheet1','L2')
xlswrite('Result_PhD.xlsx',transpose(theta),'Sheet1','M2')
xlswrite('Result_PhD.xlsx',transpose(alp),'Sheet1','N2')
xlswrite('Result_PhD.xlsx',transpose(bet),'Sheet1','O2')
xlswrite('Result_PhD.xlsx',transpose(Xe),'Sheet1','R2')
xlswrite('Result_PhD.xlsx',transpose(Ye),'Sheet1','S2')

xlswrite('Result_PhD.xlsx',var_d1,'Sheet1','C19')
xlswrite('Result_PhD.xlsx',std_d1,'Sheet1','C20')
xlswrite('Result_PhD.xlsx',var_d2,'Sheet1','F19')
xlswrite('Result_PhD.xlsx',std_d2,'Sheet1','F20')
xlswrite('Result_PhD.xlsx',var_alpha,'Sheet1','I19')
xlswrite('Result_PhD.xlsx',std_alpha,'Sheet1','I20')
xlswrite('Result_PhD.xlsx',var_beta,'Sheet1','L19')
xlswrite('Result_PhD.xlsx',std_beta,'Sheet1','L20')

xlswrite('Result_PhD.xlsx',transpose(rss_su1),'Sheet2','A2')
xlswrite('Result_PhD.xlsx',transpose(rss_su2),'Sheet2','B2')
xlswrite('Result_PhD.xlsx',transpose(rss_su3),'Sheet2','C2')
xlswrite('Result_PhD.xlsx',transpose(rss_su4),'Sheet2','D2')
xlswrite('Result_PhD.xlsx',transpose(rss_su5),'Sheet2','E2')
xlswrite('Result_PhD.xlsx',transpose(rss_su6),'Sheet2','F2')

%plot(SU1_PU,SU2_PU,'rs')
%subplot(2,2,2)
%plot(D,d1,'-rs')
%subplot(2,2,3)
%plot(D,d2,'-rs')
figure
[xx,yy]=meshgrid(X1,Y1);
zz=abs(sqrt((X-xx).^2+(Y-yy).^2));
%subplot(2,2,1)
%surf(xx,yy,zz);
%xlabel('X-axis of SU1')
%ylabel('Y-axis of SU1')
%zlabel('Distance between SU1 and PU')
subplot(2,2,1)
meshz(xx,yy,zz);
xlabel('X-axis of SU1')
ylabel('Y-axis of SU1')
zlabel('Distance between SU1 and PU')
subplot(2,2,2)
zze=meshgrid(dis_su1_pue)
meshz(xx,yy,zze);
rotate3d on
xlabel('X-axis of SU1')
ylabel('Y-axis of SU1')
zlabel('Distance between SU1 and PUE')
%xlabel('X-axis of SU1')
%ylabel('Y-axis of SU1')
%zlabel('Distance between SU1 and PU')
%subplot(2,2,4)
%mesh(xx,yy,zz);
%xlabel('X-axis of SU1')
%ylabel('Y-axis of SU1')
%zlabel('Distance between SU1 and PU')
%end
```

Appendix D: Codes to Evaluate Effects of Cooperative Sensing on the Detection of PUE Using the Developed Hybrid Scheme

```
close all;
```

```
clear all;
clc

x1=5;
y1=5;
x2=8;
y2=8;
X1=5.8519;
Y1=8.9881;

k=10;
z=10
u=10
pt_pue=50; %Transmit power of PUE
%C=[19.88;19.9;19.92;19.94;19.96;19.98;19.99;19.995;19.995;19.995];
% b=20.00099;

