Security and Performance Engineering of Scalable Cognitive Radio Networks

By

E. E. CHUKU

PhD

University of Bradford

2019

Security and Performance Engineering of Scalable Cognitive Radio Networks

Sensing, Performance and Security Modelling and Analysis of 'Optimal' Trade-offs for Detection of Attacks and Congestion Control in Scalable Cognitive Radio Networks

Ejike Einstein CHUKU

Submitted for the degree of

Doctor of Philosophy

School of Engineering and Informatics

University of Bradford

2019

Abstract

Ejike Einstein CHUKU

Security and Performance Engineering of Scalable Cognitive Radio Networks.

Sensing, Performance and Security Modelling and Analysis of 'Optimal' Trade-offs for Detection of Attacks and Congestion Control in Scalable Cognitive Radio Networks.

***K* eywords:** Security, performance, scalability, sensing, congestion, trade-offs.

***A* Cognitive Radio Network (CRN)** is a technology that allows unlicensed users to utilise licensed spectrum by detecting an idle band through sensing. However, most research studies on CRNs have been carried out without considering the impact of sensing on the performance and security of CRNs.

Sensing is essential for secondary users (SUs) to get hold of free band without interfering with the signal generated by primary users (PUs). However, excessive sensing time for the detection of free spectrum for SUs as well as extended periods of CRNs in an insecure state have adverse effects on network performance. Moreover, a CRN is very vulnerable to attacks as a result of its wireless nature and other unique characteristics such as spectrum sensing and sharing. These attacks may attempt to eavesdrop or modify the contents of packets being transmitted and they could also deny legitimate users the opportunity to use the band, leading to underutilization of the spectrum space. In this context, it is often challenging to differentiate between networks under Denial of Service (DoS) attacks from those networks experiencing congestion.

This thesis employs a novel Stochastic Activity Network (SAN) model as an

effective analytic tool to represent and study sensing vs performance vs security trade-offs in CRNs. Specifically, an investigation is carried out focusing on sensing vs security vs performance trade-offs, leading to the optimization of the spectrum band's usage. Moreover, consideration is given either when a CRN experiencing congestion and or it is under attack. Consequently, the data delivery ratio (PDR) is employed to determine if the network is under DoS attack or experiencing congestion. In this context, packet loss probability, queue length and throughput of the transmitter are often used to measure the PDR with reference to interarrival times of PUs.

Furthermore, this thesis takes into consideration the impact of scalability on the performance of the CRN. Due to the unpredictable nature of PUs activities on the spectrum, it is imperative for SUs to swiftly utilize the band as soon as it becomes available. Unfortunately, the CRN models proposed in literature are static and unable to respond effectively to changes in service demands. To this end, a numerical simulation experiment is carried out to determine the impact of scalability towards the enhancement of nodal CRN sensing, security and performance. At the instant the band becomes idle and there are requests by SUs waiting for encryption and transmission, additional resources are dynamically released in order to largely utilize the spectrum space before the reappearance of PUs. These additional resources make the same service provision, such as encryption and intrusion detection, as the initial resources.

To this end, SAN model is proposed in order to investigate the impact of scalability on the performance of CRN. Typical numerical simulation experiments are carried out, based on the application of the Mobius Petri Net Package to determine the performance of scalable CRNs (SCRNs) in comparison with unscalable CRNs (UCRNs) and associated interpretations are made.

Declaration

I hereby declare that this thesis has been genuinely carried out by myself and has not been used in any previous application for a degree. Chapters 4 to 6 describe work performed, submitted and accepted in conferences and journals as shown in the publication list. The invaluable participation of others in this thesis has been acknowledged where appropriate.

Ejike Einstein CHUKU

Dedication

This thesis is dedicated to my beloved mum, my wife, my brothers and sisters whose love, help, support and prayers have contributed immensely to the success of this program.

Acknowledgements

I must first appreciate God almighty for giving me the opportunity and all that is required to undertake this research successfully. Without his supports, this milestone would not have been possible. My profound gratitude goes to my supervisor, Prof. Demetres D Kouvatsos, for all his patience, advice and guidance throughout the period of this research. But for his support and generosity, this success would not have been recorded. I am deeply indebted to my family for their love, prayers and encouragement. Knowing that I have their support made the process a lot easier. Many thanks to all my friends and relatives, who supported and encouraged me, in particular; Mr Aristotle Onumo, Rana Ahmed, Esmaeil HABIB ZADEH, Daniel Ekong, and Benedict Nkwo.

Publications

Ejike E. Chuku, Demetres D. Kouvatsos "Detection of Network Congestion and Denial of Service (DoS) Attacks in Cognitive Radio Networks", 2019 IEEE 7th International Conference on Future Internet of Things and Cloud (FiCloud).

Ejike E. Chuku, Demetres D. Kouvatsos, "Impact of Scalability on the Performance of Secured Cognitive Radio Networks", Electronic Notes in Theoretical Computer Science, Volume 340, 2018, Pages 123-135, ISSN 1571-0661.

Ejike C. and Kouvatsos, D., "Combined Sensing, Performance and Security Trade-offs in Cognitive Radio Networks," 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, 2017, pp. 1-4. doi: 10.1109/NCA.2017.8171335.

Ejike C. and Kouvatsos, D "Performance Evaluation of Service Channel Scalability on Cloud Platforms" UK Performance Engineering Workshop, University of Bradford, 2016

List of Abbreviations

ADC– Analogue-to-Digital Converter

AES– Advanced Encryption Standard

AFI– Abstract Functional Interface

CCR– Chaotic Cognitive Radio

CR– Cognitive Radio

CRCN– Cognitive Radio Cloud Network

CRN –Cognitive Radio Network

CSSPM –Combined Sensing, Security and Performance Metrics

CTS –Clear-to-Send

DC –Decision Centre

DoS –Denial of Service

FIFO –First Come First Served

GCS –Group Communication System

GSM –Global Scalability Manager

GSPN –Generalised Stochastic Petri Net

IaaS –Infrastructure as a Service

IoT –Internet of Things

LED –Loss due to Encryption Delay

LSD –Loss due to Sensing Delay

NCTS –Not Clear-to-Send

OFA –Objective Function Attacks

P(FA) –Probability of False Alarm

P(FNIB) –Probability of Not Finding Idle Band

P(PUOB) –Probability of PU Occupying Band

P(SD) –Probability of Spectrum Detection

PaaS –Platform as a Service

PDR –Packet Delivery Ratio

PLP –Packet Loss Probability

PSR –Packet Send Ratio

PU –Primary User

PUEA –Primary User Emulation Attack

PV –Performance Variables

QN –Queue Network

QoS –Quality of Service

RFID –Radio Frequency Identification

RSM –Regional Scalability Manager

SaaS –Software as s Service

SAN –Stochastic Activity Networks

SCRN –Scalable Cognitive Radio Networks

SLA –Service Level Agreement

SNR –Signal-to-Noise Ratio

SPN –Stochastic Petri Net

SSDF –Spectrum Sensing Data Falsification

SU –Secondary User

SVM –Support Vector Machine

TL –Total Packet Loss

UCRN –Unscalable Cognitive Radio Networks

UHF –Ultra High Frequency

VHF –Very High Frequency

Wi-Fi –Wireless Fidelity

Contents

Contents

xi

List of Tables

List of Figures

Chapter 1

Introduction

Research have shown that over 50 billion wireless devices will be connected to the internet by 2020 [1].These devices will be competing for available spectrum space. The traditional method of spectrum assignment assigns spectrum to only licensed users. This static spectrum assignment policy leads to under-utilization of the spectrum space in the face of spectrum demand [2]. To cope with the competing demand for spectrum by existing and emerging applications, regulatory bodies such as Office of Communication (Ofcom) and Federal Communication Commission (FCC) have allowed secondary users (SU) to share licensed spectrum with primary users (PU) on non-interference basis [2] - [7]. In sharing the spectrum band with PUs, they are two basic access scenarios: spectrum underlay and spectrum overlay. In spectrum underlay, SUs and PUs simultaneously transmit in the same band as long as the interference temperature is below a set level. However, in the overlay concept, the SUs are required to search for available spectrum space for the transmission of their requests.
In this thesis, the spectrum overlay is assumed. This context requires SUs to sense the band in effort to detect the status and decide to transmit or vacate if already transmitting. Sensing is carried out by cognitive radio network (CRN). CRN is a technology that probes through the band to detect its status and transmit the result of the sensing to SUs. Sensing introduces delays as CRN spend time searching and deciding the status of the band. Unfortunately, due to the wireless nature, CRN is very vulnerable to attacks. The two major forms of attacks identified in this work are the attacks that eavesdrops on or modify the content of packets on transmission and denial of service (DoS) attacks. The former eavesdrops and falsify data on transmission for its selfish objectives. In CRN, it involves the falsification of sensing data. Example of such attack is Byzantine attacks [8]. Jamming is an obvious

example of DoS attack [9]. The both forms of attacks lead to performance degradation. The rate at which attackers eavesdrop or falsify data on transmission depend on the strength of the security. One of the ways of protecting the data on transmission is by encryption. The data is first encrypted before it is transmitted. Research in [10] stated that the longer the encryption key length the stronger the security and vice-versa. However, long key lengths have performance implications. It consumes resources and degrade the network performance. It is therefore imperative to consider a tradeoff between sensing, security and performance. In tradeoffs, either security is compromised a bit for better performance or vice versa. Since the focus of this work is on CRN, the tradeoff in this context compromises sensing, security and performance. Therefore, either sensing is compromised for security and performance or security is compromised a bit for better spectrum detection and performance.

1.0.1 Motivation

While the existing works considered the pair of either sensing and throughput or performance and security in isolation, no reference was made to all the parameters together. For instance, [11] studied sensing-throughput tradeoff in CRN with no reference to security. [10] illustrates the modelling and analysis of the performance and security tradeoff using a combined performance and security model. However, this was not tailored to any specific network, as such, the effect of sensing was not considered. Similarly, [12] determines the optimal transmission power policy that maximizes the effect of security while considering the performance gain. Unfortunately, no reference was made to the effect of sensing in this context. Chapter 4 of this thesis considers the combined sensing, security and performance in CRN. The chapter aim to determine the sensing time at which the combined metrics of sensing, security and performance is optimum.

In practice, the three processes must exist together for a complete network functions. This implies that sensing, security or transmission processes cannot work in isolation. These functions are in tandem. The CRN must first sense the spectrum in search of idle spectrum space, followed by security checks and finally transmission.

Frequent security incidents as a result of short keys or long sensing time degrades network performance, leading to increase in queue length and packet loss. If the band become idle,

waiting SU requests would be forwarded for encryption and thereafter, transmission. Though the data rate of the band may be high (for example 5Mbps), however, the encryption rate of the security node may be the bottle-neck (say 2Mbps) as shown in Fig. 1.1

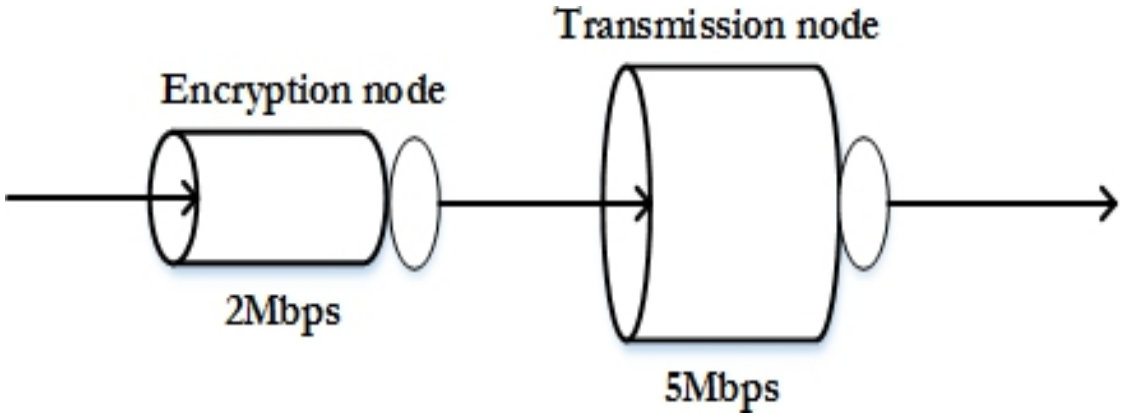

Figure 1.1: Data size illustrations

In this case, the band is underutilized. In order to manage the bursty traffic caused by prolonged wait for idle spectrum space and ensure optimal utilization of the band, scalability of the encryption resources is introduced. This involves creating additional resources and releasing same in any indication of heavy traffic measured by the queue length threshold. These resources are withdrawn when the traffic is back to normal. Chapter 5 explore the scalability features of cloud computing to manage the surge in service demand. It assesses the impact of scalability on the performance of CRN and compares the performance of scalable CRN (SCRN) with unscalable CRN (UCRN). The chapter also determines the sensing time at which the combined metrics for sensing, security and performance of Scalable Cognitive Radio Network (SCRN) is optimum.

When there is an increase in queue length or packet loss, it becomes challenging to determine if the network is under attack or experiencing congestion. This is mostly because the both processes induce similar effects in the network. These cases could lead to decline in throughput of SU. Though some researches mentioned congestion and the similar effects it has on the performance as jamming, no actual performance threshold is in place to predict a network experiencing congestion and distinguish it from one under attack. Chapter 5 proposes a packet delivery ratio (PDR) with numerical experimental to detect jamming attack

and differentiate it from network experiencing congestion. It also measures the PDR and depending on the result infer if the network is without attack, under attack or experiencing congestion.

1.0.2 Aims and Objectives

The aim of this research is to design a model-based simulation approach to:
Determine the tradeoff that offer no extremes but optimum value to the combined sensing, security and performance in a scalable and unscalable CRN
Introduce scalability in an attempt to improve the performance of CRN
Carryout network simulation and analysis to determine a network under DoS attack and differentiate from a network experiencing congestion. The objectives are as follows:
i) To translate the real system into modelling formalism for effective investigation of the behaviour.
ii) To use SAN quantitative analysis tool to determine the sensing time at which the combined metrics for sensing, security and performance are optimum.
iii) To propose a DoS attack detection mechanism that detects DoS attacks in CRN using SAN model.
iv) To determine the input values for effective management of priorities and likely pre-emptions that is expected in CRN.
v) To introduce into CRN, a sub-model that detects SU interference to PU signal.
vi) To add a redundant service channel to manage surge in service demand in the proposed SCRN.

1.0.3 Contributions

This work develops formalism for the analysis of SAN model and the extension of the application to the determination of sensing, security and performance tradeoff in a scalable and unscalable CRN. In this case, a CRN model is proposed with two classes of requests and priorities in a random selection discipline to abstract the behaviour of CRN with respect to sensing, security and performance. The sensing operation is modelled by enabling and firing

of a transition. This transition is connected to an output place of the arrival transition node and to the input place of the encryption transition node. The security control mechanism is modelled as suggested in [10]. The performance is determined by the interplay between sensing and security.

Scalability is introduced with experiments as contribution to assess the improvement in performance in comparison with unscalable CRN. In this context, a redundant service channel is proposed whose function depends on the change in service demand of SUs. This redundant channel comes into operation as the service demand increases and withdrawn otherwise. Replication and service migration is adopted to clone and transfer service to the redundant channel.

The work is also extended to include the use of SAN model for the abstraction of the network behaviour and to identify a CRN under attack and differentiate it from a network experiencing congestion. The model extends to include a sub-model with DoS detection mechanism. This mechanism involves attack detection and repairs represented by the rotation of tokens in different places.

1.0.4 Thesis Organisation

Chapter 2 presents the review of spectrum sensing, scalability and performance of CRN.

Chapter 3 introduces the methodology and network modelling tool used to determine the tradeoff between sensing, security and performance of CRN

Chapter 4 presents the simulation and analysis of combined sensing, security and performance tradeoff in CRN.

Chapter 5 introduces the impact of scalability on the performance of scalable and unscalable CRN

Chapter 6 presents the detection of network congestion and DoS attacks in CRN

Chapter 7 presents the conclusions and recommendations for future works

Chapter 2

Background and Literature Review

The advancements in the development of smart communication devices have exerted pressure on the limited spectrum resources [13]. In order to conserve the spectrum and ensure availability for new smart devices, regulatory bodies approved the use of Cognitive Radio (CR) in detection of idle bands. It is an emerging solution to sustain the availability of spectrum to aid the introduction of new technologies. Study in [8], [14] - [17] shows that large portions of spectrum allocated to PUs are not utilized in a wide range of locations as demonstrated in Fig.2.1.

The CRN is employed to enable SUs use the idle bands [18] and vacate on arrival of PUs request.This is as shown in 2.2,

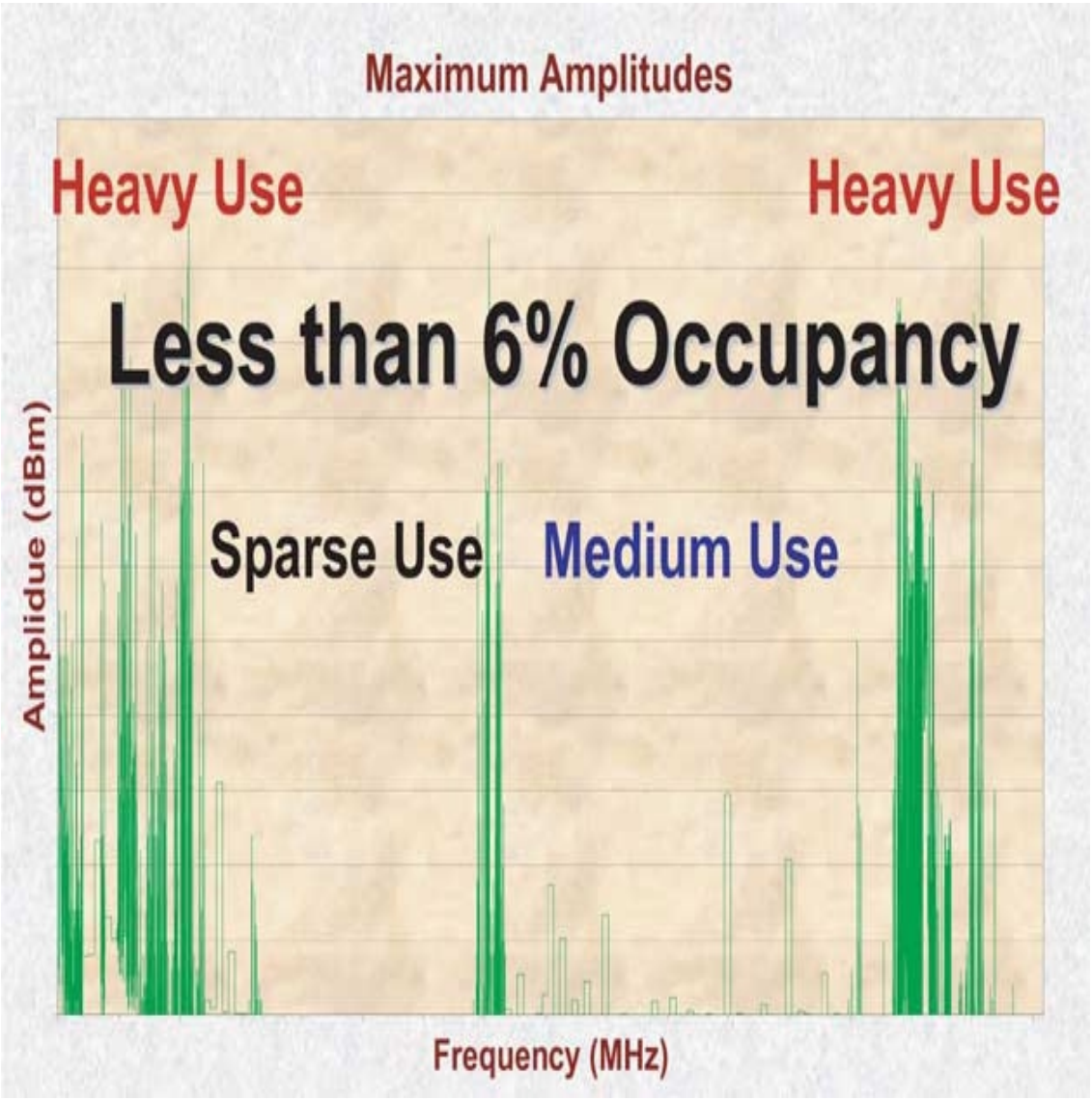

Figure 2.1: Illustration of spectrum occupancy [20]

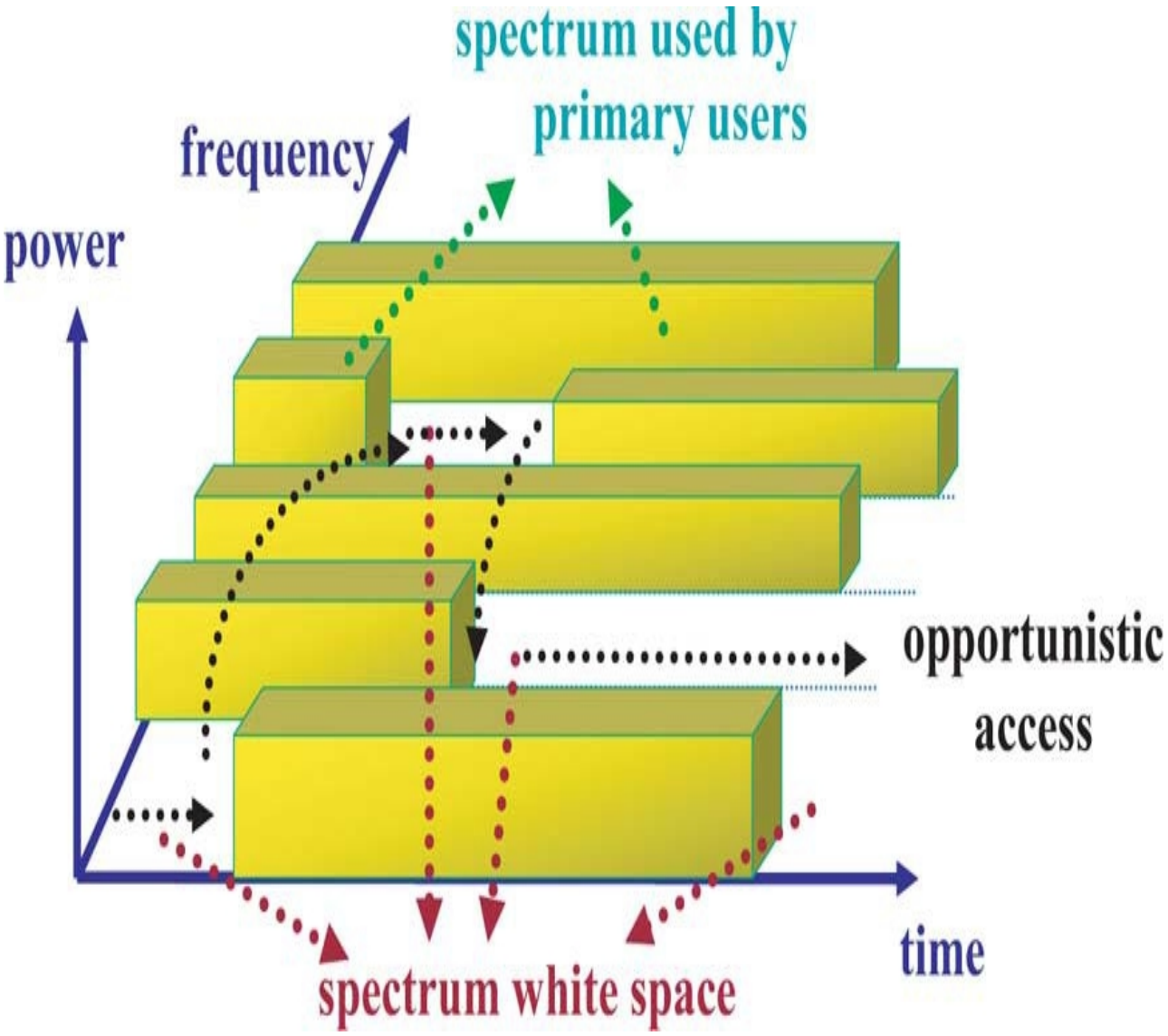

Figure 2.2: Illustration of spectrum idle space[20]

Since SU is required to relinquish the spectrum on appearance of PU, it implies that it must sense the environment to detect PU signal. For efficient protection of PUs, regulatory bodies recommend that the CR must sense the spectrum to about 0.9 probability of detecting the correct status of PU signal [19] [21]. CRN has four basic functions: spectrum sensing, spectrum decision, spectrum mobility and spectrum sharing.

2.0.1 Spectrum Sensing

Sensing is the method through which CRN determines the status of the spectrum band. CRN senses the spectrum independently or in cooperation where the outcome of the sensing is reported to a central database in an infrastructure-based network. Cooperative spectrum sensing is the collaboration of multiple CR in spectrum sensing in order to minimize total probability of errors [22]. In CR where there is no infrastructure, the ad hoc network is enabled to use the spectrum in a dynamic manner. It uses two or more wireless hops to convey information from source to destination. On finding an idle spectrum after sensing, CRN will immediately utilize it for data transmission. If SU is already transmitting during the arrival of PU request, it will suspend and vacate or locate another band and continue its transmission. Sometimes, malicious users may mimic the behaviour of PU and consequently prompt SU to give up the band. [23] proposed the use of AES-encrypted reference signal to identify legitimate PU signal. It allows key sharing between transmitter and receiver and the reference signal can be regenerated at the receiver and used to identify legitimate PU. The effect of this AES-encryption on the network is discussed in subsequent section. The key objective of spectrum sensing is to reliably detect PU signal with acceptable trade-offs. In the spectrum sensing process, CRN uses some sensing techniques to detect idle bands. The sensing techniques can be categorized into two: narrowband and wideband. The former senses and analyses one frequency at a time and has the likes of energy detection, cyclostationary detection, covariance-based detection and machine learning in its category. In wideband, the spectrum is split into sub-bands and then sensed either sequentially or simultaneously using narrowband techniques. Wideband is further classified into Nyquist wideband and sub-Nyquist or compressed wideband sensing. In Nyquist-based sensing class, analogue-to-digital converter (ADC) is used to sample the wideband signal. This case results in high power consumption and sampling. Sensing technique in this category are wavelength detection, multi-band joint detection and filter bank based sensing. The approach in compressed wideband sensing technique can be classified into two: blind and non-blind compressive wideband sensing. This is as represented in the 2.3.

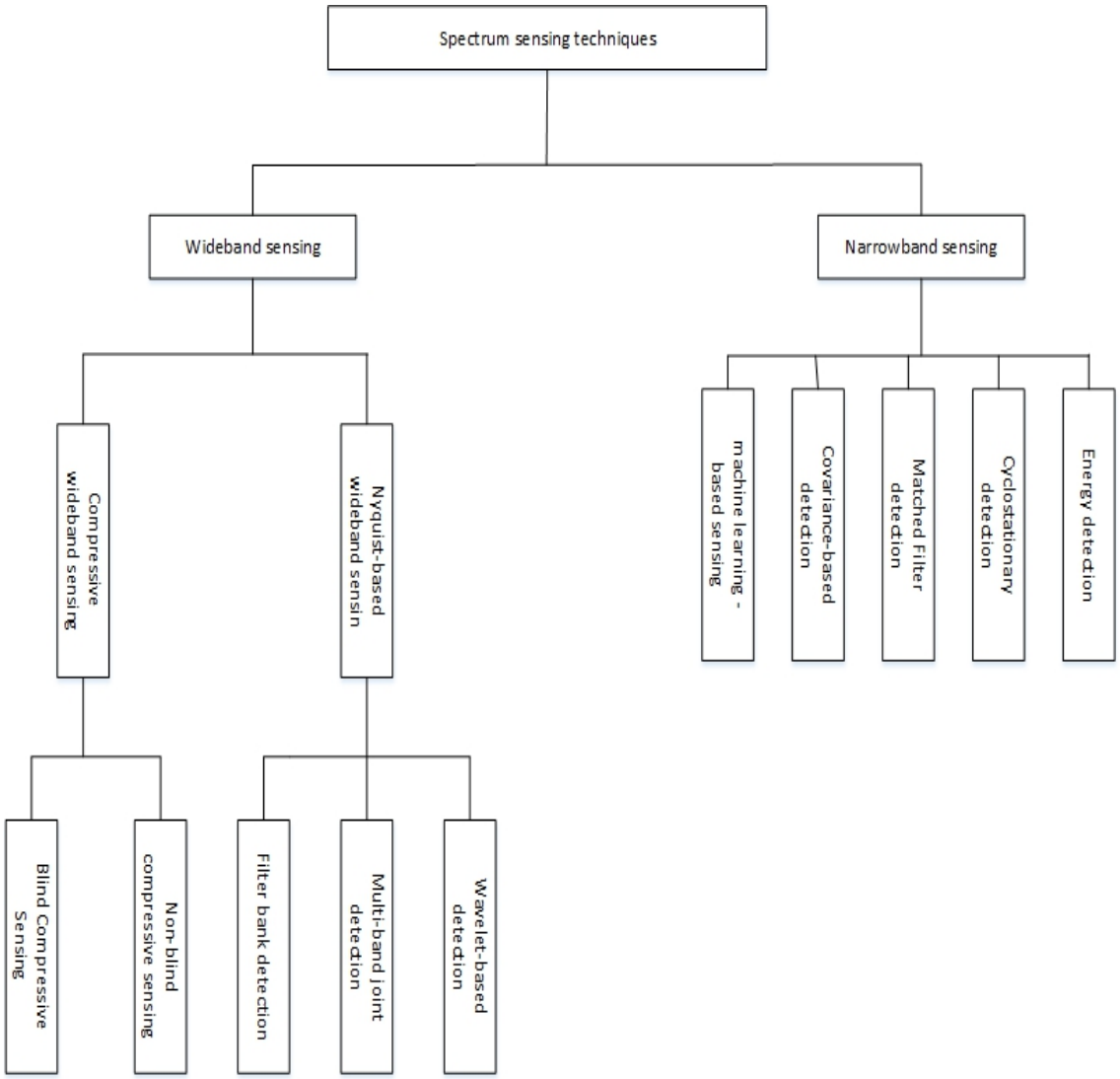

Figure 2.3: Classification of spectrum sensing techniques [24]

2.0.2 Narrowband Sensing Techniques

Narrowband is a category of sensing that analyses one frequency channel at a time over a channel of interest. This category permits SU to make decisions about the status of the band. It indicates the presence or absence of PU in the channel. The receive signal is passed through a filter and thereafter compare with a predetermined threshold. If the received signal is greater than the threshold then it is assumed there is PU and absence otherwise. Below are the sensing techniques under this category.

Energy Detection

This is the most common method for detecting PU signal in the environment [24]. The prior knowledge of the PU signal is not require [2], [24] . The technique has low cost implementation and less computational complexity which is its advantage over other sensing techniques though, it cannot distinguish between noise and signal sample. This makes spectrum space detection subject to high uncertainty. The detection process can be carried out in both time and frequency domain. To estimate the signal power in a particular frequency band in time domain, a bandpass filter is applied to the target signal. The signal is detected by comparing the output of the detector with a threshold as shown in Fig.2.4.