C=[19.97;19.98;19.99;19.991;19.992;19.993;19.994;19.995;19.999;19.999]
;
 b=20.00099;%Received power of hybrid
%a=18.5; b=19;%Received power of distance
%a=19.984; b=20;%Received power of AoA
Ploss_do=1;%pathloss within the reference distance
n=3;

for f=1:z
    a=C(f)
for v=1:z

for p=1:k
%pr1(:,q)=randi([a,b],1,1);%RSS of SU1 from PUE
    pr1(:,p)=a+(b-a)*rand(1,1);
end
    m1=(1/k).*sum(pr1)%mean of the RSS of SU1 from PUE

for p=1:k
%pr2(:,p)=randi([a,b],1,1);%RSS
    pr2(:,p)=a+(b-a)*rand(1,1);
end
     m2=(1/k).*sum(pr2)%mean of the RSS RSS of SU2 from PUE

for p=1:k
%pr2(:,p)=randi([a,b],1,1);%RSS
    pr3(:,p)=a+(b-a)*rand(1,1);
end
     m3=(1/k).*sum(pr3)%mean of the RSS RSS of SU2 from PUE

for p=1:k
%pr2(:,p)=randi([a,b],1,1);%RSS
    pr4(:,p)=a+(b-a)*rand(1,1);
end
     m4=(1/k).*sum(pr4)%mean of the RSS RSS of SU2 from PUE

for p=1:k
%pr2(:,p)=randi([a,b],1,1);%RSS
    pr5(:,p)=a+(b-a)*rand(1,1);
end
     m5=(1/k).*sum(pr5)%mean of the RSS of SU2 from PUE

for p=1:k
```

```
%pr2(:,p)=randi([a,b],1,1);%RSS
    pr6(:,p)=a+(b-a)*rand(1,1);
end
     m6=(1/k).*sum(pr6)%mean of the RSS of SU2 from PUE

for p=1:k
%pr2(:,p)=randi([a,b],1,1);%RSS
    pr7(:,p)=a+(b-a)*rand(1,1);
end
     m7=(1/k).*sum(pr7)%mean of the RSS of SU2 from PUE

for p=1:k
%pr2(:,p)=randi([a,b],1,1);%RSS
    pr8(:,p)=a+(b-a)*rand(1,1);
end
     m8=(1/k).*sum(pr8)%mean of the RSS of SU2 from PUE

for p=1:k
%pr2(:,p)=randi([a,b],1,1);%RSS
    pr9(:,p)=a+(b-a)*rand(1,1);
end
     m9=(1/k).*sum(pr9)%mean of the RSS of SU2 from PUE

for p=1:k
%pr2(:,p)=randi([a,b],1,1);%RSS
    pr10(:,p)=a+(b-a)*rand(1,1);
end
     m10=(1/k).*sum(pr10)%mean of the RSS of SU2 from PUE

     Q=[m1;m2;m3;m4;m5;m6;m7;m8;m9;m10];
      P=sort(Q)
for T=1:9
         A(:,T)=(P(T)-P(T+1))*-1
end
     [B,I]=min(A)

     m1=P(9)
     m2=P(10)

D=abs(sqrt((x2-x1)^2+(y2-y1)^2));%Distance between SU1 and SU2
d1=10^((pt_pue-m1-Ploss_do)/(10*n));%Distance between SU1 and PUE
d2=10^((pt_pue-m2-Ploss_do)/(10*n));%Distance between SU2 and PUE
alpha1=acosd((d1^2+ D^2-d2^2)./(2*d1*D));%angle between su1 and PUE
beta1=180-acosd((d2^2+D^2-d1^2)./(2*d2*D));
xe=(x1*tan(alpha1)-x2*tan(beta1)-y1+y2)/(tan(alpha1)-tan(beta1));
Xe(:,v)=xe;
xe1(:,v)=(xe-X1).^2;
ye=tan(alpha1)*xe-x1*tan(alpha1)+y1;
Ye(:,v)=ye;
aoae(:,v)=(alpha1-al).^2;
ye1(:,v)=(ye-Y1).^2;
%Xee(:,v)=sqrt(xe1);
%Yee(:,v)=sqrt(ye1);
dse(:,v)=(d1-d).^2;
%drse(:,v)=sqrt(dse)
 m1=P(5)
 m2=P(6)

D=abs(sqrt((x2-x1)^2+(y2-y1)^2));%Distance between SU1 and SU2
d1=10^((pt_pue-m1-Ploss_do)/(10*n));%Distance between SU1 and PUE
```