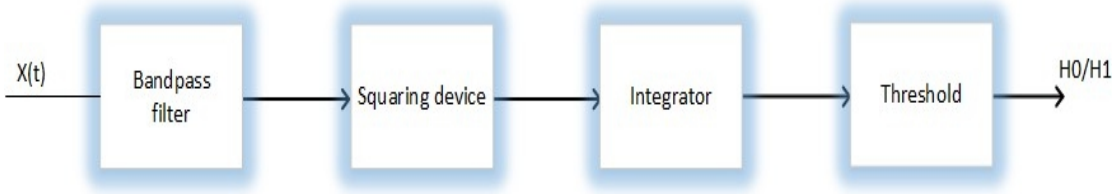

Figure 2.4: Energy detection technique [2]

where x(t) is the signal received by SU when sensing the channel. The result of the comparison is used to decide the presence or absence of PU signal [4] [11] [23]. The computation of this technique is efficient but has a very common disadvantage which is when the variance of the signal is unknown to the sensing node.

Cyclostationary Feature Detection

In wireless communication, identification of the properties of a particular radio signal for a given wireless access system can be used to detect the signal. In CRN, such method could be applied for detecting PU signal. The received signal in CR are modulated signal which exhibit built-in-periodicity within the training sequence. This is by extracting the features of the received signal and performing the detection based on the extracted feature. This implies that the knowledge of the source of the signal maybe required. This technique may perform better than energy detection if enough simple is used. The technique is able to distinguish between signal and noise sample since noise is stationary and has no correlation.

This technique is demonstrated in Fig. 2.5. In the figure, an analogue-to-digital converter is used to digitize the signal. The fast Fourier Transform is thereafter used to compute the frequency in the signal. This is performed by the use of of N-point FFT.

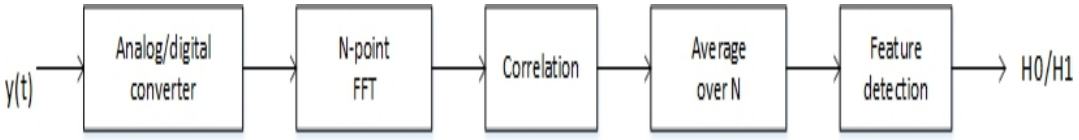

Figure 2.5: Cyclostationary feature based detection technique [2]

The value of N-point FFT block are correlated and then the mean value taken over the number of samples N. The outcome is then compared to a threshold to determine the status of the band. The complexity and the requirement for a large sample for better estimation and the precision of the features in frequency domain makes it difficult to use [3].

Matched filter Detection

This method maximizes the received signal-to-noise ratio. It requires a complete knowledge of the PU signal. The knowledge could be modulation format, data rate, carrier frequency, pulse etc. The information is pre-stored in CR memory. In the technique, the received signal samples are compared with sample signal obtained as a test sample from the same transmitter as shown in Fig. 2.6

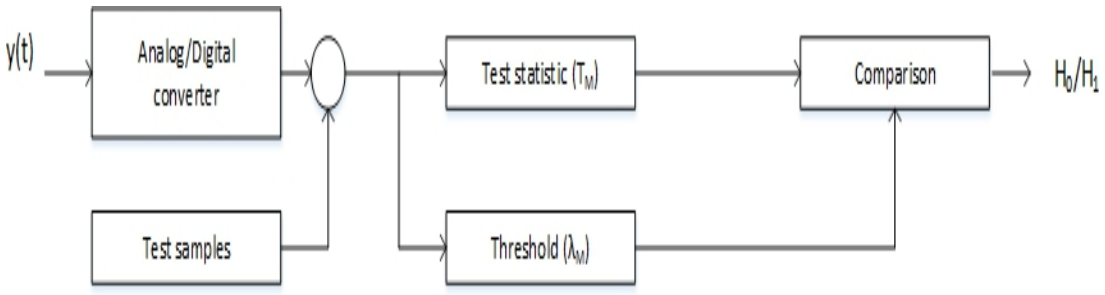

Figure 2.6: Matched filter detection technique [2]

The test statistics are computed from the sample signal and then used to compare with the threshold. In this case, if the test statistics is greater than the threshold, then the signal is assumed present and absent otherwise. The test statistics for matched-filter detection technique is expressed as:

$$T_M = \frac{1}{N} \sum_{n=1}^{N} y(n) x_p^* \quad (2.1)$$

where N is the number of samples

y represents the sample vector and x_p is the sample signal.

The test statistics T_M is compare to the threshold in order to decide the status of the band.

If λ_m denotes the threshold then

$T_M < \lambda_m$: implies absence of PU signal and

$T_M > \lambda_m$: implies presence PU signal

This technique is optimal as it does not require much sample for effective spectrum detection. The major challenge is obtaining a prior information about PU signal as it is not always readily available. This technique is not always recommended unless the complete signal information of the PU signal is known [3] [25]

Covariance Based Spectrum Sensing

In this sensing technique, multiple antennas are deployed for spectrum sensing. It uses sample covariance matrix of the signal received and singular value decomposition (SVD) to detect the status of the band. This scheme uses the correlation of the received signal from these antennas at different times for decision making. The eigenvalues of the signals received from PU are determined using the singular value decomposition method. This is after correlation and differentiation from the noise. The minimum and maximum eigenvalues are calculated and compare with a threshold to determine the status of the band as shown in Fig.2.7.

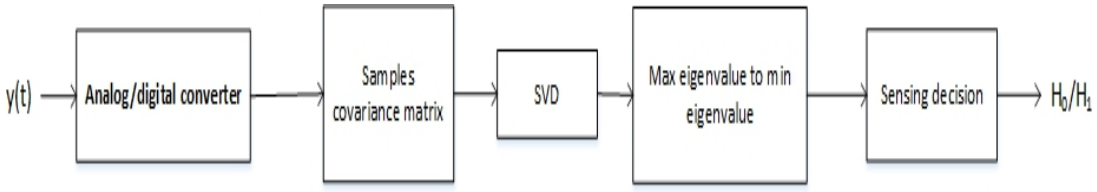

Figure 2.7: Covariance based sensing technique [2]

Machine Learning Based Spectrum Sensing

In this sensing technique, the detection of spectrum space is by conceiving the process as classification problem in which two states (free or occupied) of each frequency channel are determined by the classifier, supervised or unsupervised. Some authors proposed K-means and support vector machine as a sensing model for CR. While K-means is mainly to determine the PUs pattern of transmission and statistics, the support vector machine (SVM) is used to determine the status of the band. The knowledge of machine learning has been deployed to carry out spectrum sensing in CRN. This is mostly used in cooperative spectrum sensing. This can be classified into two steps. The first step in which unsupervised machine learning technique are used for data analysis and to determine the patterns of PU signal. In the second step, models are trained with data obtained in the first step. The first step uses K-means algorithm to identify the status of the band [2].

Spectrum Decision

Once a white space is identified, CR will decide on the appropriate band that will satisfy its quality of service requirements in terms of data rate, service time etc [25]. When an SU sends a request to access the spectrum opportunity, the spectrum server will narrow down the search space by comparing the demanded data rate with a threshold. In [26], the maximum data rate for IEEE 802.11b (operating in 2.4GHz) and IEEE 802.11g (operating in 5GHz) standards are 11Mbps and 54Mbps respectively. The third generation (3G) wireless systems offer data rate of less than 1.0 Mbps. When requesting for spectrum space for data rate greater than 1Mbps, the 3G cellular system is excluded from the search.

2.0.3 C. Spectrum Sharing

Sometimes more than one SU may be competing for a spectrum space. Their transmission is coordinated in order to avoid collision. Admission control is applied and may be based on the effective benefit offered by SU while fulfilling the quality of service requirements. This may be in terms of the SU that exert less interference to the PU signal.

2.0.4 Spectrum Mobility

This is the ability of CRN to relinquish its channel and continue its transmission on another channel on detecting the PU signal. In this case, a new band is either selected or the communication will cease. Spectrum mobility necessitate the search for a new link in order to continue communication on detecting PU signal. Spectrum sensing and spectrum mobility function together to select the next available channel when there is need for it.

2.0.5 D. Cooperative Spectrum Sensing

In cooperative spectrum sensing, more than one CR participate in sensing and report the result of the sensing to a common geological database or decision centre (DC) as shown in the Fig. 2.8.

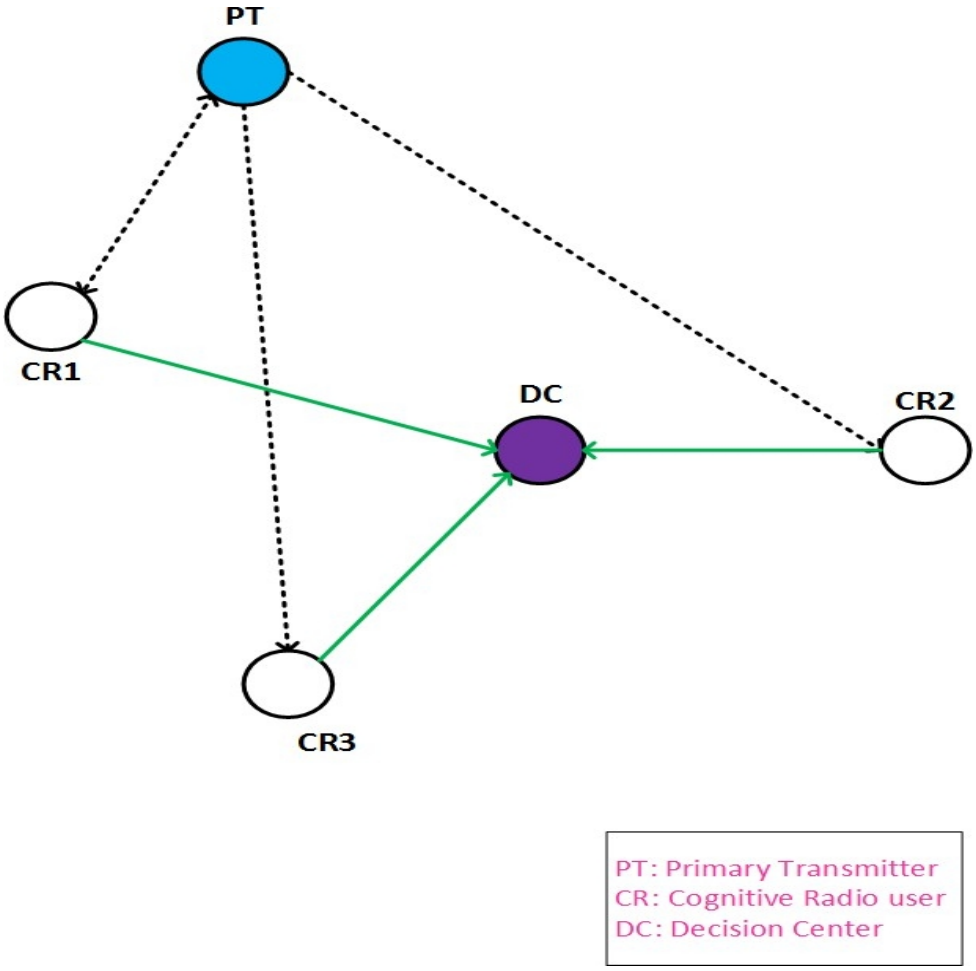

Figure 2.8: Coperative spectrum sensing model [27]

The geological database stores spectrum opportunity as central coordinate instead of multiple geological coordinates [26]. SU within same location can access the band without interfering with PU signal. To further avoid interference, cognitive radio using machine learning can estimate the idle time. The idle time is similar to Time-to-live in conventional network. The idle time decreases if unoccupied until it gets to zero which is when it is again occupied by PU. Cooperation in spectrum sensing enhances the optimization of spectrum resources because the more the number of cognitive radio involved in sensing, the more accuracy in detecting idle band. The challenges of multipath fading is also solve using cooperative spectrum sensing. Multipath fading is a fluctuation of signal experience as a result of constructive and destructive interference resulting from territorial objects such as mountains, trees, buildings etc. However, cooperative spectrum sensing has its drawback which is that all participating

cognitive radio must report the result of the sensing before a decision is taken. This enhances the protection of the incumbent but diminishes the opportunity available for SU to use the spectrum. A research in [3] proposed model to determine the number of CR in cooperation that will give minimum error probability and maximizes the throughput. The results of the experiment show that the optimal number of CRs increases as the number of CRs in cooperation increase but the maximum throughput decreases as the optimum number of CRs increases.The next subsection considered several vulnerabilities and threats in the context of CRN.

2.0.6 Threats in CRN

Security is an important issue for consideration in CRN. Several vulnerabilities of CRN can be exploited by adversaries to cause severe performance degradation [29]. For instance, attackers can introduce DoS attack that could deny SU the opportunity to use the spectrum. This is classified as malicious. This kind of attack only aim to cause hindrance for others and may not necessary be to maximize its own benefit [30]. Some attacks may particularly aim to eavesdrop or modify the content of packets on transmission. The ease at which these attacks gain access to the data on transmission depends on the encryption algorithm. These attacks cause performance degradation as it will result in SU not able to use the channel when not occupied by PU. Below are some of the attacks common to CRN.

Spectrum Sensing Data Falsification (SSDF) Attacks: This attack specialises in transmission of false sensing data to SUs. It is mostly carried out by malicious SUs. In the attack, malicious user induce CR to send false sensing data to the SUs [8] [30] [28] [29]. This form of attack induces increase in false alarm and miss spectrum detection because the decision about the status of the band depends on the sensed data. When the attack leads to false alarm, the idle space is wasted since SU will assume the band is occupied when actually idle. Conversely, in a miss spectrum detection scenario, SU will assume the band idle and forward its request resulting in regulatory violations.

Primary User Emulation Attacks (PUEA): it has been observed by researchers that one of the biggest challenges to spectrum utilization by SUs is PEUA. This attack takes to mimicking PUs signal characteristics in order to ward off prospective SUs and selfishly use

the channel. This research area has attracted a lot of research interest with many works solution such as localization and encryption being proposed to tackle it. Localization in this case is the estimation or verification of the origin of the signal. This was proposed in [26] to track malicious SUs in effort to secure radio resource allocation in in CRN.

Objective Function Attacks (OFA): This is the type of attack in which CR are prevented from receiving the signal it requires in order to adapt to change. There exist in CRN a cognitive engine consisting of several radio parameters under its control. These parameters are computed by the engine by solving one or more objective functions. This objective functions could be manipulated by adversary, forcing the radio to send false data to SU [8] which may lead to SUs delaying its transmission even though the channel is idle.

Jamming Disruption Attack: This is one of the most common form of attack to CRN. It involves creating attacks through interferences [29]. Jamming is carried out by transmitting signal to the receiving antenna on the same frequency as legitimate transmitter, thereby limiting legitimate reception by the receiving antenna [30]. This is similar to PUEA, however, PUEA emits primary like signal just to manipulate the sensors [30]. The network is liable to CRN-specific sensor-jamming attacks if an energy detection technique is used for spectrum sensing.

Eavesdropping: One of the security threats common to both wireless network and CRN is eavesdropping. Eavesdroppers maliciously seek access to the content of data over wireless links such as CRN and exploit the information against the end user.

2.0.7 Impacts of Attacks on CRN

The main impact of attacks to CRN is the denial of service and modification or eavesdropping on data on transmission. In DoS attack, adversaries may alter the sensing information transmitted by the sensing node of CRN leading to miss detection or false alarm. In this context, SU in the case of false alarm withholds its transmission on the assumption that PUs are transmitting on the spectrum. This way, SU misses the opportunities to use the band. In miss detection scenario, adversaries make radio believe that there are no PU present when actually there are PUs in the channel. This leads to regulation violations.

2.0.8 Protection of information on transmission

In order to ensure the integrity and confidentiality of information, it is important not to send data into the network without ensuring its protection against unauthorised modifications. One of the ways of ensuring the protection of data is by encryption. Encryption is one of the means through which an attack can be mitigated. It involves encoding the plain text such that unauthorised users do not gain access to it. However, encrypting the message consumes resources and degrade the network performance. Encrypting with long keys result in better security but have performance implications. It degrades the performance of the network. Similarly, encrypting with short keys improves the network performance but the network is more vulnerable to an attack. Attackers can easily compute the algorithm and use same to access the data.

2.0.9 Performance Cost of Encryption in CRN

Security application and its impact in CRN is similar to its application in traditional wireless network. In both networks, requests are encrypted and transmitted in a similar manner. For general security application, [10] proposed an encryption and freezing mechanism to deal with the security issues in a system. It quantified the effect of security in the form of throughput. Throughput increases or decreases as the encryption key length changes. In [31], different algorithms for encrypting messages were studied. The study shows that processing time depends on the used algorithm, the size of input and the length of key. The time required for each algorithm to encrypt a message was measured. Long key length as stated in [31] guarantee adequate security. However, the performance implication may be readily high due to security processing.

Encrypting with long key lengths requires high computational power and high energy consumption. In this case, [32] proposed cloud computing integration with CRN in order to allow CRN to perform the computation in the cloud and outside its own energy.

2.0.10 Cognitive Radio Network (CRN) and Cloud Computing

They have been ongoing research efforts to integrate CRN in the cloud platform. This is due to the numerous advantages that can be achieved from such integration. Cognitive radio communications have been limited by energy consumption and computational power. However, integrating CRN and cloud allows CRN to carry out its computation inside the cloud and outside its own power supply [32]. Integrating these two diverse fields helps in resource pooling. Resource pooling as a feature of cloud computing is combining the resources together and releasing them on demand. The resource pooling provides solution to channel uncertainty. Channel uncertainty is as a result of fading or shadowing of signal generated by PU. In this case, SUs could be influenced to operate on a seemly occupied channel. To overcome this, [33] proposed cognitive cloud network in conjunction with cooperative spectrum sensing algorithm to improve spectrum sensing performance. In this case the received signal from the sensing nodes are sent to the cloud. Where decisions about the status of the band are made.

2.0.11 Cloud Service Delivery

Cloud computing has been a trending topic in industry and academia due to its IT service delivery platform which can be applied in in the context of CRN for operational improvement [3]. It emanates as a result of factors ranging from change in traditional computing and communication technology to business processes. The cloud service providers can integrate the features of cloud computing and CRN to predict the real time availability of idle band for cognitive use. This certainly improves the performance of CRN. Using the concept of cloud computing, CRN can achieve elastic service in the form of on-demand resources whenever they need them. The challenges of over stretching of on-premise infrastructure gave rise to the introduction of on-demand and elastic service delivery made possible by scalability feature of cloud computing. It was developed to overcome the challenges of unpredictable service demands of users [34]. Cloud computing model evolved by observing the concept of utility computing, automatic computing and software as a service (SaaS). In [35], utility computing pools outsourced computing resources and infrastructure and deliver them as

on-demand services with usage-based payment structure. In CRN, different bands are pooled together in cooperative spectrum sensing technique and idle spectrum bands are reported to a central database located in the cloud. Due to the unpredictable nature of service demand as shown in Fig. 2.9, maintaining sufficient infrastructure to meet the unexpected high surge in service demand can be very costly.

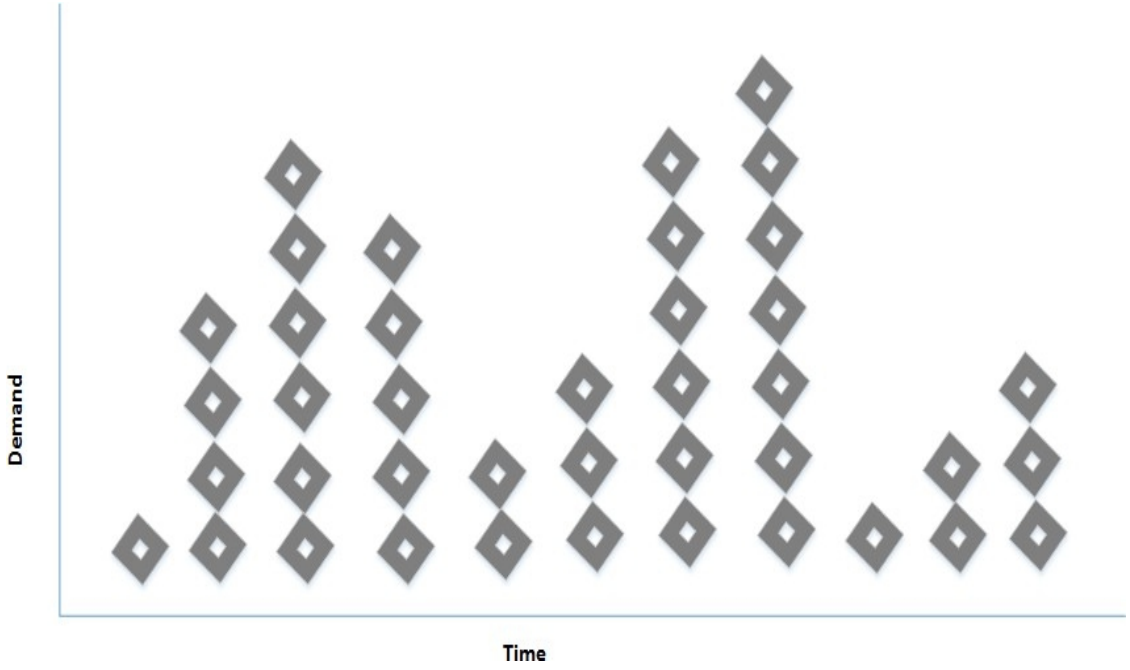

Figure 2.9: Illustration of scalability

Alternatively, under provisioning of resources always results in significant impact in terms of quality of service [36] as there may not be enough resources to cope with the peak periods. In CRN, On-premise infrastructures with one spectrum band may not have enough idle space to service all the users. It poses problem to businesses where the demand for their services may suddenly become busty. Traditional IT infrastructures have different ways of dealing with situation like this but it could be cumbersome. One of the ways adopted by traditional IT specialist is to purchase additional and more powerful infrastructure to cope with the increasing service demand. This could disrupt an ongoing process leading to significant impact in quality of service. However, cloud computing delivers better platform which is automatic provisioning of another service channel, storage and networking on-demand to cope with the increasing users demand. This is good for business development.

Scalability is one of the most important features of cloud computing and CRN that allows

resources to be scaled up or down according to the operational needs of an organization. The resources are scaled up when there is an increase in service demand and are scaled down as the demand declines. Thus, scalability is used, subject to service rates and channels operational parameters to improve system performance and avoid service degradation. The evaluation of the impact of scalability on the performance of service channel over a typical cloud platform is based on different performance measures. Research in [37] shows that scalable systems offer better performance and reduce costs. In particular, a scalable system is able to sustain a good level of performance upon sudden busty traffic flows and ensure that servers do not breakdown due to overload. The usage-based payment structure ensures that there is charge for provisioning of additional service infrastructure. Some features of cloud computing which could also be applicable in CRN are presented below.

2.0.12 Virtualization

This is a feature of cloud computing that can be applied in CRN to achieve scalability. It was introduced to overcome the challenges of physical hardware by allowing multiple pseudo-servers to run on a single physical device [39]. Virtualization is used to achieve scalability in CRN. They are many forms of virtualization: server or system virtualization, storage virtualization and network visualization [40]. In this chapter, we will be considering server visualization, the is server is able to host and run different systems on a single physical machine. In server virtualization, a control program is run on a hardware platform and cloned on other virtual machines. Each of the virtual machines operates and run its individual program as if it is on a different hardware platform. It is not only for efficiency but also saves power, space, and cooling since all the pseudo servers are still running on one machine. Research has shown that cloud applications consumes 90% less energy compare to on-premise ones.

2.0.13 Scalability and Fast provisioning

This is the ability of the server to be scaled up or down according to the demands of the organization [41]. In an organization with erratic workload, one of the following scenarios

must apply:

1. An over provisioning of servers leading to unused server capacity, as such, resulting in significantly higher cost per process than desirable.
2. Under provision of server resulting in significant impact in terms of quality of service.

None of the above is good as they both result in direct business impact; either through high costs or through decrease outputs caused by service degradation. The present day business such as Twitter and Facebook has shown high level volatility in their computing needs. The growth is much that the application of traditional approach is no longer a solution to process the volume of information required to keep up with the scaling demand. Cloud computing enables resources to be used when required and at the required scale. Though per unit charge by service providers may seem high but may be cheaper compared to owning and maintaining the resources.

2.0.14 Scalability Features of Cloud Computing

Scalability is the ability of the cloud resources to grow or shrink to cope with the organizational workload [49] without suffering degradation of the quality of service. One of the key factors of concern when considering a move to the cloud is the trust for resources availability, scalability, and cloud performance [50]. Scalability is always proportional to the cost of addition of resources. Details of scalability measures are hidden from the users. For instance, users do not have to know the location of their data or how to save or access them in the cloud. Scalability has been considered hard to achieve due to unpredictable volume of service demand from the consumers. Services with poor scalability measures will either experience service degradation due to under provision of resources or incur more cost due to over provisioning of resources.

2.0.15 Scaling Indicator

Indicators are the set performance parameters that show the status of each service channel. In order to scale the channels to cope with the service demand, it is necessary to use the scaling indicator to monitor and track the performance of the service channels [35]. Typical

scaling indicators could be:

Average number of request to the service channel per unit time.

Average queue length of the service channel

The average response time.

Once the indicator has been set, it is used to determine when additional service channel is needed or when to withdraw an already added channel. There is a tendency for the set indicator to go positive as the request per unit time increases. This is as explained in the next section. In this work we uses the queue length, as scaling indicator.

2.0.16 Scalability of Servers

This is the addition or removal of virtual servers due to increase or decrease of computing demands. This happens when there is surge or decline of consumer's service demand [51]. However, when the average service demands increases, inevitably leading to unwanted delay or possibly request lost, additional virtual server is automatically provided to avoid service degradation. For instance, if the average inter arrival time of a request to a dedicated server is 20 seconds and the average service time of the server is 10 seconds, it implies that the server will be busy only half of the time. The server is only 50% utilized, the delay and average queue length will be minimal. However, if the average inter-arrival time decreases to say, 15 seconds, with the same service rate, the server will be busy 75% of the time. The average delay and average queue length will still be minimal and tolerated. If the inter-arrival time is further decreased to 10 seconds, they maybe rise in delay and queue length as server is always busy and any new arrival may have to wait on the queue. Decreasing the inter-arrival time further will lead to unstable system. It will result to high increase in delay and queue length. When the queue length of the dedicated server gets to a certain threshold, a new server is automatically provided to avoid loss. For system to be stable $\lambda < \mu$ [52], where λ is the arrival rate and μ is the service rate. This is used to explain what happens when a company experiences a peak flow. Identification of peak periods and provision of needed conditions to deal with it is an important way of handling worst case scenario in an organization.

2.0.17 Scalable Service Structure

The scalable service systems consist of multiple server service nodes as shown in Fig. 2.10. Clients do not have to know the physical location of the service nodes providing them service. Scalable service system has management components that monitor the real-time status of the nodes and allocate jobs to them. In [19], two key components were proposed to manage the service scalability: Global Scalability Manager (GSM) and Regional Scalability Manager (RSM) [37].

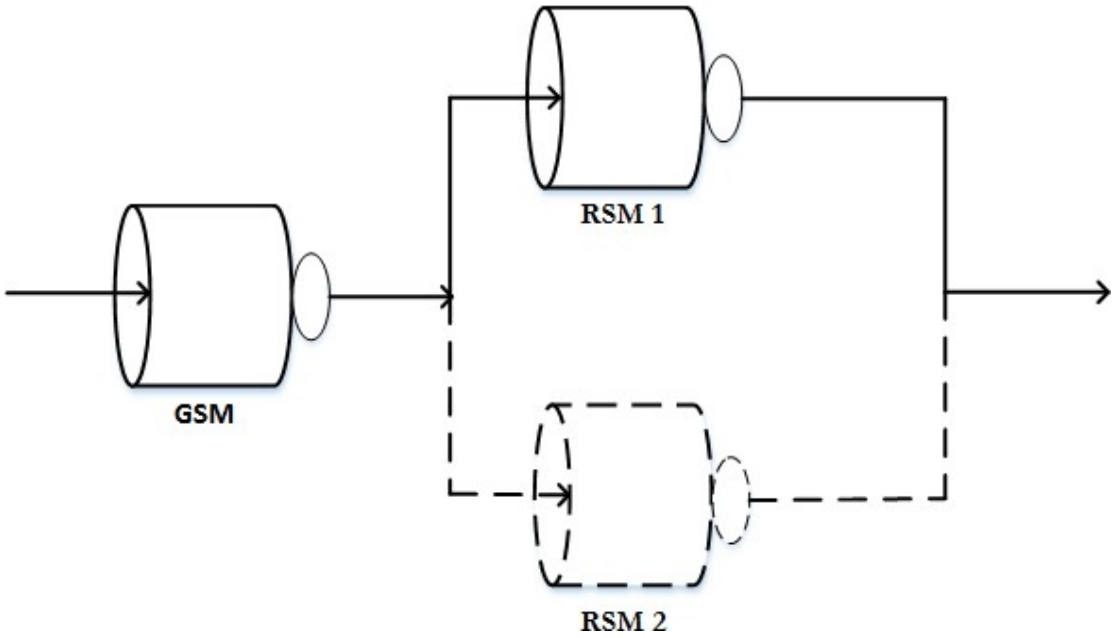

Figure 2.10: Scalability model

The GSM controls the service scalability. It balances the load [53] [54] among the channels and provides quality service delivery. However, RSM is a management component installed on each service node. It always checks the status of the service channels and allocates jobs appropriately to them. With this scalability service mechanism, our service system provides functions to add or remove new channels at runtime refer to as node management. Whenever the average request from users goes to normal, the added service channel is immediately withdrawn to avoid extra charges.

2.0.18 Service Migration

This is the transfer of users from the dedicated service channel to a new service channel [55]. It is assumed that the new service channel has already been cloned to deliver the same service as the dedicated channel but can only be made available to users when the workload is too much for dedicated service channel to handle. After the migration, the new service channel is expected to deliver the same service obtainable from the first. Service migrations only occur when there is surge in demand that results to increase in response time and queue length. The server is withdrawn immediately the service demand goes back to normal.

2.0.19 Cost of Scalability

The additional server service demand is not without a cost. Cloud service providers introduce more charges for additional service delivery. The additional service could be rendered in the form of added computing resources or storage facility. Service providers can apply any measure to meter the extra service rendered to customers. Quality, volume and cost of service should be as agreed on SLA [55] [56] [60].

2.0.20 Performance Implications of Scalability

An unexpected surge of request from users always results in service degradation. This is due to over stretching of the storage and service facility [37]. Provision of new storage and service facility which could be in the form of mobile cloud helps reduce the load on the service node. The improvement in the performance of the system as a result of the introduction of another service station is seen in the form of reduced queue length and reduced response time. The result of our analysis is as demonstrated in the subsequent session.

2.0.21 Cognitive Radio Cloud Network (CRCN)

One of the challenges in CRN is the real time storage and data processing. This is due to the limited storage and processing ability of the CR devices resulting in the need for added capabilities as demonstrated in [57]. In this context, the main function of the Cognitive

Radio Cloud Network (CRCN) is to keep up-to-date information about the availability of the spectrum space for cognitive use. This information is maintained in the cloud and updated by the sensing nodes. In [58], it was suggested that that CRCN should have databases for storing the previous information about the spectrum occupancy. CR uses the existing information about the use of spectrum to understand the environment and plan strategies to use the band without harmful interference to PU. Cognitive Radio and Internet of Things Research in recent time are moving towards IoT and CRNs. With the advent of machine-to-machine communication, IoT in conjunction with CRN will transform human activities through connectivity, resulting in internet of mobile things [59]. The new IoT paradigm will have significant impact on the everyday life in the nearest future such as assist living, improved learning, automation, industrial manufacturing, processes management, e-health facilities etc. Objects in IoT will be interconnected through both wired and wireless technology. IoT objects in this context are connections of different objects such as sensors, actuators, Radio Frequency Identification (RFID) tags, mobile phones etc. [59] highlighted how IoT can be supported by cognitive radio functionalities such as spectrum sensing. Motives behind IoT in CRN It is expected that due to the advancement of CRN in IoT that the CRN-based IoT framework may become a necessary requirement in the near future. In this case, the IoT objects will be able to think, learn, and possibly make decisions due to the ability to discern social and physical worlds. Therefore, the standardization and use of CR-based IoT objects are expected to increase in the nearest future. Because the traditional spectrum allocation do not support sharing of spectrum band, it will be impossible to introduce new smart devices since the available spectrum space may not accommodate them. In order to overcome the challenges, the future CR-based IoT devices will be equipped with sensors making it possible for them to sense, learn their environment and determine when the band is unoccupied by PU and use it. This will certainly pave way for the development of smart cities.

2.0.22 Previous works on Cloud and Scalability

Jae et al proposed a system to avoid service degradation when a service channel develop problem [37]. He used replication and service migration to explain how service of a dedicated

server is cloned and transferred to a new service channel whenever there is server failure. Prasad et al used different scalability metrics to measure the effects of scalability of a system[6] [50]. Different scalability examples were used to explain his view. System architecture and behaviour which handles traffic arriving to it at a steady state were considered. Non scalable system with single bottleneck which cannot be speeded up was explained. Trieu et al Presented scalability and performance of web application in a compute cloud. They illustrated the powerful scaling capabilities of cloud environment and also presented different scaling indicators [35]. To explore their key scaling indicators, they carried out the performance measurements on an online collaboration application which aim to maximize resource utilization of the system.

Chapter 3

Methodology

3.0.1 Research Design

This research design outlines the procedure and requirements for the implementation of solutions in this work.This as shown in Fig. 3.1.

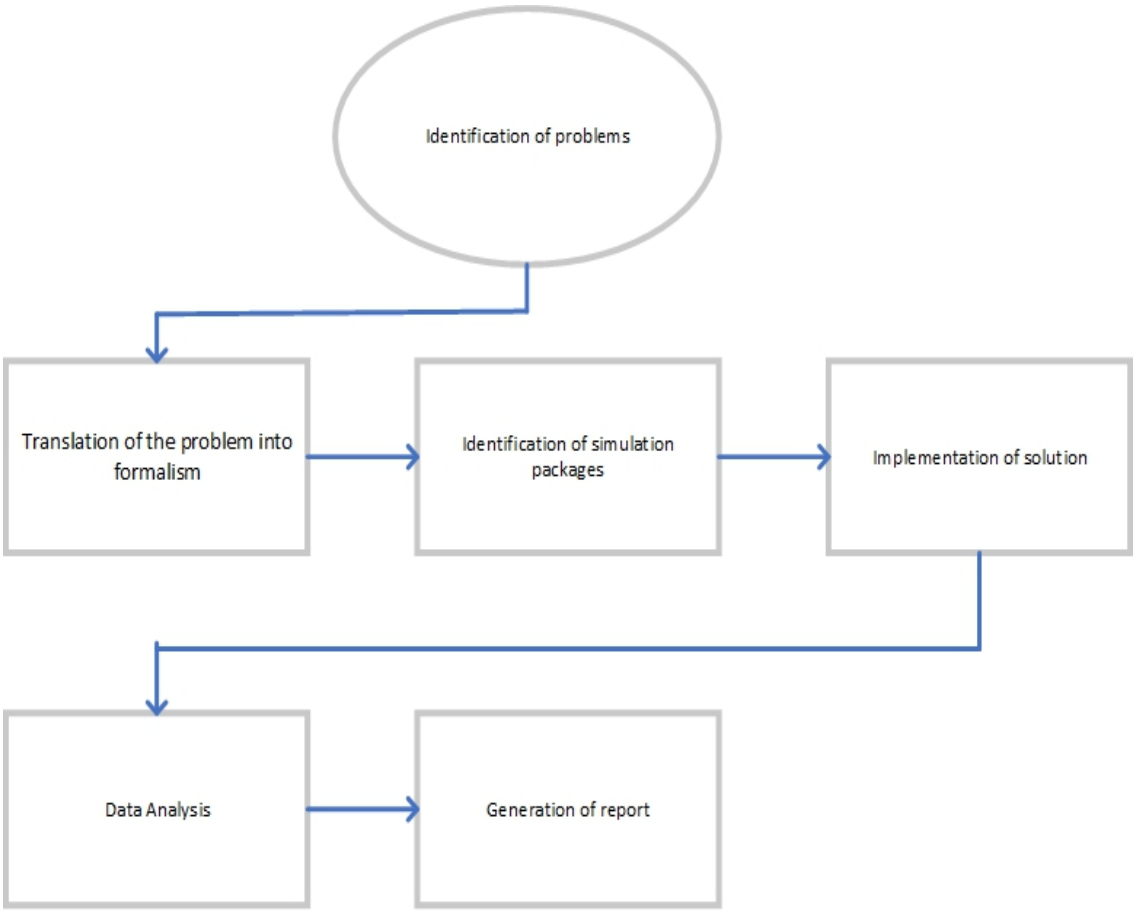

Figure 3.1: Research design

It involves the following:

Problem specification: The problem was identified through reading of contemporary literature in CRN to identify the state of the art.

Translation of the problems into formalism: The problem was translated into formalism. The formalism in this case is Stochastic Activity Network (SAN).

Identification of simulation tools: A test of different simulation was carried out to identify the most suitable tool that supports the formalism. In this case, Mobius simulation package was identified. Find in table 3.1 some of the tools that were tried.

Simulation tool	Limitations	Remark
Stochastic Petri Net Package (SPNP)	No user support	Rejected
Java Modelling Tool (JMT)	Stand-alone software which cannot be edited to support complex modelling formalism	Rejected
Telnet	Not suitable for complex solutions	Rejected
Mobius Petri Net Package	Suitable for complex solutions, user support available and can be reprogrammed to support different modelling formalism.	Accepted

Table 3.1: Identification of tool

Implementations of solution: The simulation was implemented using the identified Mobius Petri Net tool

Analysis of data: The data was analysed and the results presented

Generation of report: The report was generated using latex text editor

3.0.2 Network modelling Tools

To achieve the desired aims and objectives, specific network modelling tool as mentioned above would be required. This tool is used to generate the required traffic to mimic the behaviour of a real system. Good understanding of the modelling process is essential in order to fully harness the strength of the tool. This include the ability to translate the model into a formalism with knowledge of the real system. Examples of modelling formalism are petri nets, SPN (stochastic petri net) and GSPN (generalized stochastic petri net). SAN

(stochastic activity network) is a generalisation of SPNs [61] which has some similarities with GSPNs. SANs as a formalism supports mobius tool.

Petri Nets

Petri net is a formalism that is developed and used to abstract complex methods for analysing and interpreting the flow of information [61]. The formalism has been proposed for analysing systems with concurrency and conflicts. It possesses a number of properties. Through these properties, system designers are able to identify if the specific functional properties of a system under design have been met. These properties can be grouped into behavioural and structural properties. While behavioural properties depends on the initial marking of the petri net, the structural properties is associated to the topology or net structure of the petri net. Petri nets are graphically represented by a directed bipartite graph with circles as places and bars or boxes as transitions. The arcs associated to this model can be classified as input, output and inhibitor arcs. The input arcs are arrow-headed arcs from places to transitions. An output arcs are arcs from transitions to places while inhibitor arcs are circle-headed arcs from places to transitions.

Places: these are used to represent queue or buffer for incoming request when the server is busy [62] [63]. It is graphically symbolised as circle as shown below. Places contain tokens and are represented with dots which are referred to as requests in our model. It can contain finite or infinite number of requests (tokens). Firing of transition removes a token from the input place and deposit in the output place which changes the state of the system. Places contains tokens which are drawn as dot inside the places. Fig. 3.2

is the circle and bars representing places in simulations. Places can be a buffer or queue for installing incoming jobs when the server is busy.

Transitions: These represents actions that changes the state of the system. The actions abstracts various characteristics that is obtainable in many formalism. The state change behaviour of atomic model formalism is a result of the functionality provided by the transitions. The dynamic change in behaviour of a model is determined by the number of tokens and its distribution. Changing the distribution of tokens in places demonstrates the occurrence of

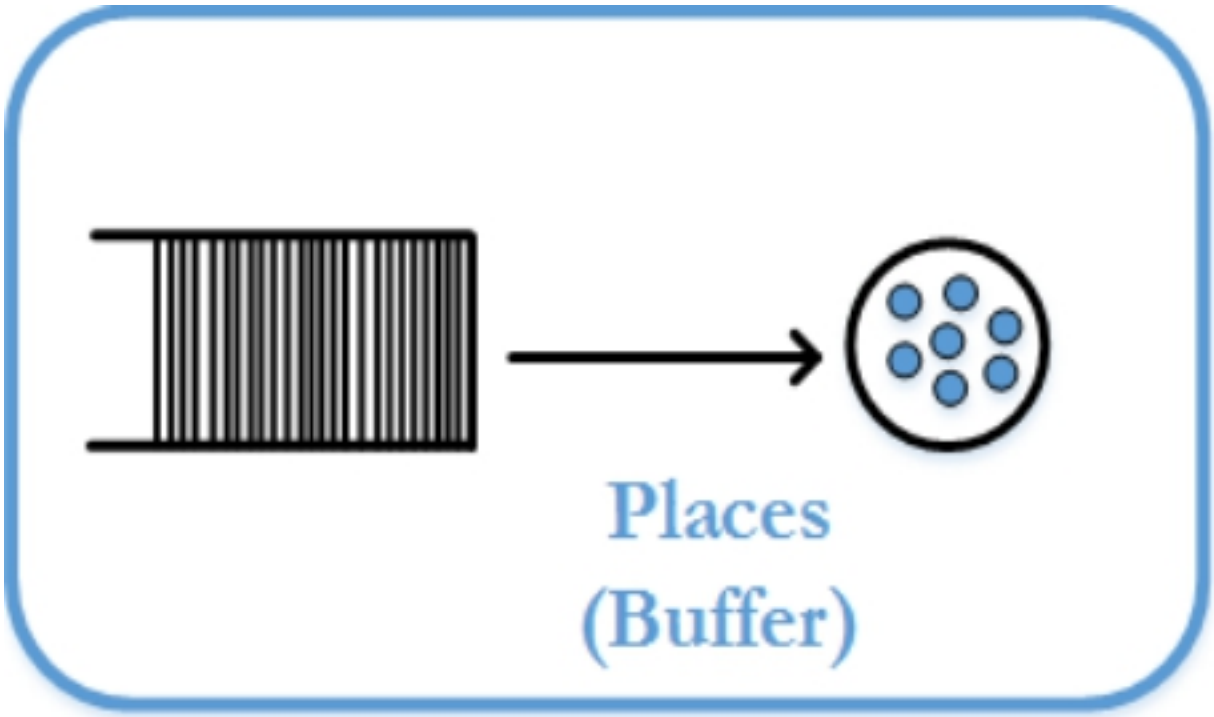

Figure 3.2: Place and Tokens in Petri Net Model

events or execution of operations. Transitions are graphically represented as a vertical bar as shown in 3.3.

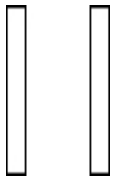

Figure 3.3: Transitions

A transition is enabled if the input place contain a number of token greater than or equal to the given threshold defined by the multiplicity of the arc. A transition without an input place is referred to as source transition whereas one without output place is called a sink transition. A transition without an input place is always enabled. For in instance transition t1 in Fig. 3.4 is always enabled. Note that only enabled transitions can fire.

In the model in view, it is used to generate arrival and service time required in the network.

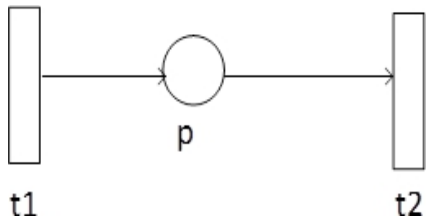

Figure 3.4: Places and Transitions

Firing depends on the exponential delay associated to the transition. Firing of a transition deposits a token in the output place. They are two types of transitions: immediate and time transitions. Immediate transition as the name implies is used to represent activities that fires once the enabling condition are fulfilled. In time transition, exponential delay is associated to its firing. When the transition is enabled, it will wait until the time associated to its transition elapse before firing [61].

Tokens: Tokens are used to represent requests going into the network. It is represented with dots inside places. In our model, tokens are generated by both PU and SU as requests to be transmitted.

Arcs: These are used to connect an input place to transition and from transition to output place [63]. The enabling rule involves only input arc while the firing depends on the input and output arcs. As shown in figure below, an arc directed from a place pj to a transition Tj indicates that pj is the input place of Ti and is denoted by I(Ti, pj)=1. Also, the arc from Ti to pj defines the pj as the input place of Ti and is represented as O(Ti,pj)=1. The initial marking of the petri net in the figure is M0 = (2 0 0 0). In this marking, only the T1 is enabled and firing of the T1 will result in change in marking. Fig.3.5.

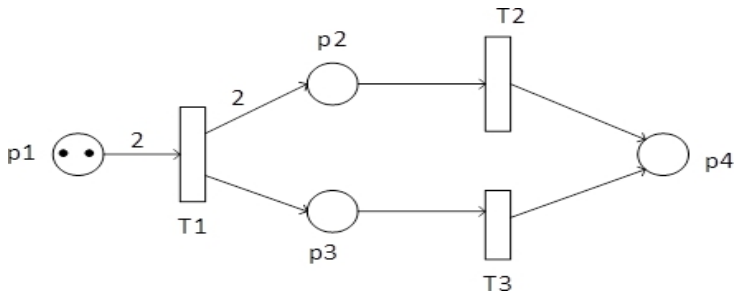

Figure 3.5: Enabling and firing of transitions

Inhibitor arc: This is used to enable firing of a transition when a place contain a token less than the multiplicity required to enable the transition. It is represented by circle-headed arcs and can be used to model priority and system freezing as would be demonstrated in our model.

Stochastic Petri Nets (SPN)

This is used to represent a petri net with exponential firing delay. This firing delays are associated to random variables that results in probabilistic models. In this case, each transition ti has a firing delay with probability firing density function with negative exponential pdf. It is assumed that each transition has a timer. The value of the timer is is sampled from the negative exponential associated to each transition. When a transition is enabled, the timer is decremented and the transition fires when the transition records zero. It is then obvious that the timed transition can be used to model the execution of activities in a distributed environment.

Generalised Stochastic Petri Nets (GSPN)

This is introduced as an extension to SPNs. It is aimed at improving the modelling power of SPNs. The extension includes an immediate transition that fires as soon as being enabled. It is used to convey the notion of independency on time specification. The immediate transition fires first when simultaneously enabled with timed transition. This therefore suggests that some events completion does not correspond to time consuming activities.

Stochastic Activity Networks(SAN)

SAN is one of the formalism supported by Mobius. It is a generalisation of the basic SPN formalism. High level modelling formalism can be enabled using graphical primitives in SAN. The four primitives objects of SAN are places, activities, input gates and output gates [62]. Places are represented graphically by circles and denotes the state of the modelled system. Activities are used to define the actions that changes the state of the system while the input

gate controls the enabling of the activities. The input gate is symbolised graphically by a triangle with the flat side connected to a transition. The output gate defines the changes in marking that occur on completion of activities and it is represented graphically by a triangle connected from the transition to the flat side. A place can be connected directly to a transition. This is equivalent to a connection with an input gate with a predicate that enables the activity.

3.0.3 Analysis of Petri Nets

Modelling alone is of little importance without corresponding analysis of the modelled system. The analysis of the system is expected to lead to important insight into the system behaviour. The three main approaches in the analysis of petri net models are simulation, matrix-equation and reachability analysis. However, in consideration to the network understudy, simulation is considered for further explanation.

3.0.4 Simulation

Though this simulation is inexpensive and time consuming, however, undesirable properties of the model can be revealed through the simulation technique. Despite that it is convenient and straightforward approach used by Engineers in validating the properties of the designed model, however, it may not prove the correctness of the model in general case. Simulation has been used when other techniques could not provide the needed result. More formal languages (formalism) were developed due to the advancement in techniques for solving models. In this case, each formalism presents its advantages. For instance, some formalism have very efficient solution methods. Stochastic activity networks formalism were developed for complex model behaviours. Tools have been developed along this formalism. A tool is introduced around one or more solution techniques. Simulation is one of the solutions that could be used to evaluate the system behaviour. Some of the tools listed by [62] are GreatSPN which is based on GSPNs, UltraSAN resulting from SANs, SPNP from stochastic reward network. Though these tools are useful in the context of what they were developed for, however, there are some limitations. The limitations in this case is that all aspect of the

intended model must be in a single formalism. In this context, it is challenging to solve a system model facets requiring multiple modelling techniques. Mobius has advantage in this case as it has built integrated multiple formalism which each model can be solved. With Mobius, several components can be designed and connected together in order to maximize the potential interaction. Having a modelling tool that can simulate multiple formalism allows innovative combination of modelling techniques.

3.0.5 Overview of Mobius Simulation Package

Mobius tool is a modelling tool that supports multiple formalism. The compatibility of a formalism with Mobius depends on the ability of the developer to represent the formalism in an equivalent model that uses Mobius components. The merits of specific formalism are peculiar to the model in which it is constructed. This is because models are constructed in specific formalisms.

3.0.6 Background Components

In order to define the framework of a model, it is required to ascertain and abstract the idea present in a formalism. It is also essential to take broad view of the process of constructing and classifying the models. The process of model construction has been divided into steps with each step being associated to a new model type. In consideration to the steps, the first step in the construction process is model generation using formalism. The basic model in the framework is known as atomic model which comprises of state variables and actions. Example of state variables are places which holds state information about model and the actions that changes the state of the system. The next step is to compose the model if it is part of a larger model. The advantage of the composed model is to make it modular and easier to construct leading to efficiencies in the solution process. The next step is to determine some required metrics using some reward functions. This matrices are used to predict sensing, security and performance tradeoff value for CRN. This can be captured in Mobius by executing it as a separate model type called reward models. This is followed by a solver which is applied in order to compute a solution to reward model. Any method that

computes a solution to reward variable is refer to as a solver. The solution computed to a reward variable is called result.

3.0.7 Mobius Package Description

Formalisms are translated into model framework components. This is done using abstract functional interface (AFI). The AFI presents an interface linking formalisms and solvers which allow interactions between formalism-to-formalism and formalism-to-solver. The components of model formalism are implemented as classes resulting from AFI classes before it can be applied in the mobius tool. In mobius, models can be solved numerically or by simulations. C++ code is generated from each model, the implemented together with mobius basic libraries to obtain the executables for the solver. This executable then generate the results after run. The mobius modelling architecture is as presented in Fig. 3.6 .

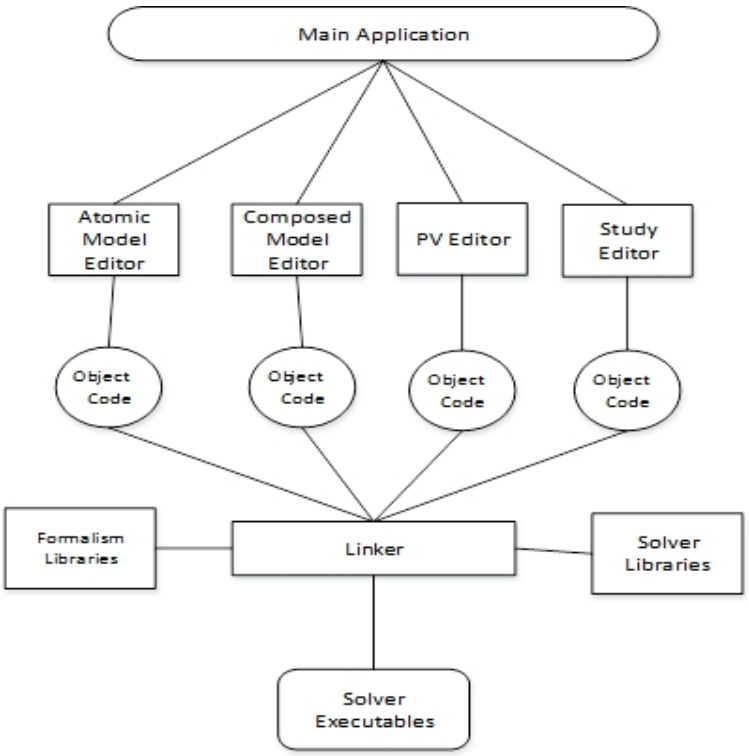

Figure 3.6: Mobius modelling architecture

It is certain that most modelling techniques can be supported within the context of mobius tool. The number of interactions between different process can be maximized by making modelling processes modular. In this case, reward formalism, composed and connection

formalism may be added freely.

Atomic Formalism

Models consist of one or more atomic models. Atomic models can be created or edited using editors such as SAN editor (Atomic model editor), the PEPA editor, Bucket and Balls editor and Fault Tree editor. As earlier stated, multiple formalism including SANs are supported by mobius tool. SANs uses graphic primitives to introduce high level modelling formalism with the aim to achieve detailed performance and dependability. The primitives in this case are places, activities, input gates, and output gates.

Atomic Model Editor

This considers the atomic formalism with emphasis on creation, editing and manipulation of atomic models using mobius SAN editor. In SAN editor, the designer is allowed to undo recent operations on the model with the aid of the undo name. Example of operation that can be undone is the change of graphical location, renaming of components, text editing, and lines.

3.0.8 Composed Model

This as the name suggest consists of sub models which can be presented as a single model with own state space. The sub models preserves their formalism-specific characteristics in such that individual structured properties of the sub models are not destroyed. Building a composed model is necessary technique required to improve the efficiency in the solution process.

Reward Model

This is used to provide specifications for performance measures. Performance variable (PV) is the reward model that is implementable in Mobius. The PV based its measurement on the state of the model with respect to the rate reward or action completions in consideration

to the impulse reward. A rate reward in this context is used to describe the function of the state of the system at a time instant. The impulse reward takes into account the identity of the action that completes and also determines the state of the system. This measurement can be carried at an instant of time, at a steady state or be time-averaged over a time period.

3.0.9 Sensing, Security and Performance Metrics

Matrices are used to evaluate the sensing, security and performance viability of the network under study. In the context of CRN, in order to evaluate the performance of a real system, it is imperative to consider the following matrices. Throughput This is a metric that measures the volume of completed jobs per unit time. Throughput can be affected by factors such as security incident, arrival rate, data encryption key length and transmission rate [10]. The throughput of a network without security is expected to be greater than that with security protection. The arrival rate of requests have performance impact on the network. Though the transmission rate may be high, however, if the arrival rate decreases, the throughput will also decrease. Similarly, if the encryption key length is long, the network, though is secured but will have decrease throughput.

Probability of System in a Secured State

This is used to determine the chances that the network is in a secured state. The major factor affecting this probability is the encryption key length [10]. Encrypting with long key leads to a well secure network, therefore high probability of network being secured. Conversely, encrypting with short keys results in a frequent security incident and therefore decrease in probability of network in a secured state.

Probability of Spectrum Detection

This is probability of detecting when the band is free and could be used by SUs. This probability decreases with increase in PU arrival rate. It also decrease with increase in probability of false alarm. This is because CRN could detect the band occupied when actually

free.

Probability of Loss

In packet loss, jobs arriving when the server is busy and the queue is filled are dropped. The packet loss probability (PLP) depends on the capacity of the queue. It also depends on the correlation between arrival rate and service rate. For instance, if the service rate is less than the arrival rate then the packet loss probability will be high. However, if the service rate is greater than the arrival rate the probability of loss will be less.

Probability of False Alarm

This is the probability that the band is detected occupied by CRN when it is actually free. This probability of detection increases with increase sensing frequency. It also decreases with increase in false alarm. This is because CRN could detect the band as occupied when actually free, leading to unused spectrum space.

Chapter 4

Combined Sensing, Performance and Security Trade-offs in Cognitive Radio Networks

4.1 Introduction

The introduction of CRN becomes necessary due to proliferation of smart communication devices which add more pressure to the available spectrum resources. Research in [3] [11] revealed that some spectrum resources licensed to PU are not always utilized in a number of locations. To this end, regulatory bodies such as Ofcom and FCC approved the use of CRNs in the spectrum while it is idle. This implies that SUs are required to sense and detect when the spectrum band is not occupied.

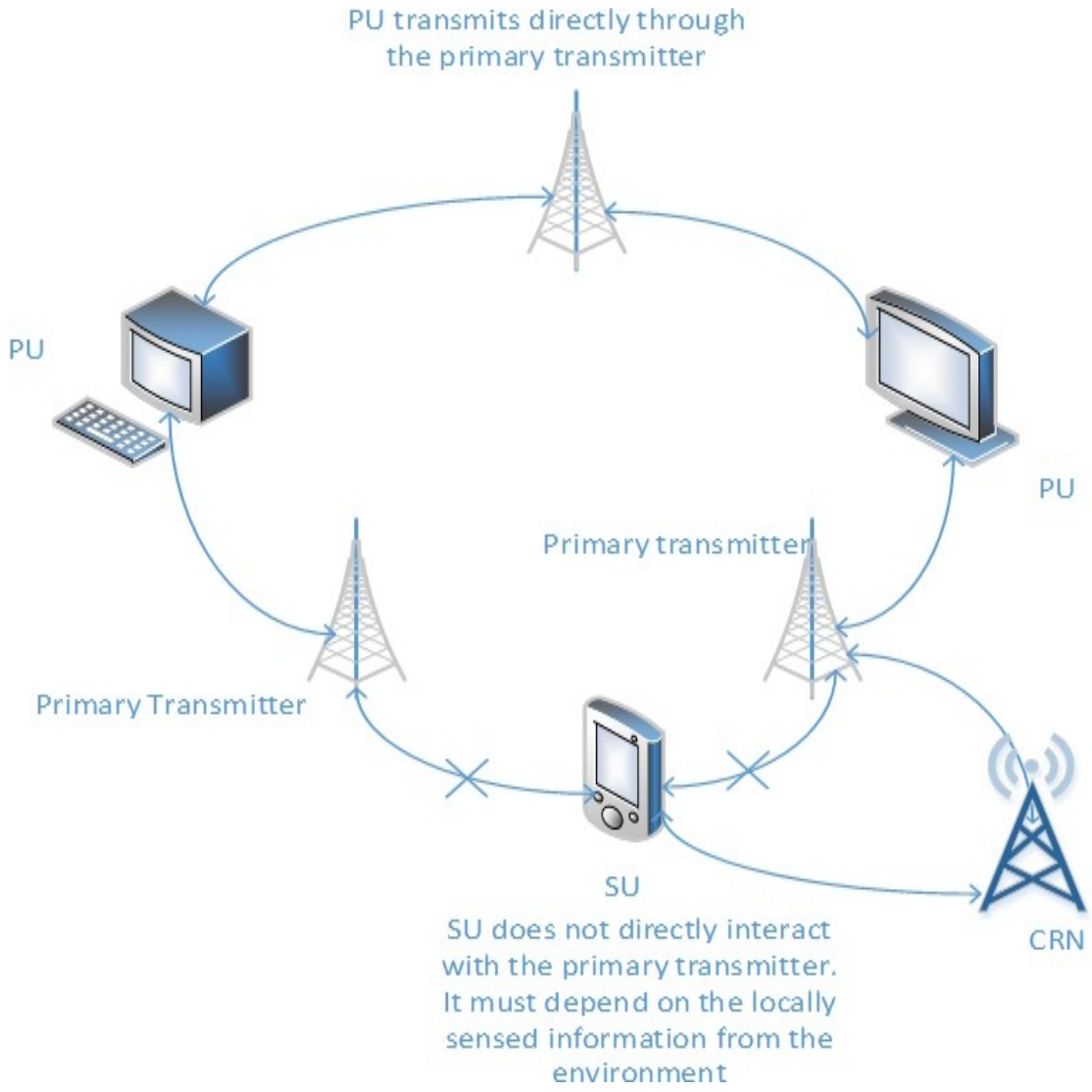

Figure 4.1: Spectrum sensing (c.f., [[15]])

SUs must search for idle spectrum space through CRN by sensing as demonstrated in Fig. 4.1 [15].

Sensing is carried out periodically and only when there is request to transmit. During sensing, if an idle band is detected, the request is first encrypted and then transmitted. If the spectrum is occupied, it senses again after an interval of time. To ensure efficient protection of PUs, [26] considered the estimation of the idle time of the band. This is similar to Time-to-Live(TTL) in conventional network. It starts decreasing as soon as the band becomes idle and set to zero if again occupied by PU. When the idle time is set to zero, SUs

are not allowed to use the band to avoid interfering with PU.

Due to its wireless nature, CRNs are very vulnerable to malicious attacks from eavesdroppers. In order to enhance the security, studies such as those in [64] [65] proposed an encryption algorithm in conjunction with other security measures to shield the transmitted request from potential attacks. These multiple security measures introduce additional delays and further performance degradation. Unfortunately, the existing CRN has no means of quantifying the performance degradation caused by such security mechanisms as studied in [10] and therefore did not consider the associated trade-offs. It also has no means of detecting when the encryption key has been compromised thus, the encryption continues with the same key. A novel Stochastic Activity Network (SAN) model of a node of a CRN with focus on sensing, encryption and intrusion detection mechanism is proposed. The sensing detects idle spectrum space, encryption process is used to encrypt an incoming request prior to its transmission while intrusion detection is a blocking mechanism that will eventually cease the network operation on detecting malicious behaviour. This freezing operation is necessary to prevent the system from encrypting with a compromised key. The SAN is evaluated in terms of sensing, security and performance. Specifically, for spectrum sensing of SUs, the metric of interest is the probability of spectrum detection. For security, the probability of CRN being in secure state is taken into account whilst the SU throughput is adopted as the performance metric. To this end, an additive combined metric is proposed to determine 'optimal' sensing, performance and security trade-offs.

4.2 Review of Related Works

Many studies have been proposed to improve the efficiency of CRN with respect to security, sensing and performance. In particular, an investigation was carried out in [64] on the security efficiency of AES and frequency modulation method of data protection in chaotic cognitive radio (CCR) system. The analysis of the simulation results show that it offers a high system security. A study was undertaken in [11] relating to sensing-throughput trade-off for cognitive radio networks. The focus was to determine the sensing duration to maximize the achievable throughput with sufficient protection of PUs. The analysis of the simulation

results shows that there exist an optimal sensing time which yields the highest throughput. An investigation was carried out in [22] to determine the number of sensing nodes required to cooperate in order to improve the accuracy of spectrum detection. The optimal number of cooperating radios needed to minimize detection error probability and maximize throughput in CRN for Wi-Fi networks were derived. Each of the research above independently studied either security or sensing and performance in CRN. None of these studies considered the combined metric of sensing, security and performance with the aim to quantify the effect of encryption and security control and consequently predict a trade-off that offers no extremes but optimum with respect to sensing, security and performance.