```
d2=10^((pt_pue-m2-Ploss_do)/(10*n));%Distance between SU2 and PUE
alpha1=acosd((d1^2+ D^2-d2^2)./(2*d1*D));%angle between su1 and PUE
beta1=180-acosd((d2^2+D^2-d1^2)./(2*d2*D));
xe=(x1*tan(alpha1)-x2*tan(beta1)-y1+y2)/(tan(alpha1)-tan(beta1));
Xe(:,v)=xe;
xe2(:,v)=(xe-X1).^2;
ye=tan(alpha1)*xe-x1*tan(alpha1)+y1;
Ye(:,v)=ye;
aoae(:,v)=(alpha1-al).^2;
ye2(:,v)=(ye-Y1).^2;
%Xee(:,v)=sqrt(xe1);
%Yee(:,v)=sqrt(ye1);
dse(:,v)=(d1-d).^2;
%drse(:,v)=sqrt(dse)

 m1=P(1)
 m2=P(2)

D=abs(sqrt((x2-x1)^2+(y2-y1)^2));%Distance between SU1 and SU2
d1=10^((pt_pue-m1-Ploss_do)/(10*n));%Distance between SU1 and PUE
d2=10^((pt_pue-m2-Ploss_do)/(10*n));%Distance between SU2 and PUE
alpha1=acosd((d1^2+ D^2-d2^2)./(2*d1*D));%angle between su1 and PUE
beta1=180-acosd((d2^2+D^2-d1^2)./(2*d2*D));
xe=(x1*tan(alpha1)-x2*tan(beta1)-y1+y2)/(tan(alpha1)-tan(beta1));
Xe(:,v)=xe;
xe3(:,v)=(xe-X1).^2;
ye=tan(alpha1)*xe-x1*tan(alpha1)+y1;
Ye(:,v)=ye;
aoae(:,v)=(alpha1-al).^2;
ye3(:,v)=(ye-Y1).^2;
%Xee(:,v)=sqrt(xe1);
%Yee(:,v)=sqrt(ye1);
dse(:,v)=(d1-d).^2;
%drse(:,v)=sqrt(dse)

 m1=P(I)
 m2=P(I+1)

D=abs(sqrt((x2-x1)^2+(y2-y1)^2));%Distance between SU1 and SU2
d1=10^((pt_pue-m1-Ploss_do)/(10*n));%Distance between SU1 and PUE
d2=10^((pt_pue-m2-Ploss_do)/(10*n));%Distance between SU2 and PUE
alpha1=acosd((d1^2+ D^2-d2^2)./(2*d1*D));%angle between su1 and PUE
beta1=180-acosd((d2^2+D^2-d1^2)./(2*d2*D));
xe=(x1*tan(alpha1)-x2*tan(beta1)-y1+y2)/(tan(alpha1)-tan(beta1));
Xe(:,v)=xe;
xe4(:,v)=(xe-X1).^2;
ye=tan(alpha1)*xe-x1*tan(alpha1)+y1;
Ye(:,v)=ye;
aoae(:,v)=(alpha1-al).^2;
ye4(:,v)=(ye-Y1).^2;
%Xee(:,v)=sqrt(xe1);
%Yee(:,v)=sqrt(ye1);
dse(:,v)=(d1-d).^2;
%drse(:,v)=sqrt(dse)
m1=P(1)
 m2=P(10)

D=abs(sqrt((x2-x1)^2+(y2-y1)^2));%Distance between SU1 and SU2
d1=10^((pt_pue-m1-Ploss_do)/(10*n));%Distance between SU1 and PUE
d2=10^((pt_pue-m2-Ploss_do)/(10*n));%Distance between SU2 and PUE
```