4.3 Sensing- A Review

Sensing is performed by CRN to detect the presence or absence of PU signal in order to avoid SUs interfering with it [66]. It is carried out at intervals of time. If X_n is the signal received by SU during sensing, then the signal can be divide into N segments. Binary hypothesis testing is applied as in [6] - [19] in order to determine the signal energy in each of the segments in N, where T(X), the energy available to SU, which is used to decide the presence or absence of PU at time t, is given by

$$T(X) = \frac{1}{N} \sum_{t=1}^{n} |X_n|^2 \tag{4.1}$$

where X_n are sets of signal segments $x_1, x_2, \ldots, x_n$ i.e., $X_n = [x_1, x_2, \cdots, x_n]$. To decide the presence or absence of PU signal in the band, the received signal energy is compared with a predetermined threshold [11]. This threshold varies according to the noise variance in energy detection σ_w^2 and can be determined by equation (4.2)[11] [6]

$$(! = \sigma_w^2 + \frac{Q^{-}1(P_f\, a).\sigma^2}{\sqrt{N}}{}_w \tag{4.2}$$

where Q is the complementary cumulative distribution function of the standard Gaussian variable. Let H_0 represent noise only and H_1 denote noise and signal. If the signal energy

T(X) available to SU is greater than the threshold *(!* then PU is assumed to be active on the band, otherwise, the band is unoccupied and can be used by SU [17]. Let σ_s^2 be the transmitted signal power by PU and σ_w^2 the noise power, then we can define the signal-to-noise ratio (SNR) Y as $\sigma^2/_s\sigma^2$ $_w$From central limit theorem, considering T(X) under hypothesis H_0, T(X) can be approximated as a real Gaussian variable with mean σ^2_w and variance σ_w^4/N. T(X) under hypothesis H_1 can be approximated as a real Gaussian variable with mean $(1+Y)\sigma^2_w$ and variance $(1+2Y)\ \sigma^2\ /_wN$. From the analysis presented in [67] and [6], it follows that

$$T(X) = \begin{cases} \sigma_w^2,\ \sigma_w^4/N & H_0 \\ (1+Y)\sigma^2_w,\ (1+2Y)\ \sigma^2_w/N & H_1 \end{cases}$$

If we assume $f_{H\,0}(x)$ as given in equation (4.3) to be density function of T(X) when H_0 is true i.e.

$$fH_0(x) = \frac{1}{\sqrt{2\pi\sigma^2_w}} exp - \left[\frac{1}{2}\frac{x - \sigma^2_w}{\frac{\sigma^4_w}{N}}\right] \tag{4.3}$$

and $f_{H\,1}(x)$ as shown in equation (4.4) to be density function of T(X) when H_1 is true

$$\frac{1}{\sqrt{2\pi\sigma^2_w}} \left[\frac{1}{2}\frac{x - (1+Y)\sigma^2_w}{\frac{(1+2Y)\sigma^2_w}{N}}\right]^2 \tag{4.4}$$

then we can decide the presence or absence of PU signal by comparing the T(X) with the threshold as given in equation (4.2).

4.4 Spectrum Detection and False Alarm- A Review

Spectrum detection relates to the correct detection of the status of the spectrum band. From SU perspective, high probability of detection provides more chances for SU to utilize the spectrum band leading to rise in throughput. As stated earlier, if T(X) is greater than the threshold *(!* and there is PU active on the spectrum then there is correct detection of the status of the spectrum band. This is as given in equation (3.5) [11]

$$prob(T(x) > (!|H_1 true) = \int_{(!}^{\infty} fH_1(L(x))dL \tag{4.5}$$

where L(x) is the probability density function (PDF) of the test statistics T(X). The equation (4.5) is the probability that the received signal is greater than the threshold given that PU is active on the band. The probability of spectrum detection in the simulation is the number of successful spectrum space detection to the number of sensing attempts. Conversely, false alarm is falsely detecting the spectrum band to be occupied when actually it is idle [3]. It is mostly attributed to multipath fading, which is the attenuation affecting a signal as it travels through the space (c.f., [68]).In contrast to spectrum detection, if T(x) is greater than the threshold *(!* but there is no PU active on the spectrum then there is incorrect detection of PU status (false alarm) on the spectrum. This is as given in equation (4.6)

$$prob(T(x) > (!\, H_0 true) = \int_{(2}^{\infty} f_{H_0}(L(x))dL \qquad (4.6)$$

where L(x) is the PDF of the test statistics T(X). This is the probability that the received signal T(X) is greater than the threshold given that the PU is not active on the band.

4.5 Proposed Model

In this section, the proposed SAN model of a node of a cognitive is presented. It is an open network that consist of security control and performance model with sensing, encryption and transmission nodes. The security control is connected to performance model through inhibitor arc as shown in Fig. 4.2. The vertical bars represent the transition that generate the actions that changes the state of the system. For clarity, the set of places which represent buffers in the performance model are replaced with queues to differentiate it from set of places in the security model which are not buffers. Tokens are the requests (PUs and SUs) being transmitted through the network. The arcs connect input place to transition and from transition to output place. There is also an inhibitor arc that can inhibit the actions of transitions as appropriate.

The security control model serves to cease the operation of the network when an attack is detected. A token in the place 'secure' indicates undetected attack on the the network. This token moves round the model according to the rate of security incidents. Firing of transition

'Sec Inc' denote a system under attack but not detected. The attack is detected when the transition 'detect' fires, depositing the token in the place 'restore' implying that the system is being restored from security incident. The cycling of the token in the security control unit of the model affects the throughput of SU.

It is assumed that PUs have unrestricted access to the spectrum. It is also assumed that the arrival process is poisson while the corresponding encryption and transmission times are exponential. When an SU detects an idle band, it sends its request to encryption node. The encrypted data is then sent to the next node for onward transmission.This is as illustrated in the proposed SAN model of Fig. 4.2.

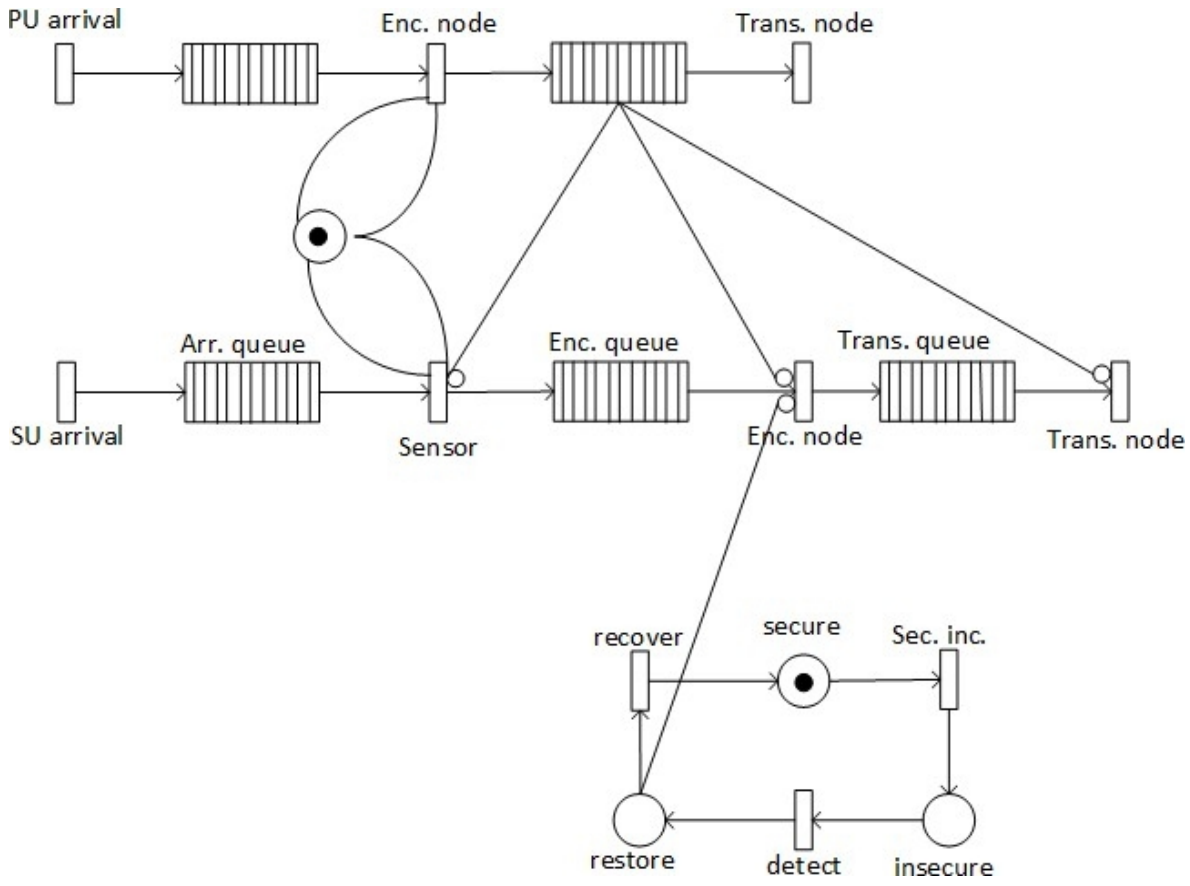

Figure 4.2: Proposed CRN model

PU and SU requests are generated by PU and SU transitions respectively. SU arrival activates the sensor indicating search for available spectrum space. If no PU is detected, then the band is assumed to be unoccupied, the SU request is forwarded to encryption node.

Conversely, if there exist at least one PU request in the transmission node then the spectrum is assumed to be occupied by PU and SU is expected not to interfere with its transmission.

4.6 Analysis and Simulation

In the analysis, there are two possible scenarios: the spectrum band is idle and correctly detected to be idle and the throughput is denoted by Th_0 and when the band is falsely detected to be busy and actually it is idle and the throughput is Th_1. In the proposed model, sensing is carried out simultaneously with encryption and transmission. To this end, as reported in [11] [19], the average throughput of a CRN is determined by

$$g = g_0 + g_1 \tag{4.7}$$

where g_0 is

$$g_0 = P(H_0)(1 - P_f a(\tau))Th_0 + P(H_0)(1 - P_f a(\varepsilon))Th_0 \tag{4.8}$$

and g_1 is

$$g_1 = P(H_1)(1 - P_d(\tau))Th_1 + P(H_1)(1 - P_d(\varepsilon))Th_1 \tag{4.9}$$

τ is the sensing time, ε is encryption time, $P_f\ a$ is probability of false alarm and P_d is probability of spectrum detection. $P_f\ a$ and P_d are determined as given in equations (4.5) and (4.6).

Equation (4.8) shows the sum of the throughput for the probability that the band is idle and detected to be idle while sensing and the throughput for the probability that the band is idle and detected to be idle within the encryption time. Similarly, equation (4.9) shows the throughput for the probability that the band is occupied and detected to be occupied within the sensing time and the throughput that the band is occupied and detected to be occupied within the encryption time. The addition of the two gives the average throughput as stated in equation (4.7). However, when the time between sensing is small, there is a higher detection of idle band though PUs are less protected from interference from SU. This may lead to rise in SU throughput. But high sensing time may reduce encryption time

and invariably leads to less secured system and more frequent security incident and drop in throughput.

In the experiment, rate of service request for PUs and SUs is 0.5. The sensing time is varied from 0.1ms to 3.4ms and the encryption time from 3.4ms to 0.1ms. This implies that each participating secondary user is assigned a frame size of 3.4. The frame is divided into 3 parts as shown in Fig. 4.3.

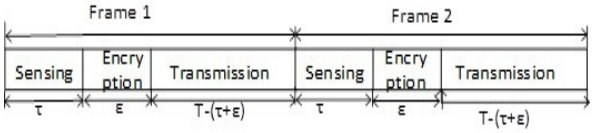

Figure 4.3: A typical frame for CRN

the first part is sensing, the second part is for data encryption and the last part is for data transmission. Each part is divided into slots [19]. The higher the number of slots in each part the more the number of activities in that part is carried out. The time to security incident at its very secure state is 15100ms and decreases in steps of 1000ms until it gets to 1100ms, then it decreases further in steps of 100ms until to 100ms and further decreases to (time–time/2)s in each progression until it gets to 12.5ms. In the analysis, when the sensing time is short, the remaining frame time after sensing is used for encryption. The strength of the security of the system is determined by the length of encryption key which also determines the encryption time [10]. The longer it takes to encrypt, the more secure the system become. This implies that short sensing time leads to a secured and less frequent security incident and more throughput of unlicensed users. As shown in 4.3, when the sensing time is 0.1ms, 3.2ms of the time frame is used for encryption and 0.1ms is used for transmission. This is demonstrated more clearly in Fig 4.4. As shown, it takes shorter sensing time and more frequent sensing to detect spectrum space. In this case, $x < x_1 < x_2$. This indicates increase in sensing time from x to x_2 and subsequent decrease in probability of spectrum detection. In (i), the sensing time is short indicating more detection of idle spectrum space. However, it takes longer encryption key time to encrypt the requests. This leads to increase in throughput. This increase is sustained until the sensing time is greater than the encryption key time. At the point, there is also increase in the rate of security incident and leading to decrease in SU throughput.

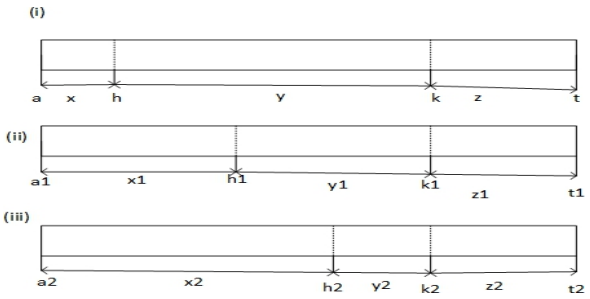

Figure 4.4: Illustration of interplay between sensing, encryption and transmission in CRN

However, longer sensing time increases the probability of false alarm. For effective spectrum detection algorithm, the probability of detection should be as high as possible while the probability of false alarm should be as low as possible.

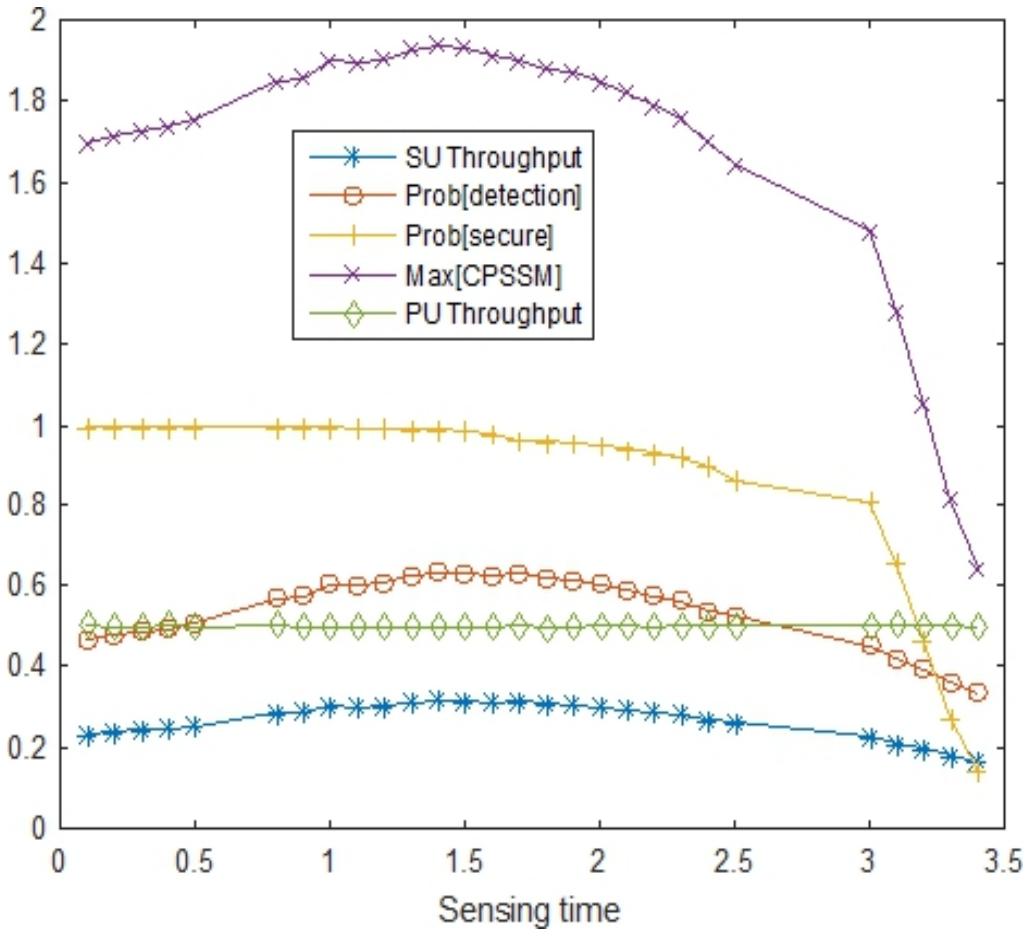

Figure 4.5: Combined probability of detection,probability of being secure and and normalized throughput

Given that the average inter-arrival time of SU request time is 2ms while the sensing and encryption times varies as explained earlier, the throughput of SU is expected to continue to increase until the sensing time is greater than the average inter-arrival time. Reasoning naively, one would expect sharp drop in throughput at that point, but that is slightly not the case since before then, the network would have experienced severe security incidents leading to fall in throughput much earlier than expected as shown in throughput of SU in Fig. 4.5. The probability of detection is high initially due to frequent sensing but decreases as the sensing time increases. Similarly, the probability of system being in secure state is high at the beginning due to smaller sensing time but decreases as the sensing time increases as evident in Fig.4.5. The combined performance, sensing and security measure (CPSSM) is the additive sum of the probability of spectrum detection, probability of the system being in secure state and normalized throughput calculated as shown in equation (10)

$$CPSSM = P(SD) + P(Sec) + NormT \tag{4.10}$$

where P(SD) is the probability of spectrum detection, P(Sec) is the probability that the network is secure and Norm T is the normalized throughput of SU. CPSSM is a straight forward measure for sensing, performance and security tradeoff. Fig. 4.5 shows that it has a clear maximum at sensing time corresponding to 1.4ms. Similarly, an experiment was carried out to determine the minimum point for the combined metrics of probability of false alarm, probability of loss and probability of the network in an insecure state. The probability of loss in this context is the probability of the number of requests that is dropped due to false alarm or PU occupying the channel. In the experiment, the queue limit is set to 5. This implies that any job transmitted after the queue if filled will be dropped. As stated earlier, probability of false is the probability that the spectrum band is idle but CRN declares it occupied. The probability of false alarm in this experiment was determined using the following simple equation.

$$P(SD) + P(FNIB) = 1 \tag{4.11}$$

but

$$P(FNIB) = P(PUOB) + P(FA) \tag{4.12}$$

Therefore,

$$P(SD) + P(PUOB) + P(FA) = 1 \tag{4.13}$$

$$P(FA) = 1 - (P(SD) + P(PUOB)) \tag{4.14}$$

Where P(FNIB) is the probability of not finding idle band, P(PUOB) is the probability of PU occupying the band and the P(FA) is the probability of false alarm. P(PUOB) is represented in the model as the probability that the transmission queue in Fig. 4.2 is greater than zero. As shown in Fig. 4.7, the probability of loss decreases because though there is initial frequent spectrum sensing and subsequent detection of idle band, it takes longer encryption time to encrypt the request before transmission. The encryption node in this context is the bottleneck. This probability raises again when the rate at which the CRN detects and forward requests is less than the encryption rate. Similar to the maximum value for the combined metrics, the minimum point can also be determined by straightforward addition of these metrics as shown in Fig. 4.6.

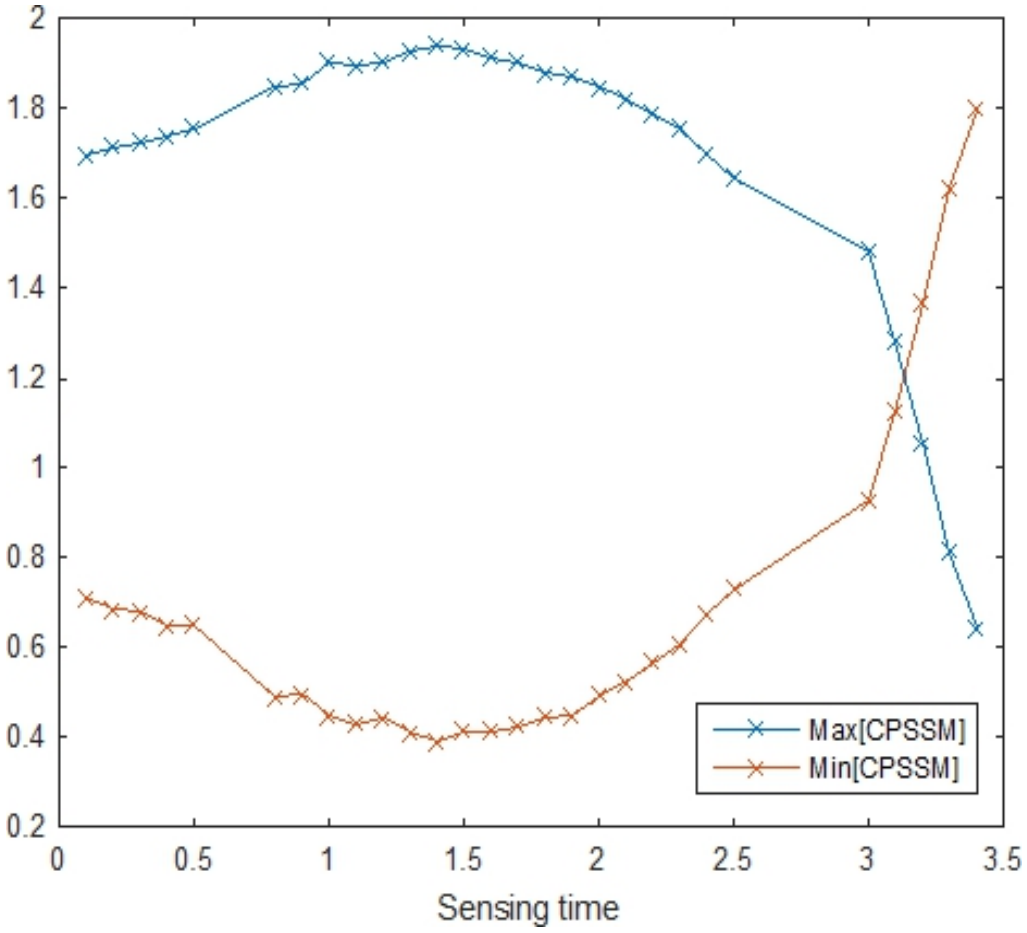

Figure 4.6: Max and Min for the CPSSM

Fig. 4.6 compares the minimum and maximum point for the CPSSM. As shown in the figure, the minimum and maximum point for the CPSSM occur at same sensing time of 1.4ms.

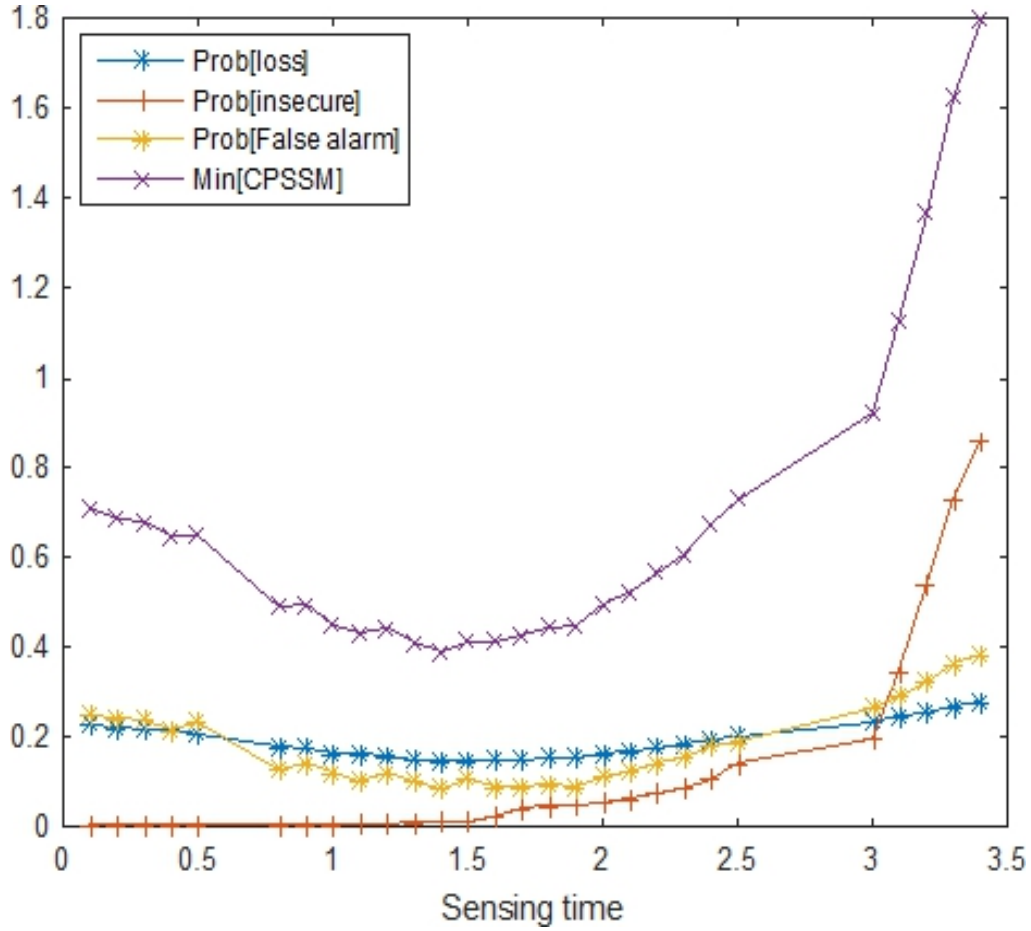

Figure 4.7: Metrics for probability of false alarm, probability of network in insecure state and probability of loss

In practice, this is the average sensing time at which CRN is expected to find an idle spectrum band and if no idle band is detected after this time, then it will sense again after an interval of time.

4.7 Summary

A CRN is proposed with the capability of sensing and encrypting requests in conjunction with security control mechanism. In this context, an 'optimal' impact of sensing, encryption and intrusion detection mechanism on the performance was studied and a tradeoff for optimization of parameters for sensing, security and performance, ensuring good and usable cognitive radios was determined. The result of the simulation shows that there exist an optimal sensing

time that maximizes the combined probabilities of 'spectrum detection', 'CRN being in secure state', and 'normalized throughput.' Simulation results are also presented to validate the analysis. In the next chapter, the proposed SAN model for investigating the impact of scalability on the performance of secured CRN will be presented.

Chapter 5

Impact of Scalability on the Performance of Secure Cognitive Radio Networks

5.1 Introduction

The use of CRN has become necessary due to underutilization of licensed spectrum bands. Study shows that about 75% of allocated spectrum are not being utilized in a number of locations [14] [69]. Regulatory bodies approved CR for SUs to access the idle spectrum band without interfering with the PU signal. The main bands of interest for the CR are very high frequency (VHF) and ultra high frequency (UHF) due to their excellent propagation [70]. The licensed owners of these bands are television, mobile and satellite operators. Signal from these operators can be very low and require high detection rate. Sensing is therefore required to identify an idle spectrum band. Sensing in this context is probing through spectrum band to detect when it is idle [3]. It is carried out periodically and only when there are requests to transmit. If an idle band is detected, SU will use the space for the transmission of its requests based on the SLA. CRN sensors are powered by battery [71]. A combination of sleeping and censoring is assumed as in [72] in order to conserve energy. Sleeping implies that the radio device switches off its power when not sensing to save power. Censoring in contrast denotes sensing and making decisions about the status of the band.

It was stated in [26] that PUs may not allow SUs to access their band without benefit. Usually, SUs are admitted to the band based on the benefits offered by the competing SU entities.SUs with more benefits to PUs are admitted first. For instance, SUs with history of less interference to PU signal are considered a priority over those likely to cause more

interference.

Though idle band may be identified by CRN, however, SUs may experience denied access to the spectrum due to attacks on CRN or insufficient resources for security processing and transmission, leading to drop in SU throughput. To enhance the throughput and maintain optimal security, [73] [11] proposed sensing, security and throughput trade-off. The aim was to determine the sensing time that maximizes the combined metrics for sensing, security and performance. Unfortunately, the above studies only considered static resources. In this case, though the idle band may be identified, the available static SU resources may be inadequate to fully utilize the idle spectrum band before the reappearance of PU. Additionally, there was no emphasis on the detection of SU interference to PU signal.

This chapter proposes scalability as an approach to fully utilize the idle spectrum band and at same time propose a sub-model to detect SU interference to PU signal. Scalability in this context is the ability of the CRN to dynamically add or remove resources according to the service requests [73] [74].Very often, PU activities on spectrum band may lead to delay in transmission of SU requests. However, error in detection of PU signal (miss detection) may result in an additional increase in SU throughput as would be explained in the subsequent Section. In this case SU and PU will be transmitting simultaneously on the band. This can be used to predict SU interference level to PU signal. Security incidents also obstruct SU from using the idle spectrum band. These scenarios result in increase in SU requests in the queue. To increase requests transmission, if an idle band is detected, considering that there is a build-up of SU requests, additional resources are dynamically released in effort to largely utilize the idle band for the transmission of waiting SU requests before the reappearance of PU. This way, much of the SU requests are transmitted within the given idle time of the spectrum. The main objectives of this chapter are:

1) To introduce scalability as a means of increasing the performance of CRN.

2) To compare SCRN and UCRN

3) To propose a model and quantify the interference level of SU to PU signal;

4) To produce an architectural design of CRN for optimal performance upon sudden surge in SU service requests.

5.2 Brief overview

CRN allows SUs to sense licensed spectrum in order to transmit if an idle band is detected. Due to the unpredictable nature of PU activities on the spectrum, it is imperative that SU swiftly use the band as soon as it becomes available.However, during sensing, the CRN could falsely detect the band idle when actually occupied by PU, leading to harmful interference to PU signal. CRN could also detect the band to be occupied when idle. These scenarios create harmful interference to PU, packet loss or underutilization of spectrum band for SUs. This work proposes SCRN in SAN formalism with SU interference detection mechanism to study the impact of scalability on the performance of single node of CRN towards an effective optimization of an idle band by SUs. In this context, the instant the band becomes idle and there are SUs request waiting for encryption and transmission, additional resources are dynamically released in order to largely utilize the spectrum space before the reappearance of PUs. These extra resources make the same service provision, such as encryption and intrusion detection as the dedicated resources. Typical numerical simulation experiments are carried out 'with' and 'without' scalability in consideration to miss detection and false alarm. This is based on the application of Mobius Petri Net package, in order to determine the impact of scalability towards the enhancement of nodal CRN sensing, security and performance trade-offs. The results indicate sustained performance of SUs at the CRN node due to scalability of resources during heavy traffic periods.The results also shows an unexpected increase in SU throughput when there is an interference to PU signal.

5.3 Review of Related Works

It has been proposed in the literature that the efficiency of CRN should be improved in terms of sensing, security and performance. An experiment was carried out in [75] [76] to improve the performance of service channel by applying scalability approach. The result of the simulation shows an increase in the throughput as a result of this approach. An investigation was carried out in [74] to study scalability and performance of web application on cloud platform. The work presented novel dynamic scaling architecture with load balancer

for routing user requests to web application deployed on a virtual machine. The work demonstrated an increase sustenance of performance upon sudden surge in service demand. A study was undertaken in [11] relating to sensing-throughput trade-off in cognitive radio networks. The focus was to determine the sensing duration for the maximization of the achievable throughput with sufficient protection of PUs requests. The analysis of the simulation results revealed that there exist an optimal sensing time that yields the highest throughput. An experiment was carried out in [22] to determine the number of sensing nodes required in cooperation in order to improve the accuracy of spectrum detection. The optimal number of cooperating radios needed to minimize detection error probability and maximize throughput in CRN for Wi-Fi networks were derived. One of the studies above considered dynamic infrastructure but not in the context of CRN.The study also did not reflect on security and its performance implications. The rest of studies did not take into consideration the unpredictable nature of service demand and the application of scalability as appropriate to improve the performance of CRN.

5.4 CRN and CLOUD

Cloud computing is used to define an application delivered as a service through the internet and system software that provide the service [77]. It has been found to provide some advantages to CRN. In [26], cloud computing infrastructure was used to store spectrum opportunities. This way, it was easy for SUs to access and securely use idle spectrum band. Sensors of each of the multiple spectrum reports the idle spectrum space to a geolocation database located in cloud. In this work, scalability feature of cloud computing has been exploited to improve the utilization of idle spectrum and largely transmit waiting requests. In this case, a load balancer is used to add resources when needed or withdraw it when it is no longer required.

5.4.1 Scalability of CRN Resources

Scalability is a feature of cloud computing that allows its resources to be scaled according to service demand [78]. It is difficult to achieve due to unpredictable nature of service demand and unknown nature of service invocations. In order to achieve scalability, [75] introduced two effective scalability approaches: service replication and migration. Service replication is a method of making a replica of service already running on a main server without affecting the operation of the service in progress. This is a way of securing additional resources to bear up against large volume of service requests. Service migration is an approach that places a service on another node when a node cannot provide high Quality of Service (QoS) as a result of problems. In the model under study, it is a means of transferring service to a new server when there is service degradation resulting from unpredictable service demand. This transfer occur when the number of requests in queue is of a certain threshold predetermined by SLA.The flowchart for the scalability of CR resources is as shown in Fig. 5.1.

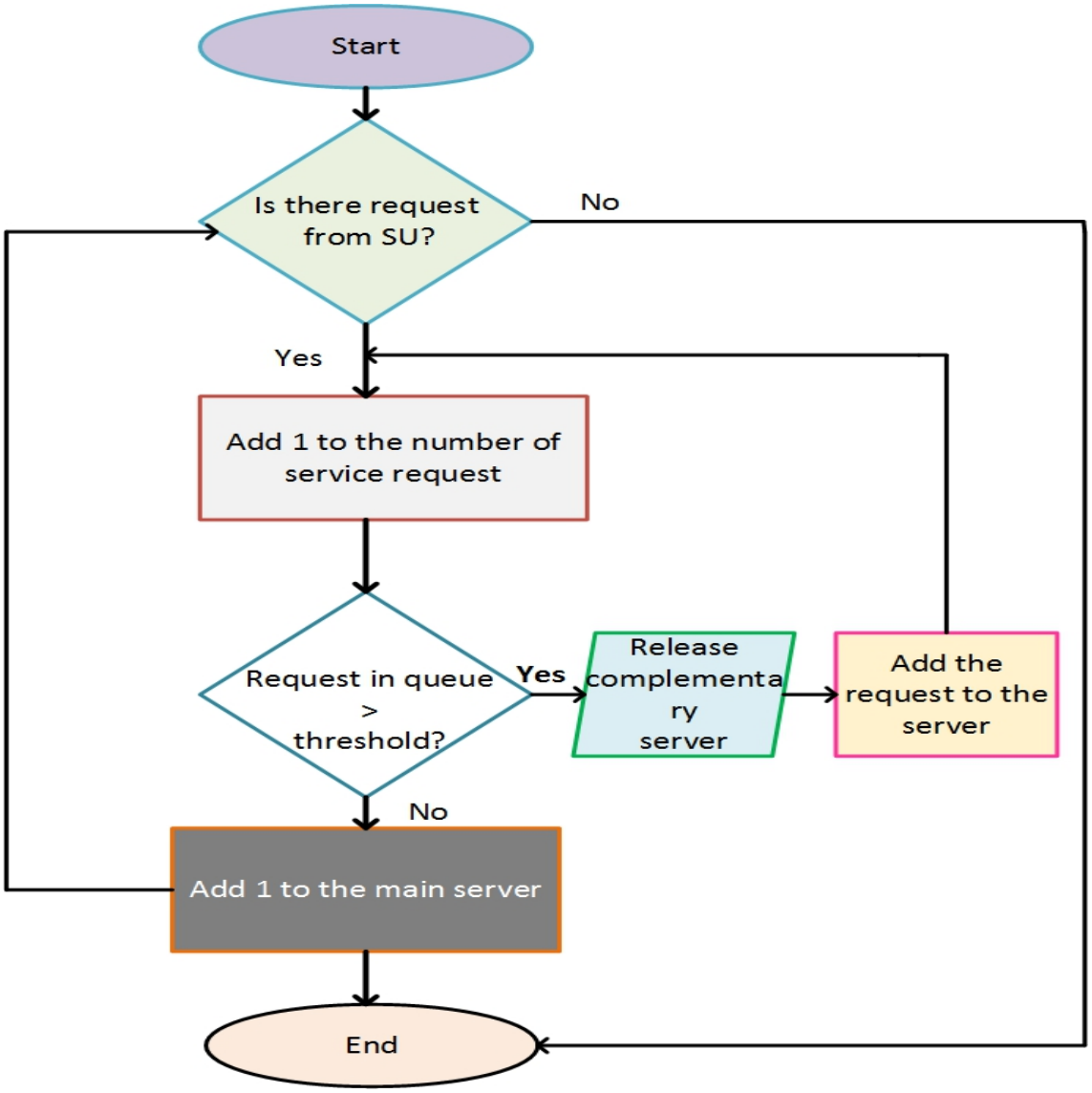

Figure 5.1: Flowchart for the scalability of CR resources

Scalability is highly needed in a long term 'ON' and short term 'OFF' PU activities. This is further explained in Section 5.7. Long term 'ON' is used to describe a period during which the band is mostly occupied by PUs. In a long term 'ON', PUs utilize the band for an extended period of time while SUs are in queue waiting for PUs to vacate. When the band becomes idle, SUs will swiftly transmit all their waiting request within the given time by releasing additional resources since the waiting requests may have already exceeded the threshold. However, the utilization of the idle spectrum band depends on the sensing time of CRN sensor. If it takes longer time to sense, then SU will be denied the opportunity to transmit all its requests. In this case, the average number of requests required to cause the

release of additional resources will remain below the threshold and no additional resources is released.

5.5 Predetermine threshold for performance measurement

In queue network model such as GE/GE/1/N, length of queue is an important performance metrics to determine the quality of service of a CRN. It is the average number of requests waiting to be served in queue. This can be expressed as [79].

$$L = \rho/2(1 + (Ca^2 + \rho Cs^2)/(1 - \rho)) \tag{5.1}$$

$$Lq = L - \rho \tag{5.2}$$

where L is the number of requests in the system

Ca^2 is the square coefficient of arrival

Cs^2 is the square coefficient of service

Lq is the number of requests in the queue

The server utilization is given by

$$\rho = \lambda/\mu \tag{5.3}$$

where λ is the request arrival rate and μ is the service rate. It is assumed that to have a stable system, $\lambda < \mu$ must hold. This in words implies that to have stable network without much volume of requests in the queue, the mean arrival rate must be less than the mean service rate [26] [79]. Queue discipline such as FIFO commonly obtainable in queue network model is complex to represent in SAN model. However, SAN model is preferred because it is a graphical tool for the representation of systems whose dynamics are characterized by conflict, concurrency, synchronization, mutual exclusion and other systems which cannot be described by a queuing network model. SANs just like GSPNs comprises of places, transitions, arcs and inhibitor arcs which defines the structural components. While places are used to represent queue or buffer for incoming requests, transitions are used to represent

actions that changes the state of the system. Arcs connect input place to transition and from transition to output place. Also, inhibitor arcs are used to enable firing of transition when a place contain a token less than the multiplicity required to enable the transition. These have been explained in detail in Chapter 3.

The network under study is represented by a single server connected to a redundant one that only come to operation if r_i >k, i=1,... where r is the number of requests in queue and k is the queue capacity. The admission of requests to the dedicated service station is a function of the capacity of the queue. If requests arrive and find the queue full, i.e. r_i=k, i=1,2,..., a complementary channel would be provided.

In the proposed SAN model, the number of requests in a queue is represented as the average number of tokens in the place 'Enc queue' as shown in Fig. 5.4. It is used as a indicator to determine when an additional resources is required. If the average number of requests in the place is greater than a predetermined threshold, then a complementary channel is released, but withdrawn otherwise.

5.6 Determining the Detection Threshold

Most existing works in CRN assume that noise power is constant in the licensed spectrum over a period of time. However, [66] presented an adaptive dynamic energy detection strategy with adjustable threshold which depends on the noise power. This is because in reality, noise power varies over time due to temperature change and depending on the radio frequency hardware characteristics. In some applications, it appears simpler to identify signal-free sample due to infrequent occupation of the channel. In CRN, it is more challenging to identify samples with only noise. In order to ensure the availability of noise only samples, [66] introduced the idea of specifying a fixed frequency band with no transmission allowed. In the proposed idea, the dedicated frequency band for noise power estimation is denoted by BR and the part to be monitored for dynamic access by Bc as shown in Fig. 5.2.

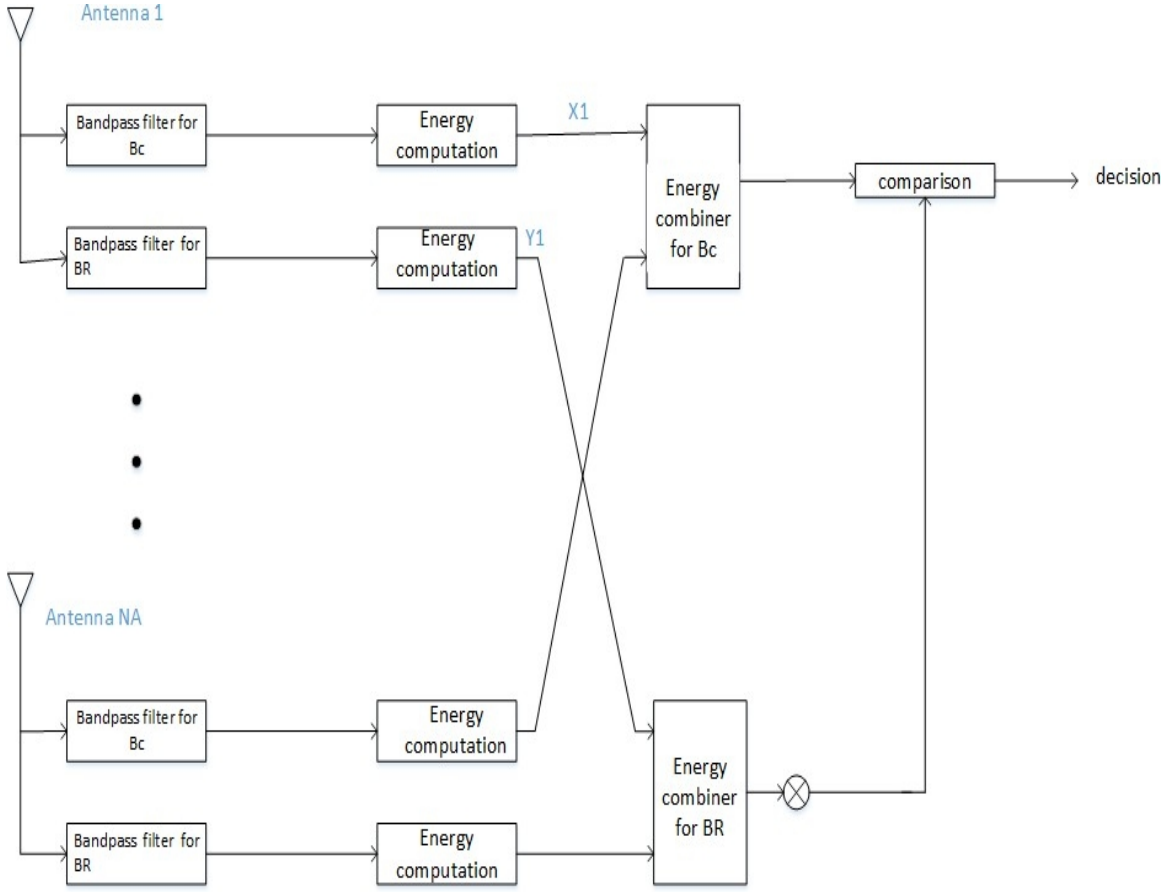

Figure 5.2: Proposed structure for determination of detection threshold [66]

Since the noise is assumed to be white, therefore, the noise power in BR is proportional to the noise in Bc. Therefore, the proposed estimation threshold is obtained by multiplying the noise power measurement in BR with a factor μ representing the desired level of false alarm probability.This is then used as a threshold for detection of PU signal.

5.7 CRN and PU activity model

It was stated in [26] [81] that PU uses the spectrum in on-and-off manner. It occupies the band for a period of time and then vacate. CRN employs spectrum sensing to detect the off period and allow SU to use it. The Fig. 5.3 demonstrates the idle and busy time of the spectrum band.

If the PU occupies the spectrum band more frequently, it will only allow short interleave

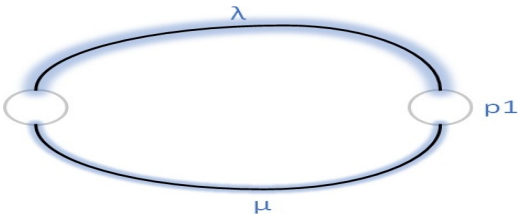

Figure 5.3: Transition diagram for the spectrum going from idle to busy state

spectrum space for cognitive use [81]. This will result in decrease output of SU. The throughput can be improved within each interleaved spectrum space by automatically releasing additional resources if the number of SU requests is greater than the predetermine threshold. For instance, the probability of spectrum band being in idle state (interleave space) for cognitive use can be estimated using Kolmogorov equations [82] as shown in equation (5.4)-(5.10). The symbolic solution to this Kolmogorov equation can be obtained using maxima. Maxima is a software package that can manipulate symbolic and numerical expressions, including differentiation, integration, Taylor series etc.

$$\frac{dp_0}{dt} = -p_0\,\lambda(t) + p_1\,\mu(t) \tag{5.4}$$

$$\frac{dp_1}{dt} = p_1\mu(t) - p_0\,\lambda(t) \tag{5.5}$$

where $\frac{dp_i(t)}{dt}$ is the rate of flow of probability to i. Solving the equation using Maxima, the following symbolic equations can be obtained [82]

$$P_0(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda e^{-}(\lambda + \mu)t}{\lambda + \mu} \tag{5.6}$$

$$P_1(t) = \frac{\lambda}{\lambda + \mu} - \frac{\lambda e^{-}(\lambda + \mu)t}{\lambda + \mu} \tag{5.7}$$

where μ is the rate at which PU reoccupy the band and λ is the rate at which the spectrum band becomes idle. The equation (5.7) shows that the long term availability of the spectrum for cognitive use is defined as [82]

$$P_0(\infty) = \frac{\lambda}{\lambda + \mu} \tag{5.8}$$

and the long term unavailability of the band is

$$P_1(\infty) = \frac{\mu}{\lambda + \mu} \tag{5.9}$$

Equation (5.9) can be further represented as

$$P_0(\infty) = (1 + \frac{\lambda}{\mu})^{-}1 \tag{5.10}$$

It simply means that if the rate at which PU accesses the spectrum band decreases, then the probability for the availability of spectrum for cognitive use increases leading to improvement in SU throughput.

5.8 Constraints on SU spectrum Access

There are some identified factors that impede the use of idle spectrum by CR users:

Regulations: Regulations have put constraints on the SU's access to spectrum band. This is because regulatory bodies restricted SUs to the use of the bands only when not in use by PUs. It is mainly to protect PUs from harmful interference of SUs [26]. Therefore, CRN is required to sense the spectrum band and only transmit if an idle band is detected. As stated earlier, longer stay of PU on the band denies SU the opportunities to use it. This is mostly common in urban areas where they are high concentration of PUs. In rural areas, there is infrequent use of spectrum band by PUs. In this case, the band is mostly available for cognitive use. However, CRN are still required to sense the spectrum to ensure no interference whenever PU wants to access it.

Errors in Spectrum Detection: Errors in spectrum detection, for instance, false alarm is an advantage to PU as such errors protects it from SU interference. False alarm is detecting the band occupied when actually idle [3]. In miss detection error, CRN falsely detects the band idle when occupied by PU and permit SU to transmit, thereby causing interference to

PU signal. Error in detection of PU signal may result in an increase in SU throughput.

Let SU throughput when only PU is transmitting be T_pu,

throughput when PU and SU are simultaneously transmitting (miss detection) be $T(pu + su)$ and throughput when only SU is transmitting be denoted by T_su.

In event of interference, the total SU throughput can be expressed as $T_i = T(pu + su) + T_su$

If there is no interference, then $T_n = T_su$

where T_i is total throughput during interference

and T_n is the total throughput when there is no interference.

This implies that if there is no interference, SU are assumed to have used only the 'OFF' period when PUs are not transmitting for their transmission. Conversely, if there is interference, then the SUs are assumed to have transmitted simultaneously with PUs and continues the transmission after the PUs have vacated the channel. This is the case that result in increase in SU throughput. This throughput is SU bits assumed to be corrupted during the interference with PU. The packets transmitted during the interference is taken to be corrupted since it will arrive out of order. This is in assumption that the network is using packet switching in which long messages are divided into smaller packets and send through the network. It uses store and forward transmission and messages are received in order before transmission. The interference may be caused by attack [8] or multipath fading. In this work, it is assumed that the probability of false alarm increases as the sensing time increases.In this case, SUs are denied the opportunities to use the spectrum band leading to decreased throughput of SU.In contrast, short sensing time leads to increase probability of miss detection. Using energy detection technique, the probability of false alarm can be expressed as [11]

$$prob(T(x) > (!H_0 true) = \int_{(2}^{r\ \infty} fH_0(L(x))dL \qquad (5.11)$$

where T(x) is the energy of the received signal which is compared to a predetermined threshold given in equation (4). H_0 denotes noise sample. L(x) is the Likelihood ratio of the data under observation. Based on the above equation, false alarm can be expressed as the probability that the received signal T(x) is greater than the threshold given that PU is not active on the band. If this probability increases, then SUs are denied opportunities to use the spectrum band.

Malicious Attack and Detection: One of the factors limiting SU from sharing spectrum band is malicious attack. Attackers may try to eavesdrop on the content of requests being transmitted. In [10], a model is proposed that encrypt request and also detect an attack. This model is not tailored to a specific system. The operation of the system is ceased on detection of attack. This causes delay and increase in the number of requests waiting to be transmitted and invariably lead to decrease in throughput of SU transmitter.
Any of the above scenarios could lead to a build-up of the number of requests waiting to be transmitted. When the queue is long, taking into account that the idle time of the spectrum band decreases as soon as PU vacate the channel, the propose system releases additional resources to complement the dedicated one. This is to largely transmit the requests before the reappearance of PU on the band.

5.9 Security implementation in the proposed SAN model

This work adopts the combined sensing, security and performance tradeoff in CRN [73]. In the model, arriving SU on finding an idle encryption node gets encrypted and then transmitted. The model included security control that ceases the operation of the CRN on intrusion detection. The effects of encryption and security control is quantified and sensing time at which the combined tradeoff is maximized is predicted. In the proposed model, sensing time is used as the reference point to determine the improvement in the performance as a result of scalability. In a short sensing time scenario, the sensing node senses more frequently, thereby detecting and transmitting more requests, though susceptible to miss detection error. However, as the sensing time increases, the probability of detection decreases resulting in sensing node as the bottleneck. This implies that when there are waiting requests to transmit, extended sensing time indicates that there is inefficient spectrum detection which limits the transmission of these requests.

5.10 SAN and Mobius Petri Net Package

QN, SAN and GSPN models are some of the modelling approaches that can be used to generate the required traffic for the network under study. As stated earlier, QN representation of the model behaviour are only possible where only few details are required in the specification of the model [83]. On this note, SAN is a preferred in the representation of the proposed model. This is because, SAN is introduced to capture system behaviour involving synchronization, concurrency and conflict phenomena. Mobius petri net package is a simulation tool that support SAN model. The package has some features to abstract the behaviour of the proposed model. A transition, graphically represented as rectangular bar as detailed in Chapter 3 are used to generate actions that changes the state of the system [84]. The transition is enabled when an input place connected to transition contain at least one token. Enabling indicate execution of process while firing of a transition corresponds to completion of execution process [84]. Enabling and firing of a transition is associated to some random delay which is exponential [84]. Circular component is used to represent the buffer for storing incoming requests. Transitions connected to the buffer are enabled immediately there is arrival of token to the place (buffer) indicating start of execution process. Tokens are requests or packets being transmitted through the network. There is arc for connecting input place to transition and from transition to output place. Inhibitor arc stops the execution of enabled transition. Inhibitor arc inhibits the firing of enabled transition.

5.11 Proposed Model

The proposed model is presented as a single node of CRN with two classes of requests (PU and SU requests) on a single spectrum band. PUs requests have priority over SUs requests. The model consists of 3 components: SU activity, PU activity sub-model and security control component. As shown in Fig. 5.4.,

the PU arrival is modelled as the firing of the transition 'PU arrival'. There are two tokens in the place 'idle space'. Transition 'PU arrival' is enabled whenever there is at least one token in the place 'idle space'. A token is deposited in the place 'PU in service' when the

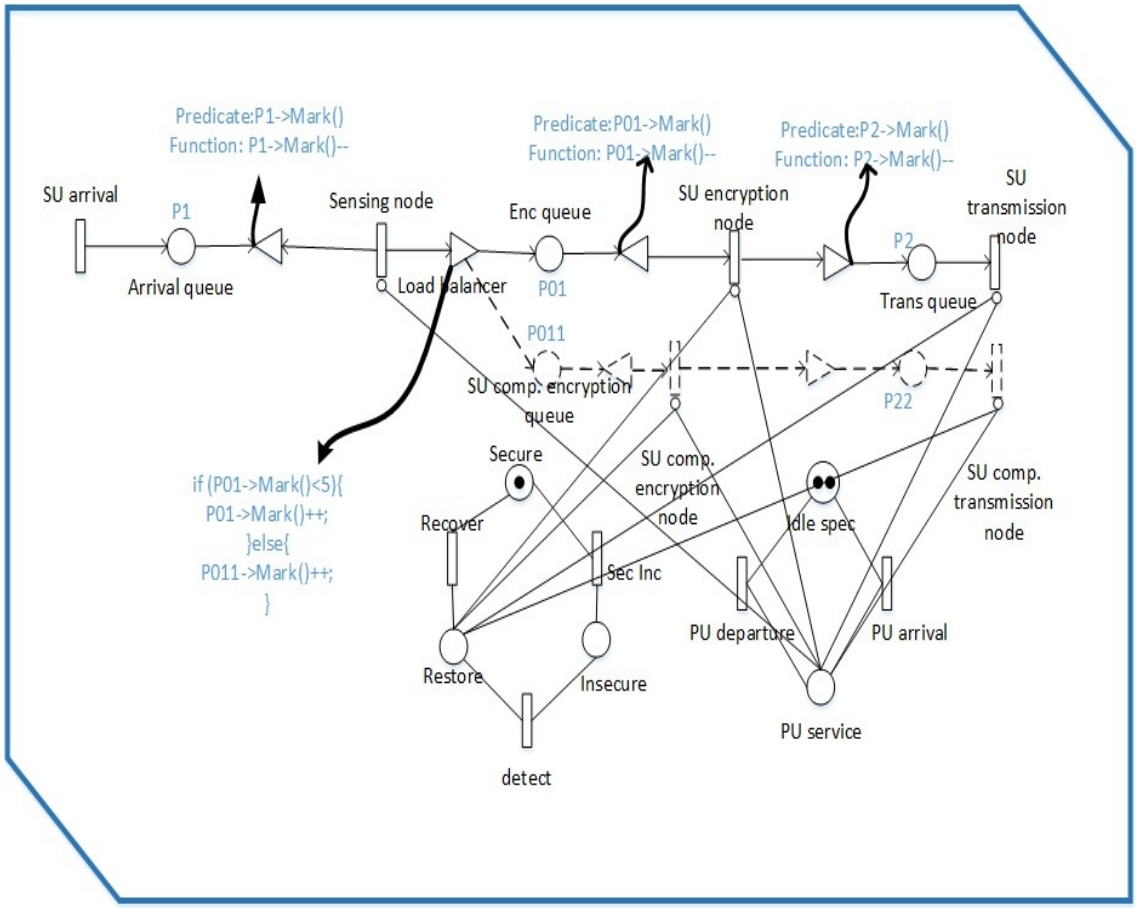

Figure 5.4: Proposed SAN model for CRN

transition 'PU arrival' completes. Firing of transition 'PU departure' transfers the token back to 'idle space' indicating completion of service by PU. The transfer of token to place 'idle band' shows that the band is now available for cognitive use.The second token is used to detect interference (miss detection) as shown in Fig. 5.5.

In the model, there are 3 states. State 1 with two tokens at the 'idle space' indicates an idle band for CR use. In other words, there are no PU request in the band. The probability that the band is idle and available for CR use is

$$P[idlespace = 2] = 1 - P[PUinservice = 1] \tag{5.12}$$

In state 2, there is PU arrival demonstrated by transfer of token to the place 'PU in service'.

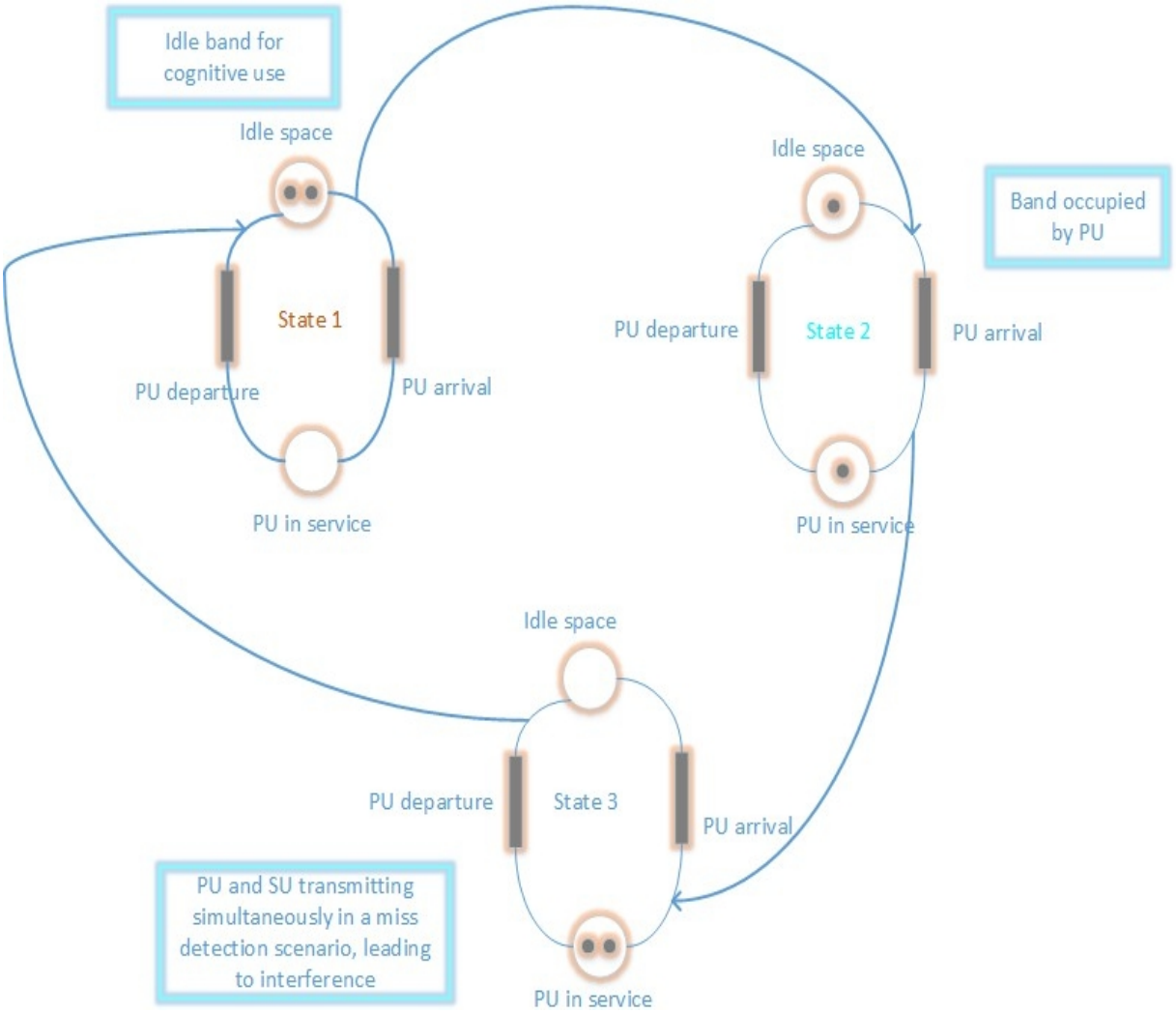

Figure 5.5: Token transitions in the proposed model

This indicates that PU is transmitting in the band and no interference from SU. The probability that the band is unavailable for CR use is

$$P[PUinservice = 1] \tag{5.13}$$

State 3 shows that the two tokens are in a place 'PU in service' implying a miss detection leading to simultaneous use of the band by both SU and PU. The probability of miss detection is

$$P[PUinservice = 2] \tag{5.14}$$

Similarly, transition 'SU arrival' generates SU arrivals which are temporary stored in SU arrival queue pending the detection of an idle band. These requests are transferred to the encryption node as soon as it is detected idle. If the node is busy by other SUs, there are stored in the queue. Load balancer are used to observe the average number of requests in the place 'Enc queue' and determines when an additional resources are needed.

SU components consist of sensing, encryption and transmission nodes. Encryption node and SU transmitter are replicated and made redundant in events of low traffic but comes into full operation when there is a surge in service demand. It is assumed that SUs pay more for this extra services rendered to them. The sensing, encryption and transmission nodes for the dedicated resources are connected to a security detection control model. The complementary resource which consist of encryption and transmission nodes is also connected to security control.

In the security control, the token in the place 'Secure' is used to indicate a secured network. However, firing of transition 'Sec Inc' shows security breach which is demonstrated by transfer of token to place 'Insecure' but not detected. The detection of the security incident is indicated by the firing of the transition 'Detect', transferring the token to the place 'Restore'. Token at the place 'Restore' block the operation of CRN until a new key is generated. The rate at which the security fails depends on the length of the encryption key. It was stated in [73] [10] that the longer the encryption key, the stronger the security of the network and vise-versa. In the proposed network, extensive sensing has adverse effects on the security and by extension the throughput of the SU. More information about the combined sensing, performance and security tradeoff in CRN can be found in [73]. As shown in Fig. 5.4, the performance part of the model has a redundant resources that only come to operation when the number of requests in the place 'Enc queue' is greater than predetermined threshold.