```
alpha1=acosd((d1^2+ D^2-d2^2)./(2*d1*D));%angle between su1 and PUE
beta1=180-acosd((d2^2+D^2-d1^2)./(2*d2*D));
xe=(x1*tan(alpha1)-x2*tan(beta1)-y1+y2)/(tan(alpha1)-tan(beta1));
Xe(:,v)=xe;
xe5(:,v)=(xe-X1).^2;
ye=tan(alpha1)*xe-x1*tan(alpha1)+y1;
Ye(:,v)=ye;
aoae(:,v)=(alpha1-al).^2;
ye5(:,v)=(ye-Y1).^2;
%Xee(:,v)=sqrt(xe1);
%Yee(:,v)=sqrt(ye1);
dse(:,v)=(d1-d).^2;
%drse(:,v)=sqrt(dse)

end
%drmse(:,f)=sqrt(sum(dse)/z);
%aoarmse(:,f)=sqrt(sum(aoae)/z);
Ex=sqrt(sum(xe1)/z);
Ey=sqrt(sum(ye1)/z);
RMSE1_max(:,f)=(Ex+Ey)/2

Ex2=sqrt(sum(xe2)/z);
Ey2=sqrt(sum(ye2)/z);
RMSE_mid(:,f)=(Ex2+Ey2)/2

Ex3=sqrt(sum(xe3)/z);
Ey3=sqrt(sum(ye3)/z);
RMSE_min(:,f)=(Ex3+Ey3)/2

Ex4=sqrt(sum(xe4)/z);
Ey4=sqrt(sum(ye4)/z);
RMSE_close(:,f)=(Ex4+Ey4)/2

Ex5=sqrt(sum(xe5)/z);
Ey5=sqrt(sum(ye5)/z);
RMSE_highest_lowest(:,f)=(Ex5+Ey5)/2

end

%{
xlswrite('Result_PhD.xlsx',transpose(rss_su1),'Sheet2','A3')
xlswrite('Result_PhD.xlsx',transpose(rss_su2),'Sheet2','B3')
xlswrite('Result_PhD.xlsx',transpose(rss_su3),'Sheet2','C3')
xlswrite('Result_PhD.xlsx',transpose(rss_su4),'Sheet2','D3')
xlswrite('Result_PhD.xlsx',transpose(rss_su5),'Sheet2','E3')
xlswrite('Result_PhD.xlsx',transpose(rss_su6),'Sheet2','F3')
xlswrite('Result_PhD.xlsx',transpose(rss_su7),'Sheet2','G3')
xlswrite('Result_PhD.xlsx',transpose(rss_su8),'Sheet2','H3')
xlswrite('Result_PhD.xlsx',transpose(rss_su9),'Sheet2','I3')
xlswrite('Result_PhD.xlsx',transpose(rss_su10),'Sheet2','J3')
%}
 %{
xlswrite('MSE.xlsx',transpose(dse),'Sheet1','G2')
xlswrite('MSE.xlsx',transpose(drmse),'Sheet1','F20')
%}

%{
xlswrite('MSE.xlsx',transpose(aoae),'Sheet1','H2')
xlswrite('MSE.xlsx',transpose(aoarmse),'Sheet1','J20')
%}
```

Appendix E: Codes for Isolating Detected PUE

```
close all;
t=100; %sensing time
c=6.66; %channel capacity
pf=0.2; %Probability of false alarm
ho=0.8; %Probability of PU’s absence

forti=5:25 %transmission time increases
   G1(ti,:)=ti/(t+ti)*c*(1-pf)*ho
   G2(ti,:)=ti/(t+ti)*c*(1)*ho
T(ti,:)=ti
end

plot(T,G2,'*b-')
hold
plot(T,G1,'*r-')

xlabel('Trasmission time (ms)')
ylabel('Throughput')
legend('Without PUE','With PUE')
grid on



t=100; %transmission time
c=6.66; %channel capacity
ho=0.8; %Probability of absentism of PU
ti=5;


 PF=[0:0.2:1]%Probability of false alarm increase

   G1=ti/(t+ti)*c*(1-PF)*ho

plot(PF,G1,'*b-')

xlabel('Probability of false alarm')
ylabel('Throughput')

grid on
```