It is challenging to choose the right input parameter that is relevant in determining the behaviour of the proposed model. However, considering the model verified by [10], it is easier to formulate the input parameter for the proposed model.

The experiment was started with sensing time of 0.1ms to 3.4ms while the encryption time varies from 3.4ms to 0.1ms for both the main server and virtual server. It is assumed that

the encryption time is proportional to the encryption key length. The rate of service request for PU varies from 0.01 to 0.5 (0.5, 0.1, 0.01) while SU requests rate is 1.0. The transition rate for SU transmission node is 10. The arrival and service rate of PU is 1. Time to security incident starts from 15100ms and decreases in steps of 1000ms until it gets 1100ms, then decreases in steps of 100ms until 100ms and further decreases by (time-time/2)ms in each progression until it gets to 12.5ms. In this work, the frame structure of [19] in which each CR user is assigned a frame size is assumed. Frame is a transmission unit which can be divided into fixed number of slots. The first slot in the frame is used for sensing the spectrum to establish the status the band. The second slot is used for encryption and the last slot for transmission. As shown in the Fig. 5.4, the request generated by SU joins the SU queue. This activates the sensing node. The sensor senses the band through the place 'PU in service' to detect the presence or otherwise of the PU signal. If there is token in the place 'PU in service' then no SU encryption process is allowed to take place and vice versa. Similarly, if the same place contain a token, no SU transmission takes place. However, if the token moves from 'PU in service' to 'idle spec' then SU requests can be encrypted and transmitted.

5.12 Results and Analysis

This experiment is carried out to determine the optimum throughput that is achievable in a SCRN and unscalable CRN (UCRN) with consideration to encryption and security control mechanism. It is also aimed to determine the optimum value for the combined sensing, security and performance trade-off in SCRN.

In a SCRN, the surge in service demand is handled by provisioning of additional resources in order to swiftly utilize the band before the reappearance of PU. However, the capacity of the resources should not exceed the spectrum bandwidth in order to avoid losses.

The Fig.5.6 - 5.22 show the result of the experiment carried out. The total throughput attained by SU in a SCRN and UCRN depend on the activities of PU on the band as illustrated in equations (5.4) - (5.10)

At the beginning, the average sensing time is 0.1ms and SU request rate is 1.0. This time increases in steps of 0.1ms until 3.4ms. It implies that the network senses at an average

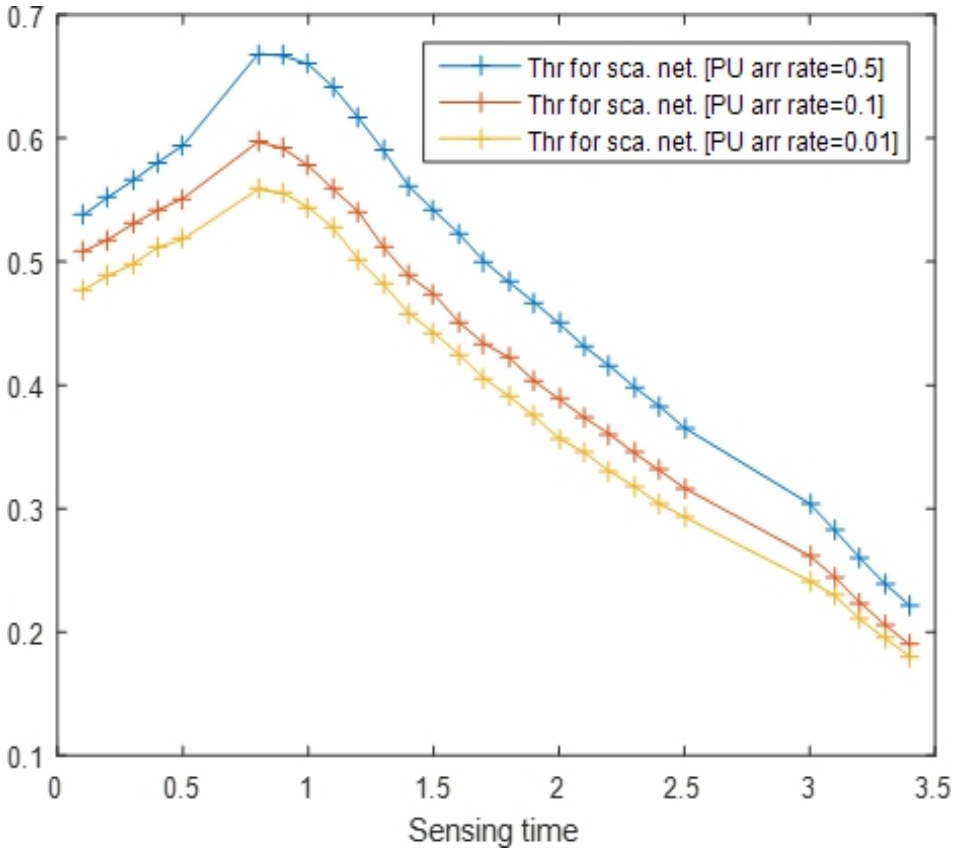

Figure 5.6: Throughput for the SCRN

rate of 10 down to 0.29. PU request rate of 0.01, 0.1 and 0.5 are used and remain constant for each experiment. Since sensing, in this case, occurs frequently at initial rate of 10, the probability of detecting and transmitting through an idle spectrum band is high, resulting in large volume of SU requests being transfer to the encryption queue waiting for encryption and to be transmitted. Consequently, additional resources, based on the queue length is introduced. This results in overall increase in throughput. The increase in throughput is expected to continue until SU request rate is greater than or equal to the sensing rate. At this instant, the complementary resources is withdrawn. The throughput as a result of the additional resources is demonstrated in Fig. 5.8.

As visible in 5.7., the improved overall SU throughput continues until its peak at sensing time corresponding to 0.9ms. Thereafter, the throughput is seen to decline. This is demonstrated

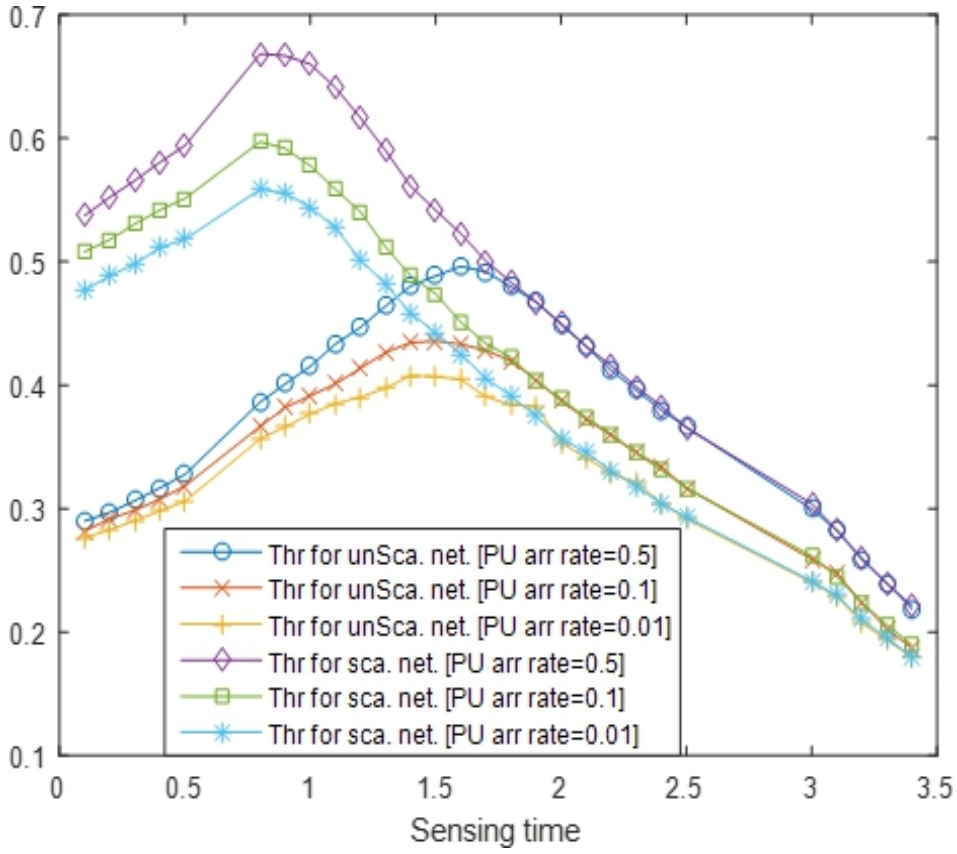

Figure 5.7: Throughput for the SCRN and UCRN

by continues drop in throughput until the resources is assumed to be withdrawn at the sensing time of 1.75ms which is the point where there is intersection in throughput between SCRN and UCRN as revealed in the figure. At this sensing time,requests generated by SU may not be largely transmitted because the sensing is not frequent enough to detect the required spectrum space to transmit them.As such,the requests are either on the queue or are lost. This implies that increase in packet loss due to sensing process is proportional to increase in sensing time as demonstrated in Fig. 5.12-5.14. It also depends on the PU arrival rate. This is because, the probability of miss detection is minimized when the PU arrival rate is 0.01, implying very minimized interference from SU. PU arrival rate of 0.5, however, demonstrates a high probability of miss detection and higher interference. Since sensing rate is determined by the rate of packet generation by SU, then it is essential that on detection of interference, SU reduces its rate of packet generation and consequently sensing frequency.

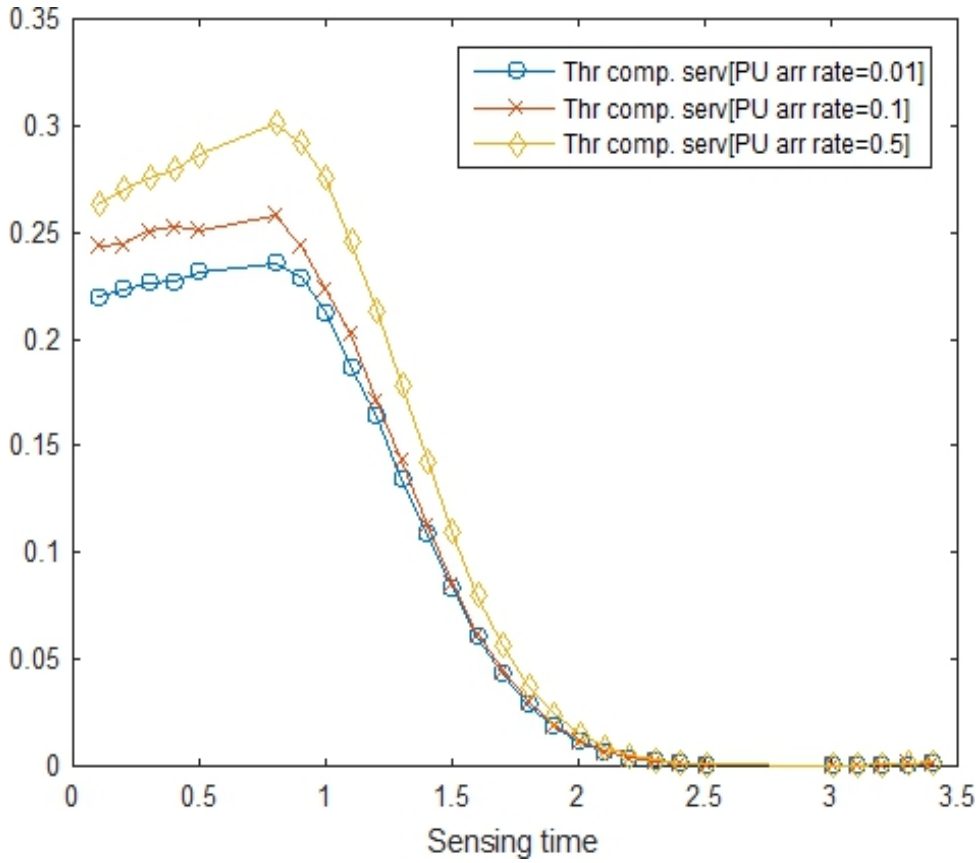

Figure 5.8: Throughput of SU via complementary resources

Similarly, the packet loss probability due to encryption delay is seen to be decreasing inversely with the sensing time. This is because, though encryption node can encrypt more request as sensing time increases, however, fewer requests are forwarded to it due to increase in the sensing delay. This is the case for both SCRN and UCRN as shown in Fig.5.9.

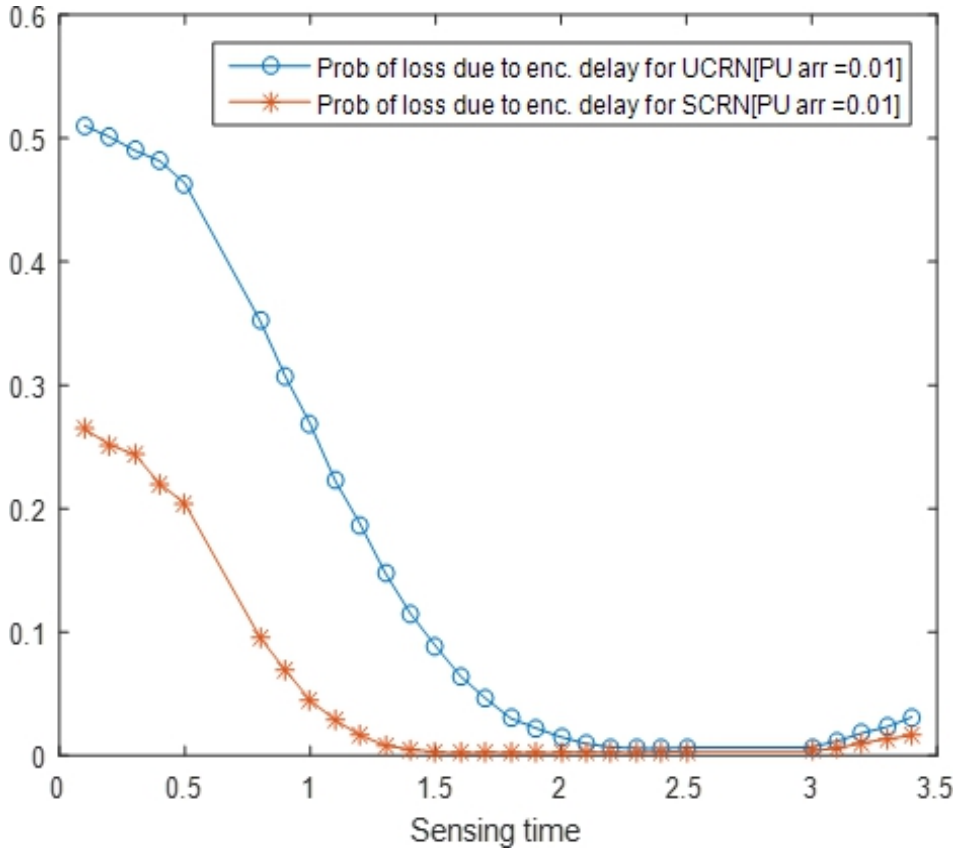

Figure 5.9: Prob. of loss due to encryption delay for the SCRN and UCRN

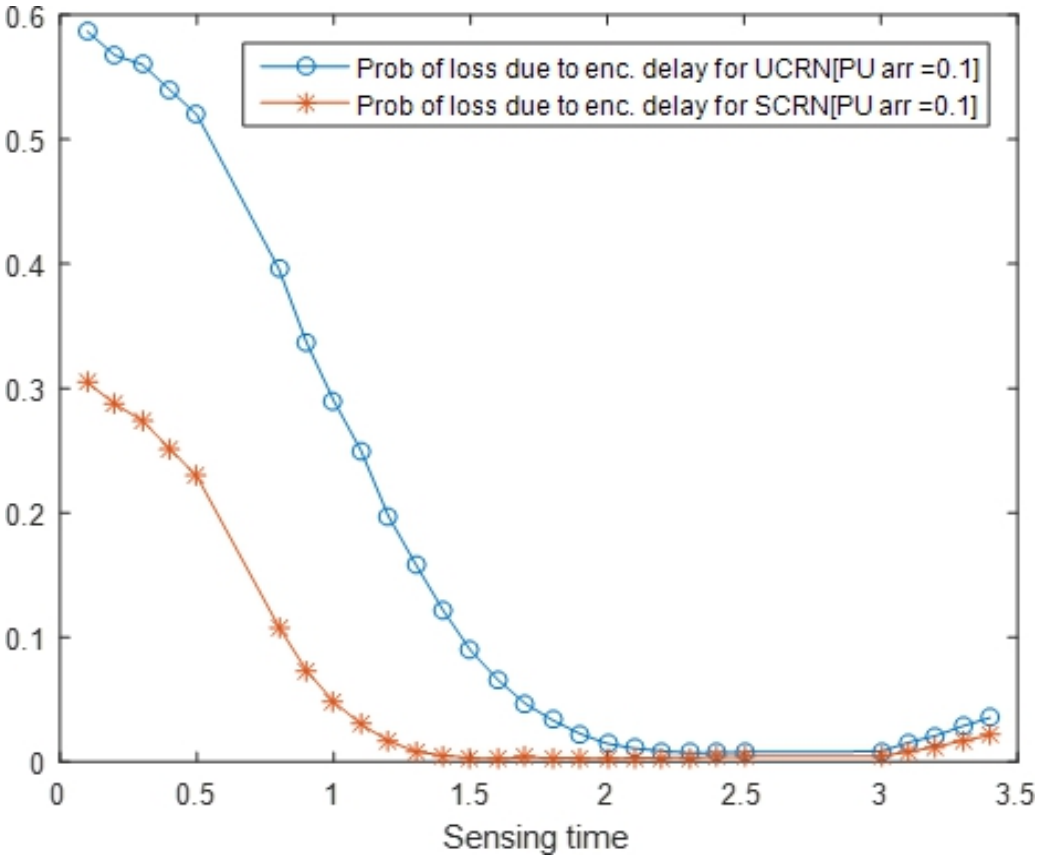

Figure 5.10: Prob. of loss due to encryption delay for the SCRN and UCRN

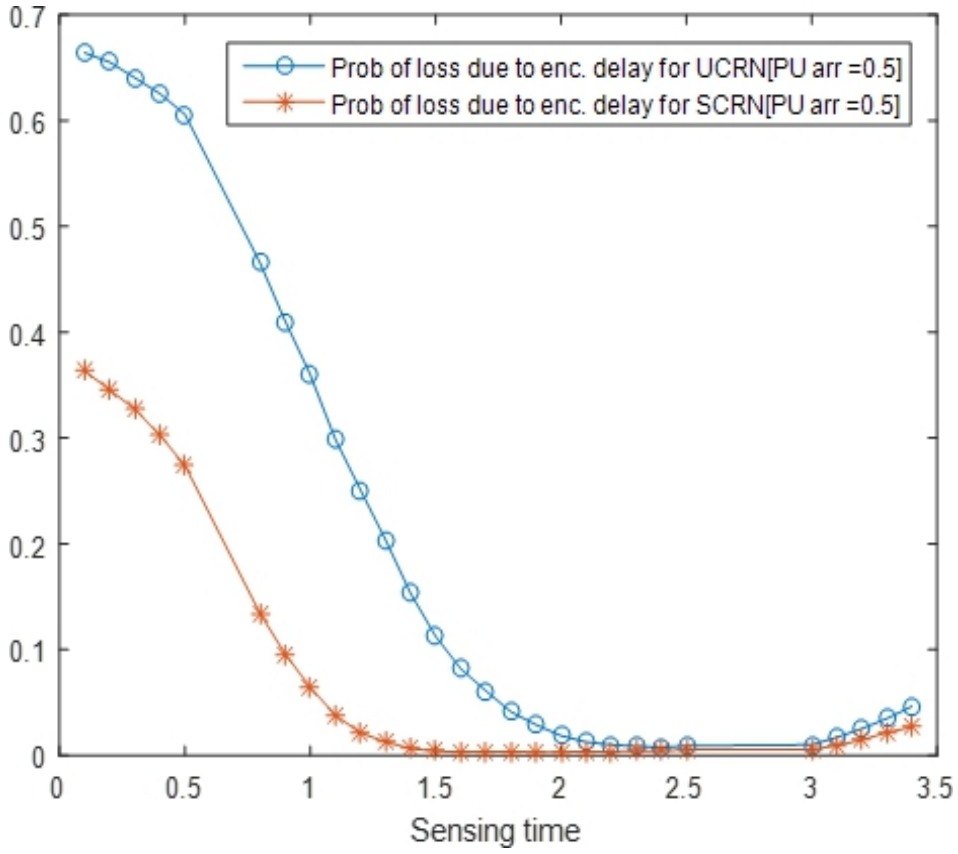

Figure 5.11: Prob. of loss due to encryption delay for the SCRN and UCRN

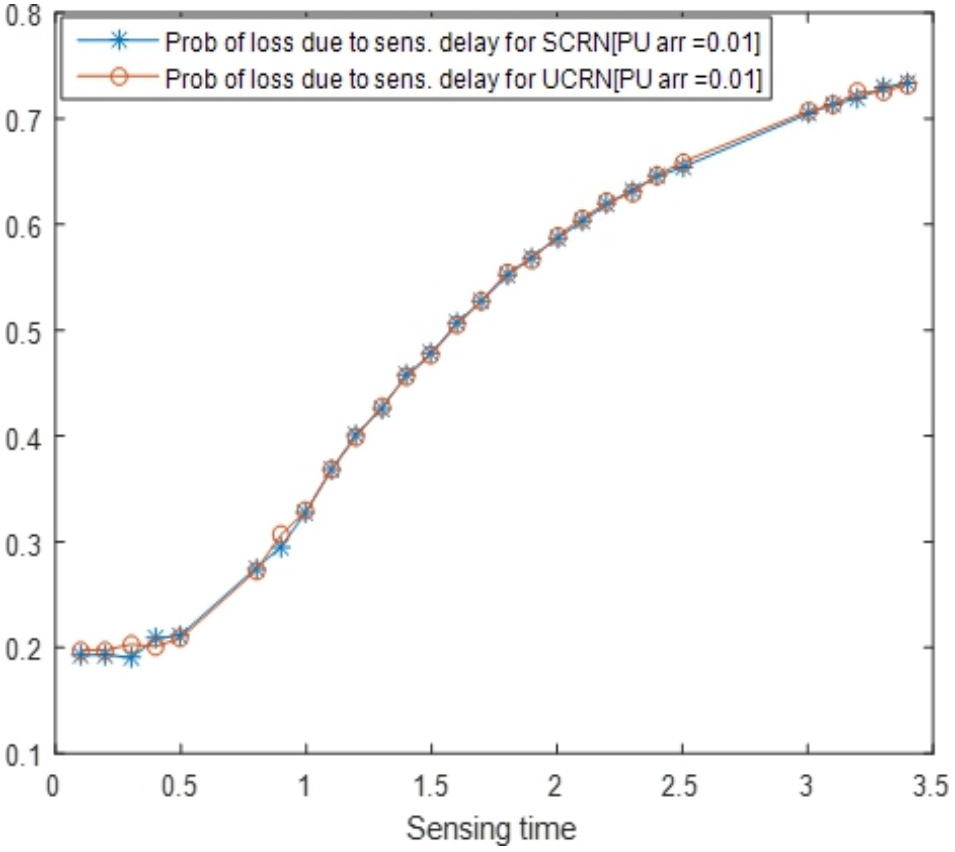

Figure 5.12: Prob. of loss due to sensing delay for the SCRN and UCRN

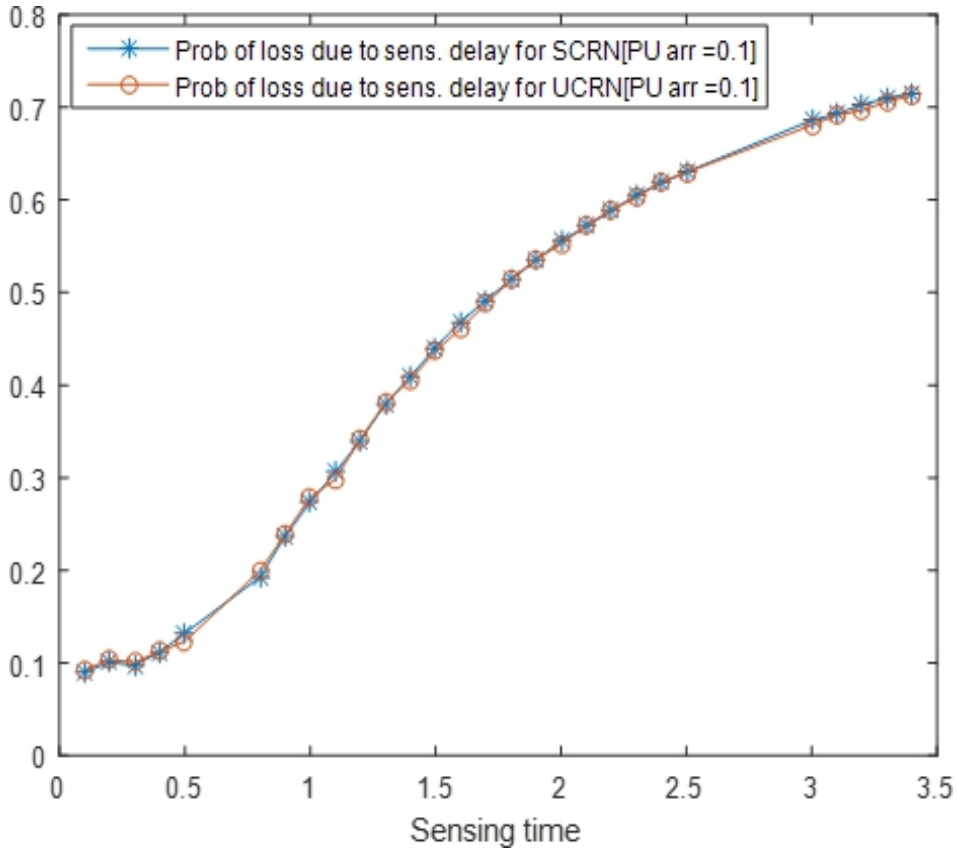

Figure 5.13: Prob. of loss due to sensing delay for the SCRN and UCRN

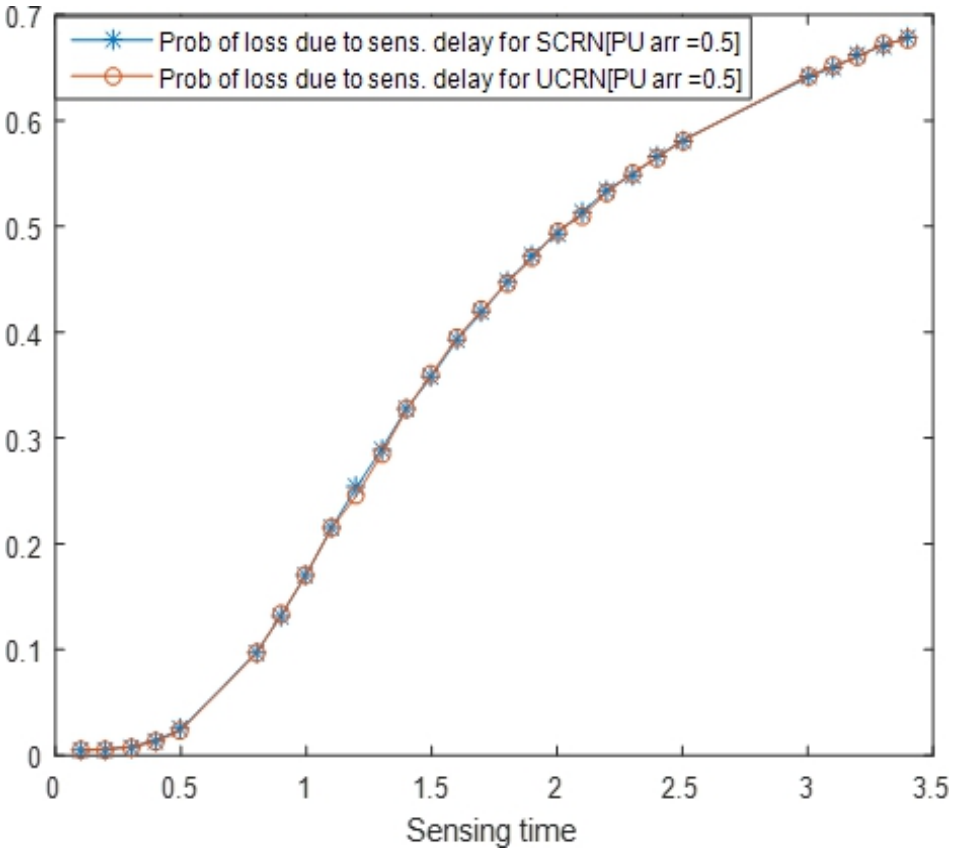

Figure 5.14: Prob. of loss due to sensing delay for the SCRN and UCRN

The total number of packet loss due to sensing and encryption delay are as shown in Fig.5.15-5.17. The improvement in the performance of SCRN and UCRN can be assessed by comparing the total packet loss in the SCRN to the packet loss in UCRN. This is demonstrated in Figs. 5.15-5.17. From the Figs, it is common to note that there is significant decline in packet loss in a SCRN in comparison with UCRN just as there is an increase in throughput. This increment and significant drop in packet loss are due to the introduction of complementary resources whenever there is surge in service demand.

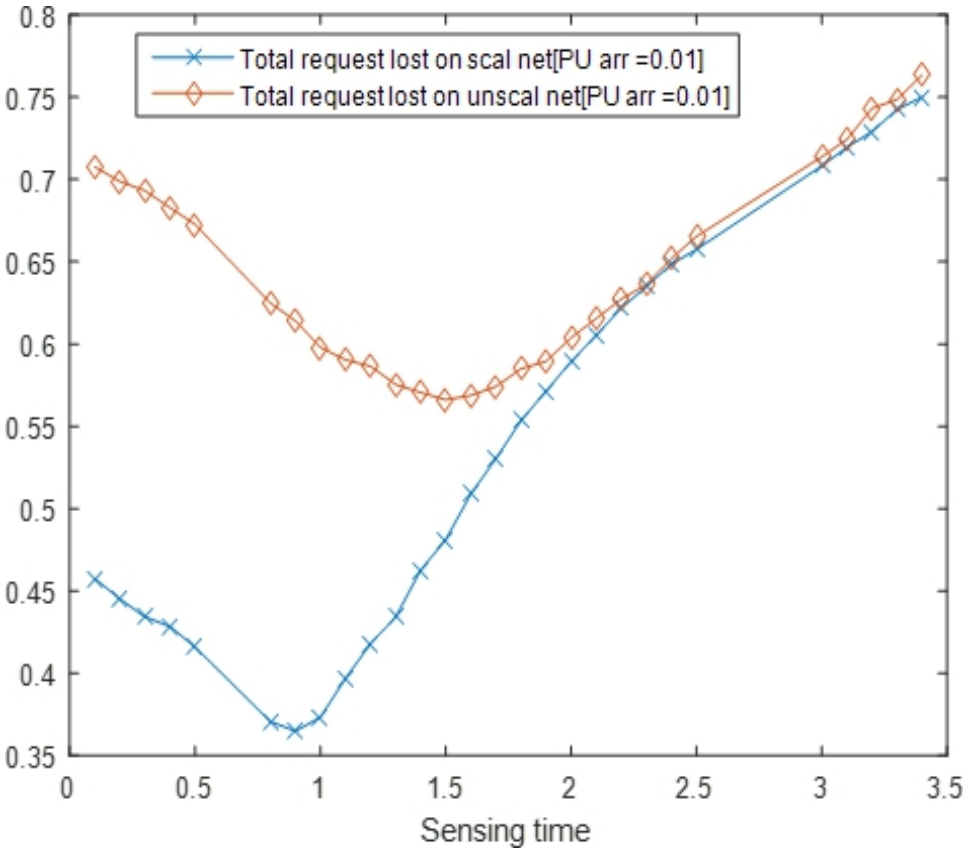

Figure 5.15: The total number of packet loss due to sensing and encryption delay for SCRN and UCRN

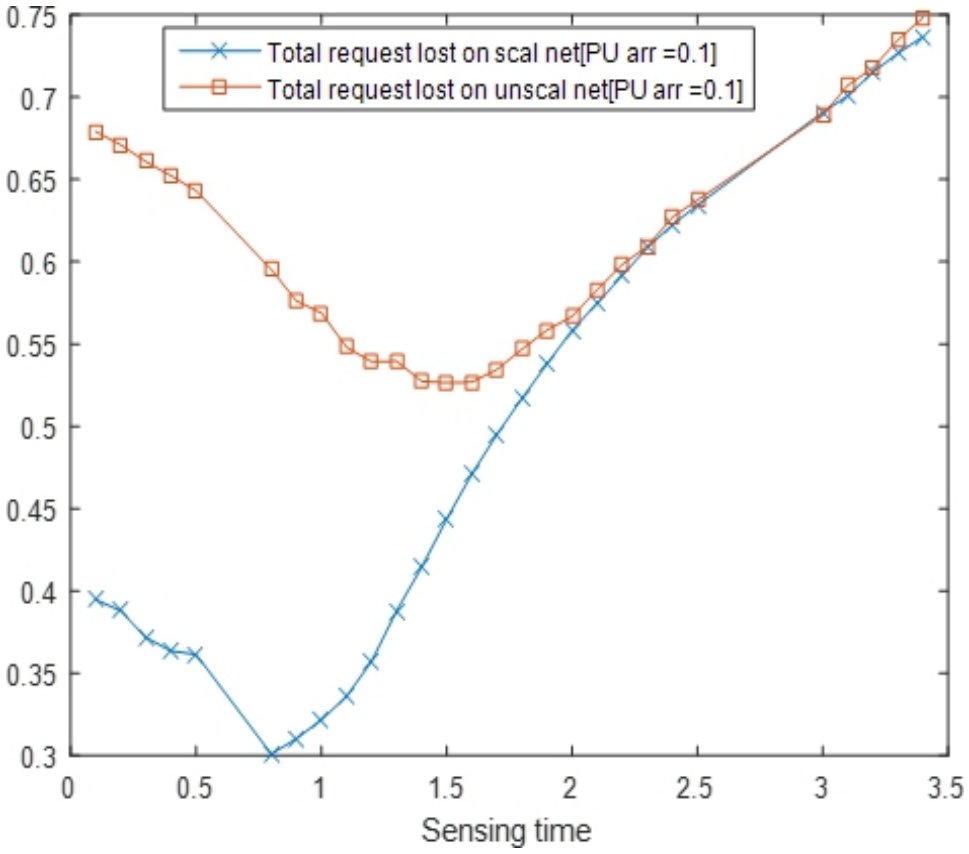

Figure 5.16: The total number of packet loss due to sensing and encryption delay for SCRN and UCRN

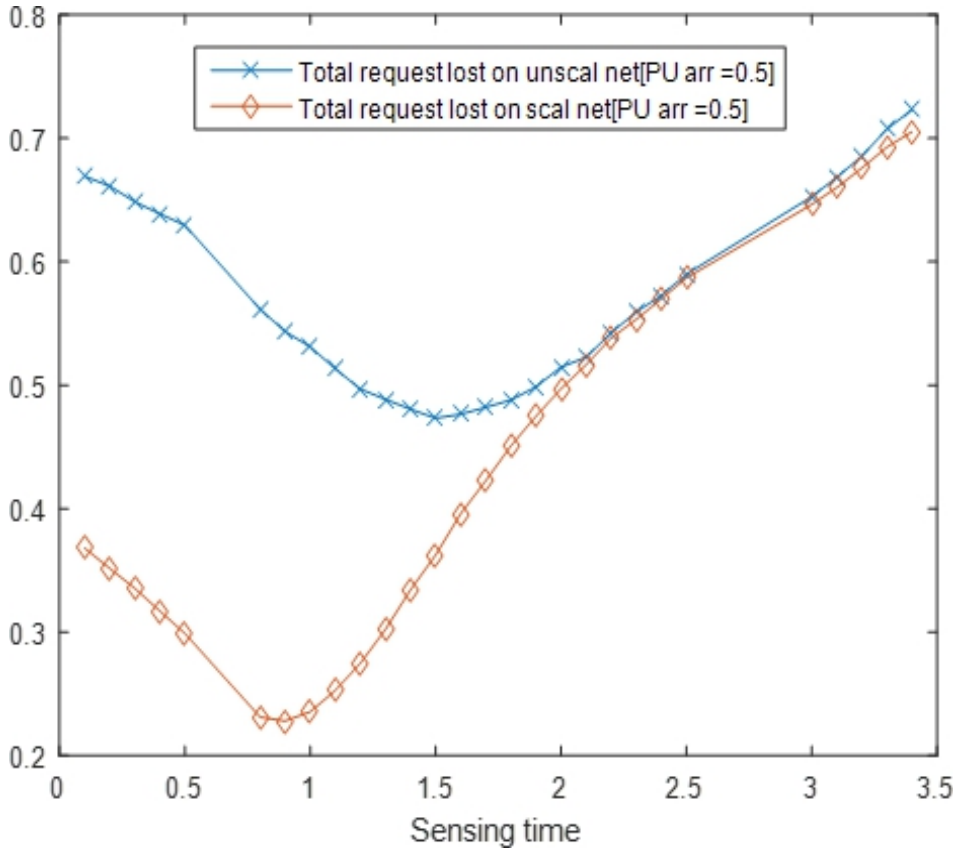

Figure 5.17: The total number of packet loss due to sensing and encryption delay for SCRN and UCRN

If the band is mostly unavailable due to PU activities as illustrated in equation (5.4)-(5.10),or false alarm detection as highlighted in equation (5.11), it may lead to build-up of SU requests in the queue.On this note, when an idle band is detected, SU with the aid of CRN transmits and continue to transmit on the band until PU reappears during which SU vacates the channel. If the number of requests in the queue increases more than a certain threshold, then additional resource would be introduced in order to swiftly encrypt and transmit the requests before the reappearance of PU. A predetermined queue length in this case is required as threshold to decide when the additional resources is required. In this work, maximum of 5 requests in the queue is needed for additional resources to be introduced. The maximum of 5 requests in queue in this case is used in order to swiftly transfer service to a new channel to aid encryption and consequently transmission of more requests and improve the throughput before the reappearance of PU. This leads to increase in throughput of SCRN than a UCRN

which is static in handling the surge in service demand as demonstrated in Fig.5.7.

The result obtained in Fig.5.7. shows that without scalability the maximum throughput of the SU is 5.97 while with scalability the throughput rose to 6.68 on PU arrival rate of 0.5. This work also intends to determine when SU transmission is interfering with PU signal. This is done by quantifying the throughput achieved when SU is interfering with PU signal. This throughput is assumed corrupted since the messages arrives out of order given a packet switching scenario. It is interesting to note that highest throughput of SU occur at the highest rate of the PU activity (0.5) on the band. Similarly, the lowest throughput of SU was obtained at the PU arrival rate of 0.01. This is true for both SCRN and UCRN. The throughput of UCRN is as shown in Fig. 5.18 Fig. 5.12.

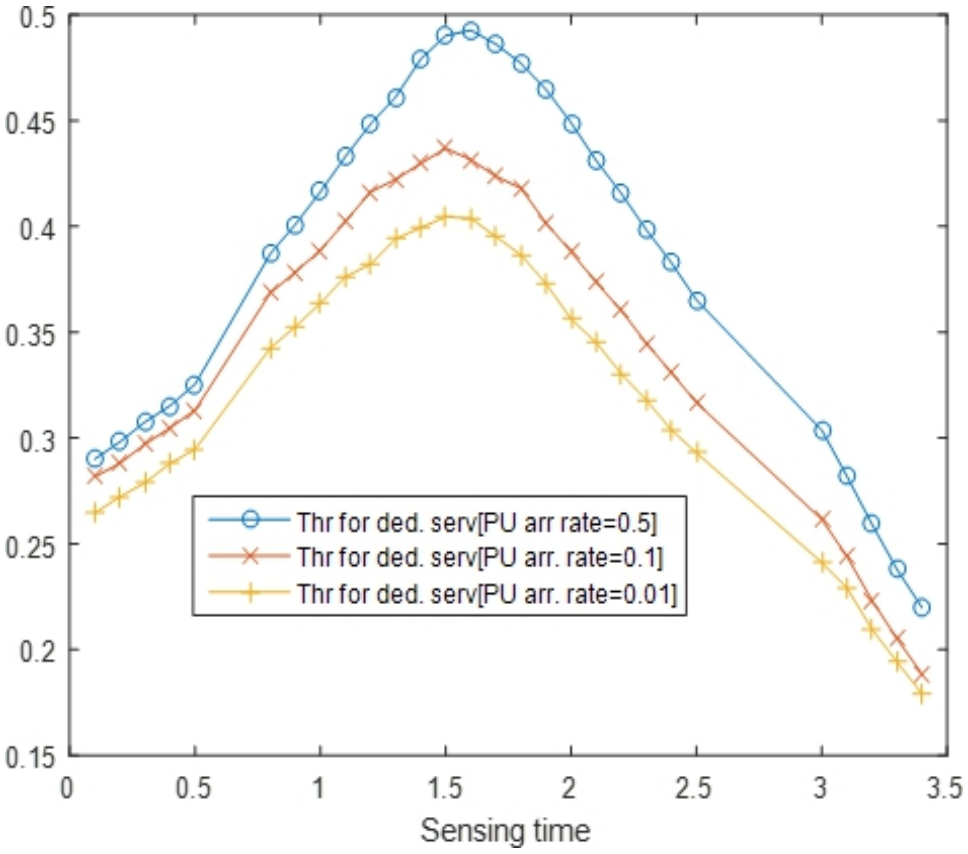

Figure 5.18: SU throughput for unscalable network.

In this context, the peak of SU throughput occur when the rate of the arrival of PU in the band is highest. An analysis revealed that the increase in throughput is due to interference resulting from miss detection given the same PU departure rate (0.01). This is because, assuming the same departure rate of PU, increase in PU arrival and CRN sensing rate, the probability of SU interference with PU signal is expected to be high. In order words, the probability of SU simultaneously transmitting with PU is raised, leading to improvement in overall throughput. The throughput of SU when interfering with PU signal can be obtained by comparing the observed throughput during the period of high interference rate when the PU arrival rate is 0.5 with the throughput obtained during the period of two different low interference with PU arrival rate of 0.1 and 0.01 respectively. This is as demonstrated in the Fig. 5.13 5.19 and 5.20 5.14.

The difference gives the total number of SU requests transmitted when SU is simultaneously

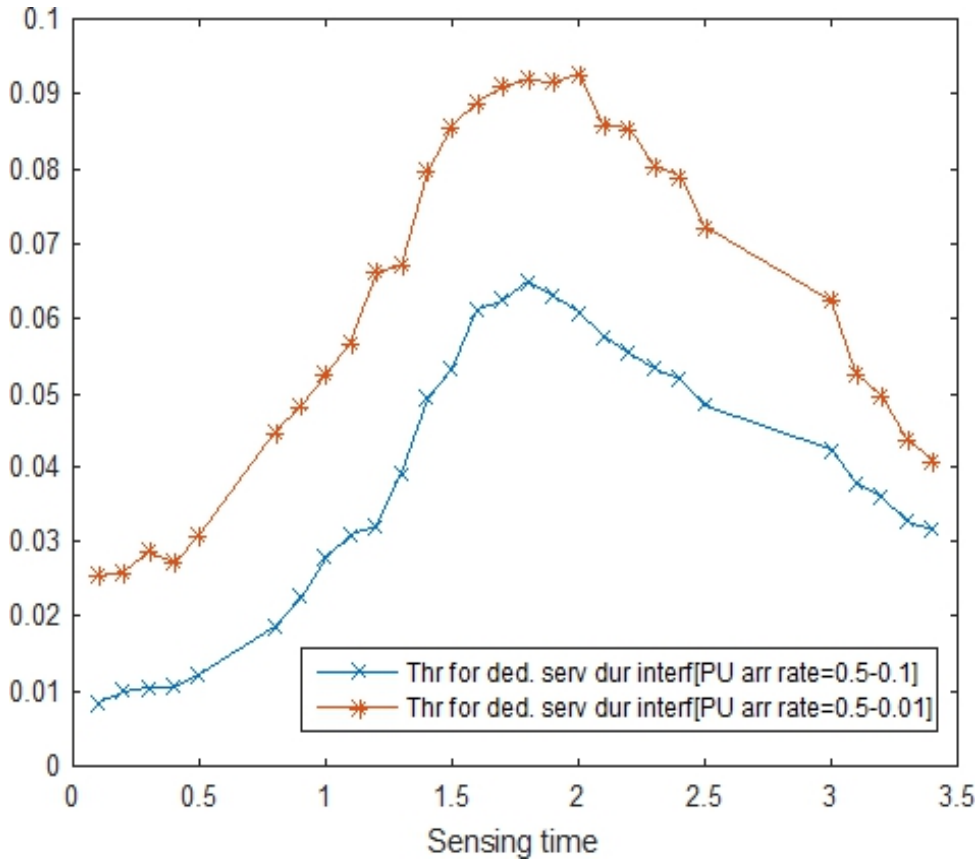

Figure 5.19: SU Throughput via dedicated server during interference

transmitting with PU. Therefore, the interference level can be detected by measuring the total throughput of SU at instant time and comparing it with an SU throughput measurement with reduced or no case of interference. For instance, if the throughput of SU when the band is idle is x, then x is used as a threshold to determine the interference level. SU throughput greater than x in this case is an indication of interference.

The experiment was also carried out to determine the trade-off between sensing, security and performance in a SCRN. It is aimed at predicting the sensing time at which the combined metrics of sensing, security and performance is optimum in a SCRN. This is is a straightforward addition of the metrics for sensing, security and performance. These metrics are probability of successful detection of an idle band, the probability of the network in a secured state, and the throughput of the secondary transmitter respectively. In this case, the probability of detection is the sensing parameter, probability of network in a secured

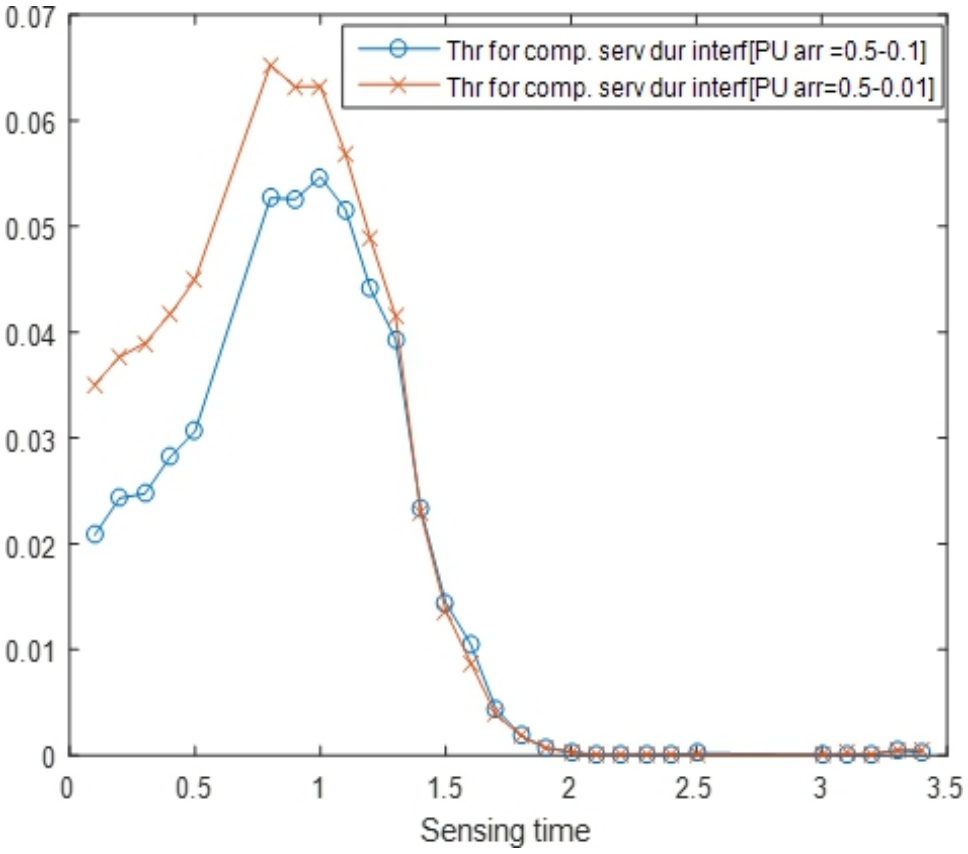

Figure 5.20: Throughput of SU via complementary server during interference

state is a security parameter and throughput measures performance. The addition of these parameter gives an optimum value for each of the measuring parameters. It is expressed as:

CSSPM=P{det}+P{sec}+throughput

where CSSPM is the combined sensing, security and performance measure in the context of SCRN

P{det} is the probability of detection

An idle space is assumed to be detected when SUs can successfully transmit on it. In this case, the number of successful SU transmissions can be a means to determine the probability of detection. Fig. 5.21 demonstrates the optimum value for CSSPM.

Similarly, the minimum value for the CSSPM is also considered. In this case, the sensing parameter is probability of false alarm, the security is measured by probability of the network

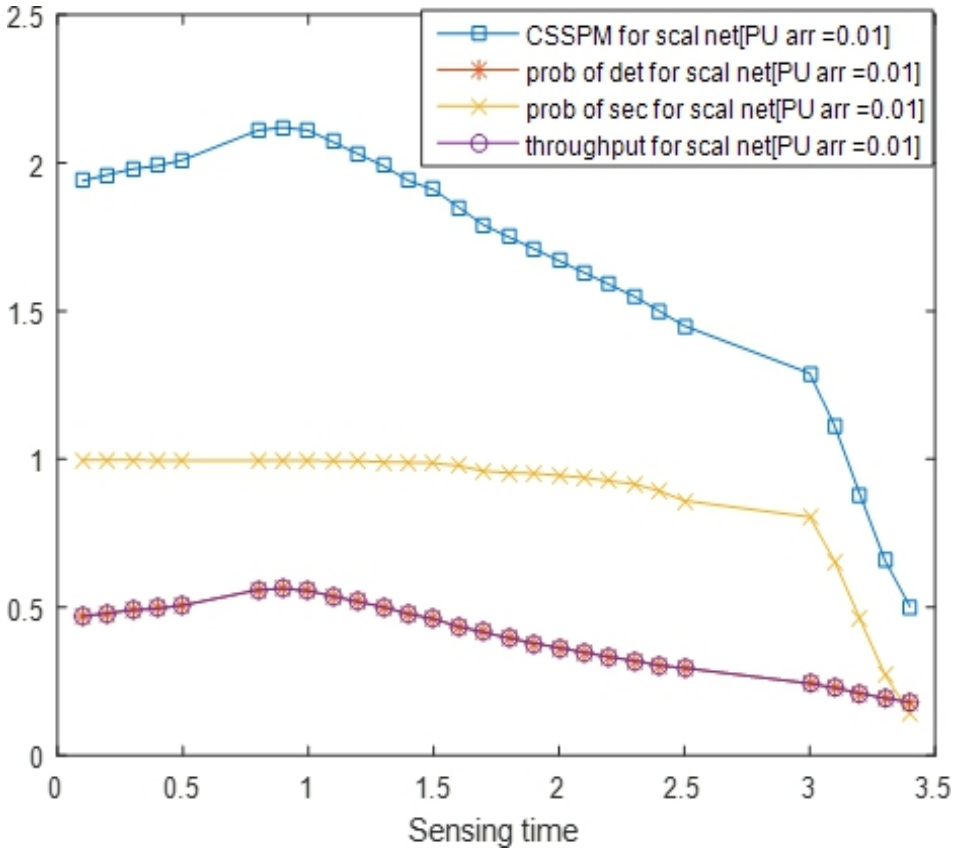

Figure 5.21: Max [Combined sensing, security and performance metrics]

in insecure state and probability of loss is performance parameter.

In the probability of loss, a finite capacity queue was considered. To determine the the total packet loss, the loss due to delays in the sensing and encryption process are added in order to obtain the total loss needed for the experiment. This is expressed as shown below.

TL= LSD + LED

where TL is the total packet lost

LSD is the loss due to sensing delay

LED is loss due to encryption delay

Therefore, the minimum value for the CSSPM is expressed as CSSPM{min}= P{FA}+P{TL}+P{insecure}

Fig. 5.22 shows the minimum point for the CSSPM. As demonstrated in the next figure, the minimum and maximum values occur at the same sensing time, giving credence to the

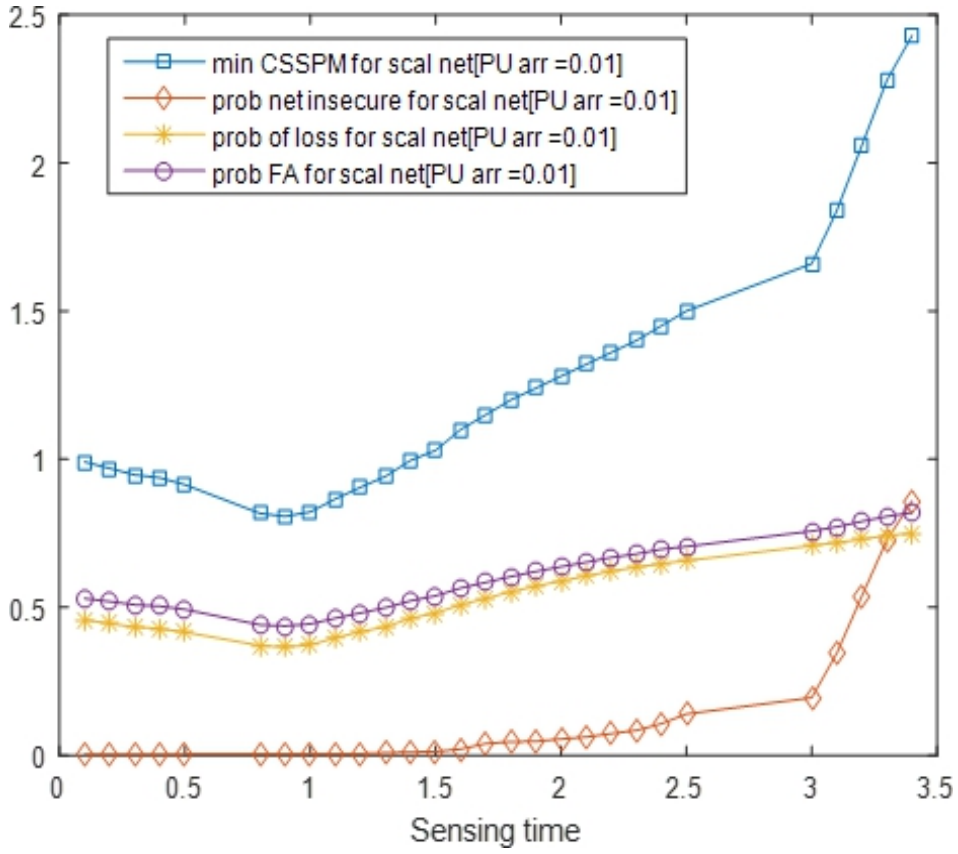

Figure 5.22: Min [Combined sensing, security and performance metrics]

experiment.

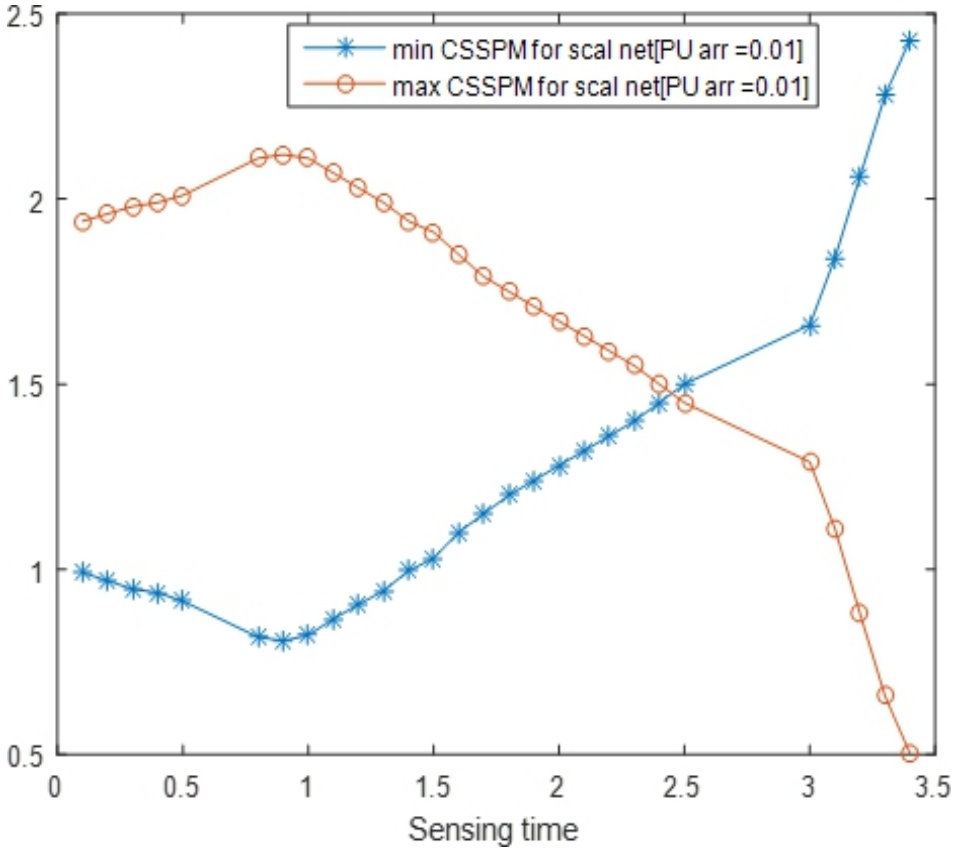

Figure 5.23: Min & Max [Combined sensing, security and performance metrics]

5.13 Summary

CRN with scalable feature of cloud computing in conjunction with encryption and security control mechanism has been proposed. An experiment was carried out 'with' and 'without' scalability to determine the impact on the performance of CRN. The result of the investigation shows that the proposed CRN can sustain good performance upon sudden surge in service demand. The experiment also reveals that scalable system attains its optimum throughput at shorter sensing time which is good for battery saving.

In the following chapter, the proposed investigation was carried out to predict a network under DoS attack and one experiencing congestion. This is necessary in order to ensure that repair is not initiated when not required.

Chapter 6

Detection of Network Congestion and Denial of Service (DoS) Attacks in Cognitive Radio Networks

6.1 Introduction

The scarcity of spectrum has necessitated the need for the introduction of CRN. As stated in the previous chapter, about ***75%*** of licensed spectrum are unused for significant period of time (c.f., [11]-[16]). As stated earlier FCC allows SUs to access the licensed spectrum with the aid of CRN. This implies that SU relies on the information from CRN before transmitting. Due to its wireless nature, a CRN is very vulnerable to attacks as a result of its adopted open policies and programming interfaces that expose the configuration options of a controlling entity such as service providers deploying CR (c.f., Bhattacharjee et al. [30] and Attar et al. [28]). The open access policy is because a portion of the radio spectrum is reserved as license-free bands such as in industrial, scientific and medical (ISM) bands [85]. The controlling entity can frequently change the operating parameters, for instance, the access policies, operating band, transmission band and modulation. As a result, the configurability features are vulnerable to manipulation (c.f., Clancy and Goergen [86]). Consequently, attackers could seize this opportunity to introduce an attack such as preventing the SUs from receiving signal from CRN in the form of Denial of Service (DoS) attack or eavesdrop on the packet on transmission. In order to secure the network from eavesdroppers (c.f., [87]) or attacks that modify the content of requests, (c.f., Wolter and Reinecke [10]) suggested encryption processing in conjunction with intrusion detection mechanism to mitigate the

attacks. Similarly, (c.f., Xu et al.[89] and Pelechrinis et al. [9]) proposed PDR to detect the presence of DoS or jammers. Though the above studies referred to congestion and the adverse effects on the performance of the network as jamming attack, nevertheless, this has not been applied in the context of CRN.

In this chapter, PDR is applied in CRN with experimental evidence to detect jamming attack and differentiate it from network experiencing congestion. The study also measures the PDR and depending on the result threshold, infer if the network is i) working normally ii) under jamming attack and iii) experiencing congestion. Moreover, a new congestion control mechanism is proposed that throttles SUs requests in the presence of any perceived congestion. It also shields the network from attacks that eavesdrop on the content of the request and at same time protects it from attacks that jam the network.

This chapter focuses on the detection of a jammer in CRNs and clearly distinguish it from network congestion. This is challenging due to the management of priorities and pre-emptions since the presence of PUs introduce ambiguity in the determination of the presence of jammer with regards to network congestion.

6.2 Study Overview

A CRN is based on a technology that enables SUs to access available licensed spectrum not occupied by PUs. As stated in previous section, a CRN is vulnerable to fraudulent attacks, which might attempt to eavesdrop or modify the contents of packets being transmitted. Moreover, denying SUs the opportunity to use a free band leads to underutilization of the spectrum space. In this case, it is important as well as challenging to differentiate between networks under DoS attack from network experiencing congestion. This work adopts the SUs performance measures of packet loss probability, mean queue length and normalised throughput of the transmission node in order to devise a PDR for SUs aiming to determine whether or not the network is experiencing a DoS attack. PDR in this case is the ratio of the number of packets successfully forwarded from the encryption node to the SU transmitter. To this end, SAN is proposed in order to investigate if the network is under a DoS attack and suggest a preventive strategy for an efficient network protection. Based on the application of

the Mobius Petri Net Package, typical numerical simulation experiments are carried out and related operational interpretations are made.

6.3 Cognitive Radio Networks (CRN)

This technology is required to allow SUs to use licensed spectrum. It senses the channel and only allow SU to transmit if an idle band is identified in an interweave spectrum access arrangement (c.f., Mehr et al.[90]). In other words, CRN is a link between the SU and primary base station. For efficient spectrum utilization, CRN is required to sense the band with high accuracy and to dynamically select the best band for the transmission of SU requests. It is assumed in this work that each CRN is assigned a frame. Frame is a period assigned to CRN during which it senses, carry out encryption process and then transmit SU requests. The transmission rate of a frame is equal to the frame rate multiplied by the number of bits in a slot (c.f., [91]). It is as demonstrated in Fig.4.3.

It senses for some time and backs off if no spectrum is detected. The average sensing time for best performance and security is determined as illustrated in (c.f., Ejike and Kouvatsos [88]). However, after sensing and detection of idle spectrum band, the malicious node could hinder the SU from receiving the signal from the CRN (c.f., Kurose and Ross [91]). In this context, an SU intending to transmit may assume the spectrum to be occupied and would not transmit, leading to a drop in throughput. It is common to expect the probability of loss to decrease, because SU will perceive the band busy and would not send its request for transmission leading to unused spectrum opportunities and consequently, drop in the probability of loss for network under DoS attack. This is in contrast to a network experiencing congestion in which the queue length and probability of loss at the encryption node are expected to be high.

6.4 Review of Related Works

Security is an important aspect of the design of the CRN. Several works in literature have highlighted the need for secured communication among SUs. These works independently

either studied detection of jamming attack or detection of intrusion in conventional wireless network but not both simultaneously. (c.f, Xu et al. [89]) proposed different jamming attack models that adversaries can rely on to disable the operations of wireless networks and also evaluate the effectiveness in terms of how each method affects the ability of the wireless node to send or receive packets. It also discussed measures that are basics for detecting jamming attacks.

An investigation was carried out in (c.f., Wolter and Reineke[10]) to determine the ideal encryption key length for optimum security and performance of a network. The study was not linked to a particular system. In the model, there is an intrusion detection mechanism aimed at detecting an intrusion as shown in Fig.6.1. The model only considered the detection of an attack that eavesdrop or modify the content of requests. It did not, however, consider an attack that can block the SUs from receiving the information it requires to enable it transmit or not. The paper employed encryption and intrusion detection control mechanism to mitigate this attack. It measured the trade-off between security and performance and predicted an encryption time at which the network has optimum performance.

A research was carried out in (c.f., Kulkarni et al.[92]) to study the secured communication between communicating entities. The paper presents protocol that maintain O($\sqrt{n}$) secrets per user where n is the number of users in a system. Similarly, this research is particularly for preventing insider attacks such as eavesdroppers that may have privileges and could use the privileges to eavesdrop or modify the content of requests being transmitted. It did not consider attack such as jamming that could cause interference to PU or deny SUs the access opportunity to the channel in the form of false alarm.

An analysis was carried out in (c.f., Syed et al.[93]) to study the use of jammer in preventing the spectrum sensing and obstructing communication between CRNs. In this model, an attacker stops the CRN from receiving information it requires to function properly. For instance, an attacker could block CRN running through a certain frequency from receiving information about the true status of the channel, resulting in severe interference to PU. The paper only considered DoS attacks or attacks that obstruct SU from receiving information it requires to transmit its request. However, it did not consider attacks that could eavesdrop or modify the content of requests being transmitted.

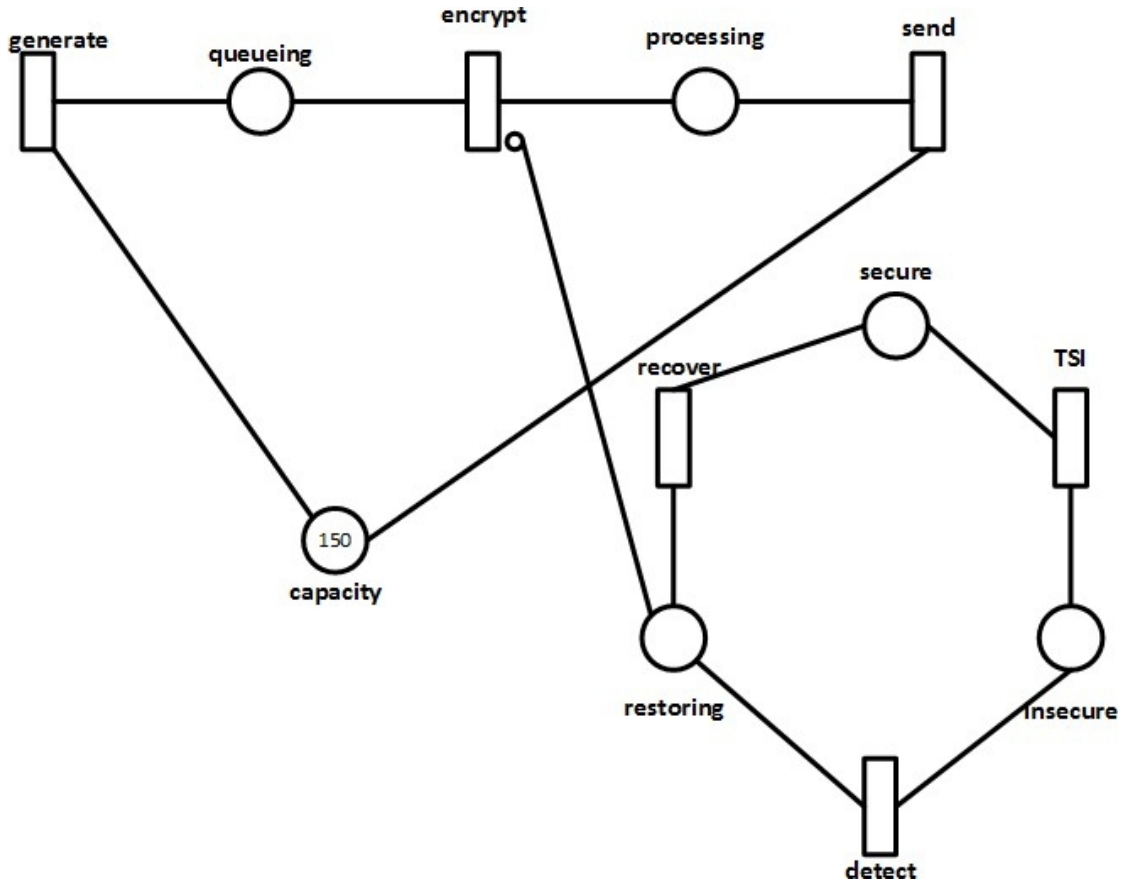

Figure 6.1: Petri net model for combined performance and security analysis (c.f., Wolter and Reinecke [10])

In (c.f., Cho et al.[94]), the performance characteristics of secure group communication system (GCS) in mobile ad hoc networks that employ intrusion detection control mechanism in dealing with insider attacks in conjunction with rekeying technique for outsider attacks was investigated. The paper only considered attacks that have privileges and could use these privileges to eavesdrop or modify the content of requests on transmission. Though the paper investigates this attack, however,the implementation of this design is different in CRN since CRN involves multiple classes. In this context, it suffice to assume that implementation in GCS has no need to manage pre-emption that may arise due to priorities as it is obtainable in CRN between SUs and PUs. This priority and pre-emption are the core features of CRN. This work is intended towards detecting the presence of jammer in CRN and also distinguishing it from network congestion. This is somewhat challenging since the presence of PU

introduces ambiguity in determining the presence of jammer as against network congestion in CRN. It involve managing pre-emption as required in CRN.

6.5 Problem Statement

In this work, it is assumed that CRN senses the channel non-cooperatively (c.f.,Ngomane et al.[95]) and only allows SU to transmit if an idle band is detected which depends on the frequency of the sensing. SU sends transmission request to CRN if it has packets to transmit. This activates the CRN sensor and depending on the perceived status of the band, CRN responds with either 'Clear to Send (CTS)' or 'Not Clear to Send (NCTS)' signals. However, attackers aiming to jam the signal could intercept this request bit and falsify it (c.f., Bhattacharjee et al.[30]) to suit its harmful objective (c.f., Bhattacharjee et al. [30] and Pathan et al.[96]). For instance, attackers could change the CTS bit transmitted by CRN to NCTS. In this case, the SUs may differ its transmission and the idle time of the band is wasted (Yang et al.[97] and Thamilarrasu et al. [98]) . The attackers could also aim to cause SUs transmission to interfere with PUs signal by changing the NCTS response of CRN to CTS resulting in SUs transmitting when there is an ongoing PU transmission causing regulatory violations (c.f., Bhattacharjee et al.[30] and Attar et al. [28]. This is as illustrated in Fig.6.2

The major challenge (c.f., Chelli [99]) is to differentiate between the NCTS signal received by SU when the channel is truly occupied by PU from the signal sent by an attacker when the network is under DoS attack. The CRN senses the spectrum and if the band is occupied, it sends NCTS signal to SUs. Similarly, if the CRN senses the channel and found an idle band, it sends CTS signal to SU, however, malicious node may intercept this response and swiftly modify it to NCTS thereby denying SU the opportunity to use the channel. Due to the similarities between network under DoS attack and network experiencing congestion, a DoS attack could wrongly be taken as a network congestion and vice versa. This situation may possibly lead to initiating repairs where and when not needed. Likewise, a network under attack could also be wrongly assumed to be experiencing congestion. Continuing to assume a network under attack is experiencing congestion could lead to waste of band resources.

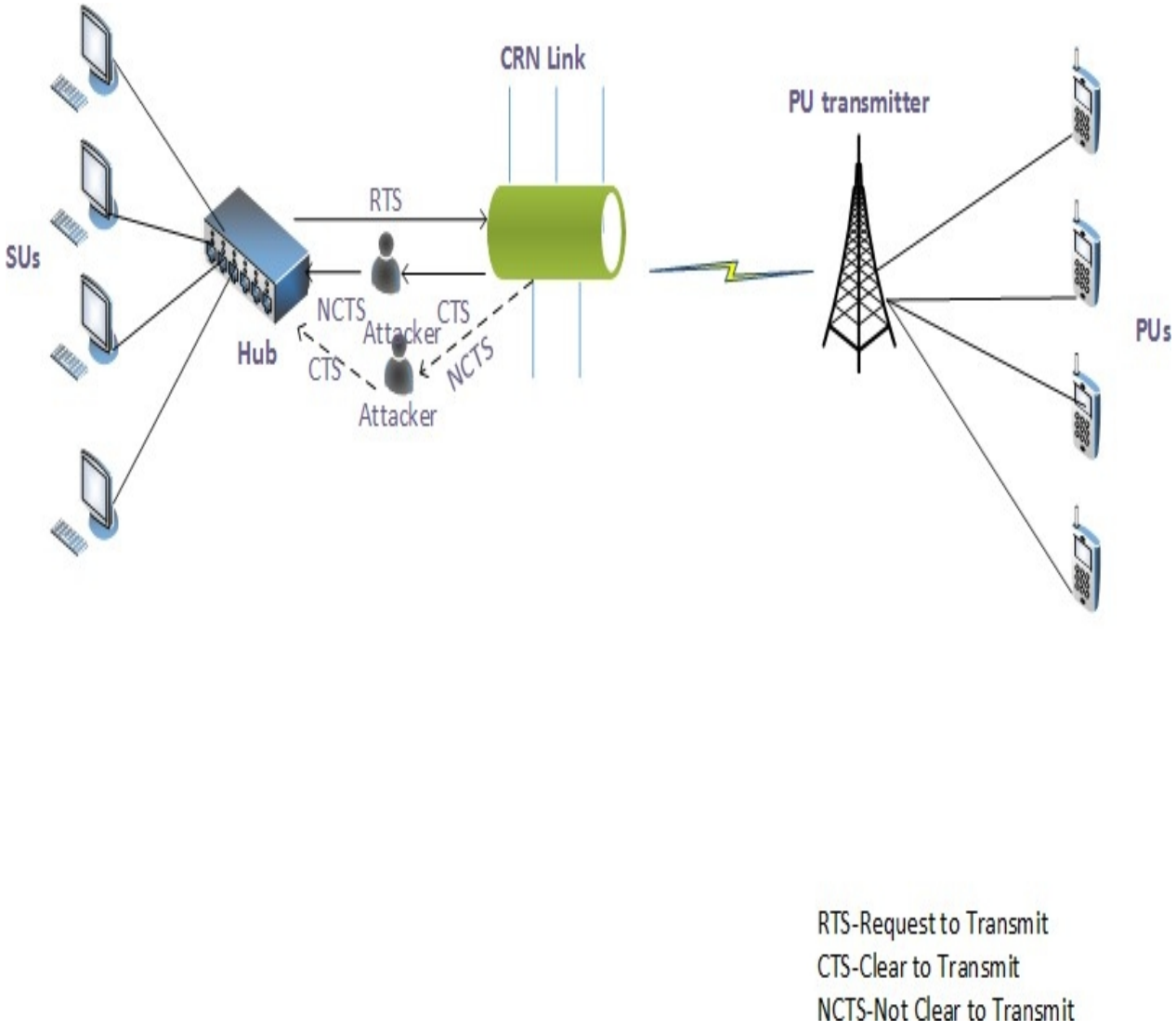

Figure 6.2: Mode of attack to CRN

This work is therefore based on the need to resolve the conflict in initiating a repair when not needed resulting from a wrong assumption that a network experiencing congestion is under attack and waste of band resources resulting from assumption that a network under attack is experiencing congestion.

Cryptography especially AES with long key length can be used to secure and ensure these attacks do not occur, however, it decreases the throughput. In some networks that requires extremes with respect to security, AES with longest key length could be applied with little or no consideration to the impact on the performance ([10]). However, in network under study,

it is assumed that performance is as important as security. In this context, a trade-off is required. Since the network is not fully secured due to trade-off, it is reasonable to guild the network against possible security breach. This necessitates the need to introduce measures to distinguish network congestion from attack.This is required in order to initiate repairs only when the network is under DoS attack and not when it is experiencing congestion as a result of the activities of PU.

6.5.1 Congested Network and Network Under Attack

To successfully distinguish between a network under attack from one experiencing congestion, some metrics are required to capture the behaviour of the model. Specifically, the Packet Send Ratio (PSR) and the PDR proposed in (c.f., Pelechrinis [9]) are the ratios of successful encryption and the ratio of successful transmissions respectively.

Packet Send Ratio (PSR): This is the ratio of the number of requests successfully received by SU encryption node for encryption to the total number of requests intended to be encrypted (c.f., Pelechrinis [9]).This is the throughput of the encryption node. It follows binomial distribution since it can be either successful or unsuccessful. It may be unsuccessful due to congestion resulting from PU activities or DoS attack. This is represented as shown in equation (6.1). For instance, if users have $\boldsymbol{m}$ packets to encrypt and only $\mathbf{n}$ $\boldsymbol{(n \leq m)}$ of the packets are successfully encrypted due to congestion or jamming attack then

$$P(X = n) = \binom{m}{n} * p^n(1 - p)^{m-n} = \frac{m!}{m!(m-n)!} * p^n(1-p)^{m-n} \tag{6.1}$$

where X is the random variable for n independent trials. Thus,

$$PSR = \frac{m!}{m!(m-n)!} . p^n(1\_p)^{m-n} \tag{6.2}$$

where $\boldsymbol{n}$ is the number of successful packet sent

$\boldsymbol{m}$ is the total number of attempts

$\boldsymbol{p}$ is the probability of success

Packet Delivery Ratio (PDR): Similar to PSR, this is the number of requests successfully

forwarded from the encryption node to the SU transmitter. In practice, it could be interpreted as the throughput of the transmitter at a given time. For example, if the encryption node encrypts and eventually forwards $\boldsymbol{n}$ of these requests to the SU transmitter but only $\boldsymbol{q}$ $\boldsymbol{(q \leq n)}$ of the requests are successfully transmitted then the PDR is expressed as (c.f., Pelechrinis [9])

$$PDR = \frac{q!}{n!(n-q)!} \cdot p^q(1\_p)^{n-q} \tag{6.3}$$

where $\boldsymbol{n}$ in this case is the number of trials.

$\boldsymbol{q}$ is the number of success

$\boldsymbol{p}$ is the probability of success

In this work, battery failure is considered an attack since draining the battery power is one of the strategies adopted by an attacker to introduce DoS attack. An attacker can exhaust the CRN resources by continually sending Request to Transmit (RTS) signal to elicit CTS from the targeted CRN. This could drain the power of the battery since it does not depend on external power source (Raymond and Midkiff[100]).

Throughput in this case is used to predict if the network is experiencing congestion or under DoS attack. This is by consideration of two factors that affects the throughput of SUs when the channel is idle: false alarm in the form of an attack and false alarm resulting from prolonged sensing. The throughput is monitored for each frame time and considered under the following cases.

Case A1: The throughput obtained when the band is idle given that there is no false alarm due to prolonged sensing time and the throughput when the band is idle given that there is no false alarm resulting from attack within the sensing time.The average throughput as shown in (c.f., Liang et al. [11] and Bhowmick et al. [67]) to be determined by:

$$V_0 = (P(H_0)(1 - P_f a_s)th_0 + P(H_0)(1 - P_f a_a)th_0)(\tau)) \tag{6.4}$$

where Vo is the average throughput for the system within the sensing time.

(P_f a_s) probability of false alarm due to sensing delay

(P_f a_a) probability of false alarm due to an attack.

th_0 denote the throughput when the band is idle and correctly detected to be idle

$P(H_0)$ is the probability that the band is idle

$(1 - P_f\, a_s)$ is the probability that there is no false alarm resulting from prolonged sensing.

$(1 - P_f\, a_a)$ is the probability that there is no false alarm resulting from attack.

Case A2: The throughput obtained while the band is idle and there is no false alarm resulting from prolonged sensing and due to an attack within the encryption time and can be expressed as (c.f., Liang et al. [11] and Bhowmick et al. [67]) :

$$V_1 = (P(H_0)(1 - P_f a_s)th_0 + P(H_0)(1 - P_f a_a)th_0)(E)) \tag{6.5}$$

where E is the encryption time

Case B1: The throughput that the band is idle but could not be detected due to prolonged sensing time or attack within the sensing time (c.f., Liang et al. [11] and Bhowmick et al. [67]).

$$V_2 = (P(H_0)(P_f a_s)th_1 + P(H_0)(P_f a_a)th_1)(\tau)) \tag{6.6}$$

where V2 is the average throughput for the system during the sensing time.

th_1 denote the throughput when the band is idle and correctly detected to be idle

$P(H_0)$ is the probability that the band is idle

$(P_f\, a_s)$ is the probability that there is false alarm resulting from prolonged sensing.

$(P_f\, a_a)$ is the probability that there is false alarm resulting from attack.

Case B2: The throughput that the band is idle but could not be detected due to prolonged sensing time or attack within the encryption time can be expressed as(c.f., Liang et al. [11] and Bhowmick et al. [67])

$$V_3 = (P(H_0)(P_f a_s)th_1 + P(H_0)(P_f a_a)th_1)(E)) \tag{6.7}$$

The average throughput for the probability that the band is idle and correctly detected to be idle within sensing time is expressed as

$$g_0 = V_0(\tau) + V_1(E) \tag{6.8}$$

g_0 in this case is expected to be greater 0 as would be demonstrated in the simulation results and analysis. Similarly,

$$g_1 = V_2(\tau) + V_3(E) \tag{6.9}$$

In this context, g_1 is expected to be equal to 0 as was the case in (Xu et al.[89])
g_0 indicates that the network is experiencing congestion while g_1 shows the network is under DoS attack.

To overcome these attacks, this chapter proposes a DoS attack detection control model. This detection control is connected to SU arrival node. It monitors communications between SUs and sensing node. If SU has request to transmit, the request activates the sensing node. The sensing node probes through the band to detect the status. Specifically, the sensing node assesses the status of the place "PU trans" as demonstrated in Fig. 6.3. One token at the place "PU trans" implies that the channel is occupied by PU and SUs transmissions are not permitted. The network is considered free from DoS attacks with a token in a place "safe" until the transition "DoS attack" completes and a token is transferred to the place "detect". A token at the place "DoS attack" cease further generation of SU arrival in the form of DoS attack. In this case, the throughput, probability of loss and mean queue lengths are expected to be zero.

This chapter also provides the solution to network congestion by incorporating congestion control mechanism. The mechanism throttles the sending of SU requests. This implies that SUs reduces its sending when the number of token in the buffer is at a predetermined threshold. For instance, the SUs may continue to forward a number of requests, say 3 requests per slot to encryption node until a certain number of requests are in the buffer. In order to avoid loss and still maintain high throughput, the SU reduces its requests. In this case, SU may reduce the number of requests to 1. This is as demonstrated in Section 7 of this chapter. The experiment shows that there is an increase in throughput by transmitting more packets when the packets in buffer is below the set threshold. However, there is also an increase in packet loss if the sending is not controlled by the SUs. The trade-off between increase in throughput and decrease in packet loss will be considered in future work.

6.6 Proposed Network Model

This model represents DoS detection in conjunction with intrusion detection mechanism in CRN. This research continues from previous work (c.f., Ejike and Kouvatsos[88]), but unlike the previous model, it consists of two security models: DoS and intrusion detection security control models. There is also PU arrival and departure which is modelled as a cycling of tokens from place 'SU trans' to 'PU trans'. All the models are attached to SU performance model and have the common function of freezing the operation of SU whenever there is a token at the appropriate place.

In the DoS model, token at the place 'safe' indicates a secure and functioning network. SUs may continue to transmit if an idle band is detected until DoS attacker is able to launch a successful attack and consequently cease the network operation. Unlike the intrusion detection control model, the token moves from place 'safe' to 'detect' and back to 'safe'. This is because an attacker can promptly cease the transmission of SU request which can immediately be suspected to be an attack. This explains why the flow did not consider insecure state before restoration.

In the PU arrival and departure model, there are two tokens in the place 'SU trans'. The tokens at the place 'SU trans' implies that the band is being used by SUs since no PU is using it. Depending on the arrival rate of PU, the tokens could move from 'SU trans' to 'PU trans' indicating the PU arrival. This is as shown in the Fig.6.3. If PU arrives, it ceases the transmission of SU requests until it vacates the band.

The second token in the place 'SU trans' is used to capture the misdetection. At the beginning, there are two tokens in the place 'SU trans' indicating an idle band that could be used by SU without interfering with PU signal. The rate at which this token moves from 'SU trans' to 'PU trans' depends on the arrival rate of PU and also the data rate of the band.

The intrusion detection control freezes the network operation upon detection of attack. A token in the place 'Sec' implies a secure network. The transfer of the token from 'Sec' to place 'insecure' indicates an undetected attack. The transfer of the token from the place 'insecure' to 'restore' demonstrates that the attack has been detected and it is assumed that repair is initiated immediately and as a result, the network operation is stopped.

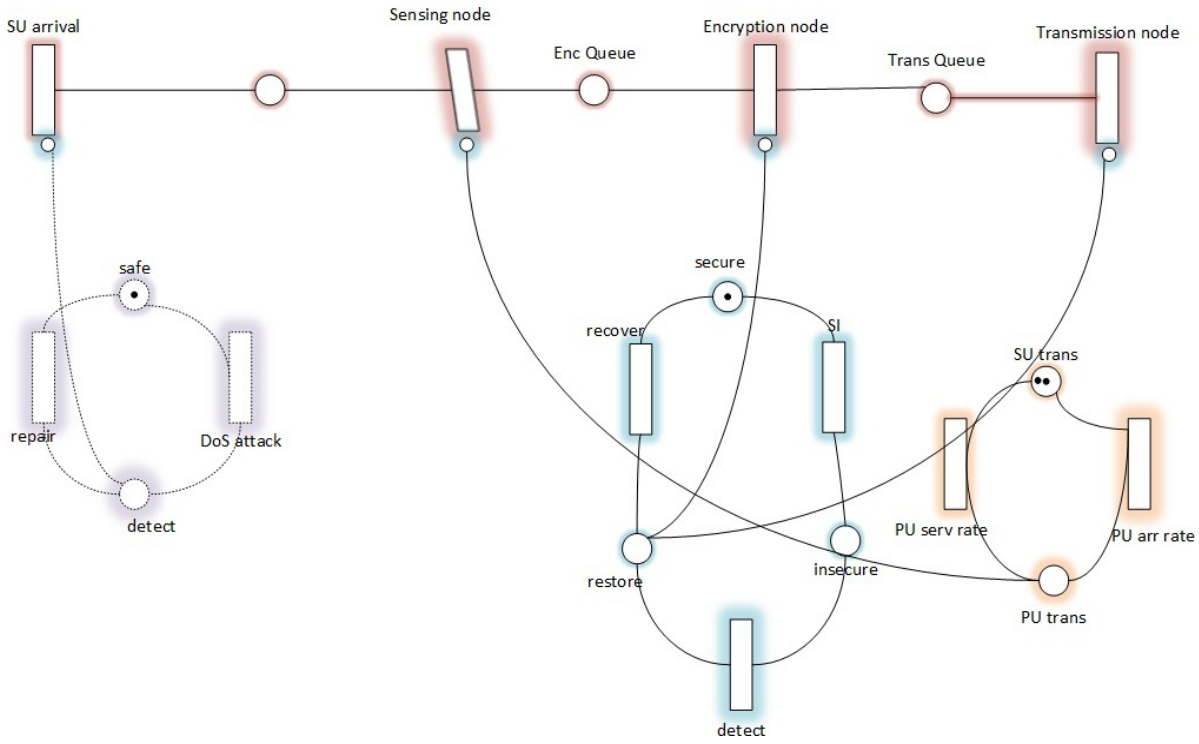

Figure 6.3: Proposed CRN Structure

6.7 Parameters and Simulations

As stated earlier, simulations are used to abstract the behaviour of a real system. In this context, it is necessary that the model is parameterized to represent the actual system under study. SAN formalisms is used to generate the required traffic to the proposed model. Mobius petri net package is the simulation tool that supports SAN model. The package has some features to demonstrate the behaviour of the proposed model. Transitions are used to generate the actions that changes the state of the system and are represented graphically as rectangular bars [62]. Places are used to store incoming request to the network. A token represents the actual request on transmission. A transition is enabled when the input place connected to transition contain at least a token. Enabling indicates execution process while firing corresponds to completion of the process. In the experiment, transitions with exponential firing delay distributions are chosen. Finite capacity queue is assumed. The table 6.1 shows the chosen input parameters.

	Ideal Cond (no att, no cong)	Cong (no att)	Att (no cong)
Attack rate	0.001	0.001	1.0
Recovery rate	1.0	1.0	0.001
Sensing rate	10	1.0	10
Encryption rate	10	10	10
Transmission rate	10	10	10
Request rate	1.0	1.0	1.0

Table 6.1: Input values

Table 6.1 shows that it would take 1000 milliseconds for an attacker to launch a successful attack when the network is on a normal working condition. The recovery rate in this case is 1.0 which demonstrates quick network recovery if there is an attack. Sensing rate of 10 as shown in Table 6.1 indicates that time between sensing is 0.1 milliseconds. This implies that hardly an idle band go undetected. Transmission and encryption rate of 10 were also used in order to ensure that they are not bottlenecks since the aim is to model a network without attack or congestion. This experiment is also carried out for network under attack and network experiencing congestion. As shown in the table, the arrival rate of SU is 1.0. The SU will continue to send its request at this rate for transmission until there is PU interruption or a security incident. Some incidents can interrupt the SU transmission. These are external attacks such as DoS that freezes the network operation when there is an attack and during repair as demonstrated in Fig.6.3 and internal attacks and restorations such as those that eavesdrop and modify the content of request on transmission. Finally, the detection of PU signal. Each of these events can disrupts the transmission of SU requests. However, network congestion may not disrupt continues transmission of SU requests but could delay it in the queue. In this chapter, the aim is to distinguish between the network experiencing a congestion and the one under DoS attack. In the next section, the results of the simulation is demonstrated with emphasis on how the network congestion improves the throughput and can reduce packet loss.

6.8 Results and Analysis

This analysis aim to investigate the behavioural difference between a CRN under DoS attack and one experiencing congestion so that appropriate measures can be adopted to control it. It is also demonstrated how DoS attack increases the probability of misdetection. This study was carried out for network under normal working condition, network experiencing congestion and network under DoS attack. The input values are as in Table 6.1. The result as shown in Fig. 6.4 demonstrates that the throughput for a network under ideal working condition is the highest with the throughput close to the input load.

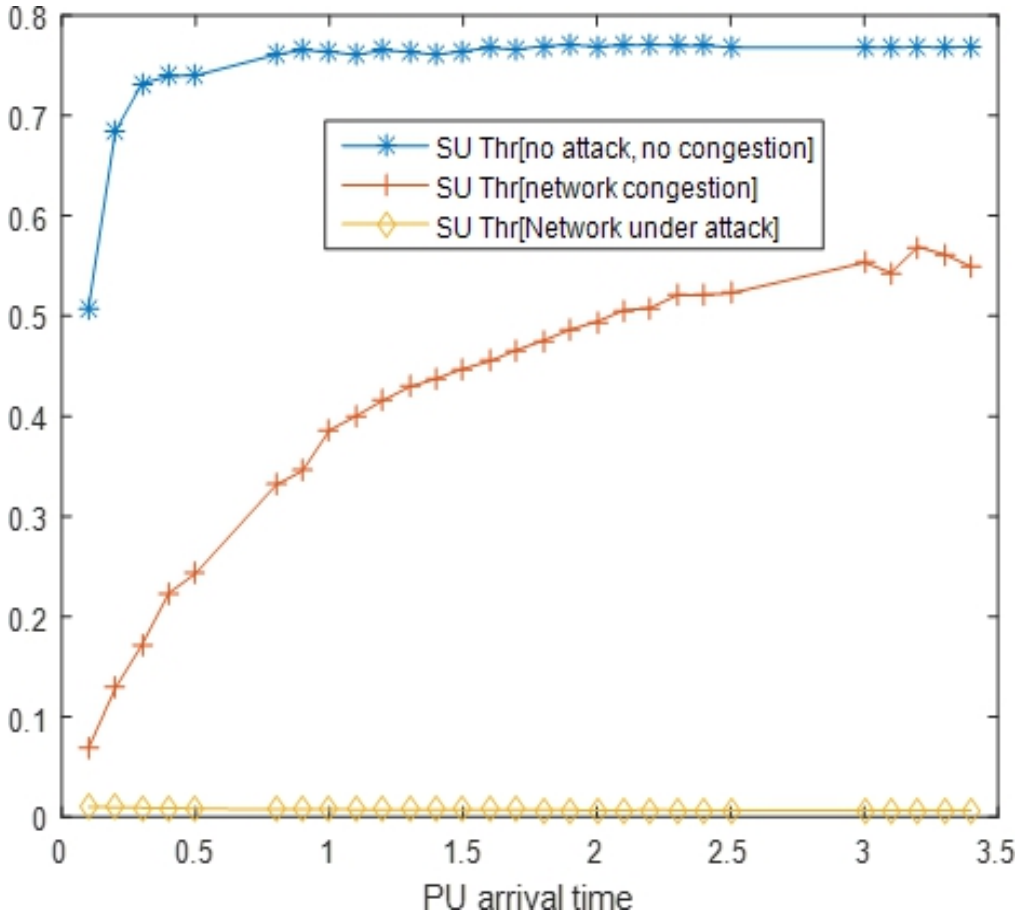

Figure 6.4: Throughput for network under different conditions

The network experiencing congestion has high throughput but far less than the input load. However, network under DoS attack has near to zero throughput. This is because, when the network is under ideal working condition, if the band is idle, the band is underutilized.

For instance, in the experiment, the applied SU load is 1Mbps but the band offer data rate of 10Mbps. This implies that the band is about 90% underutilized when it is idle. This is demonstrated in Fig.6.4 where the highest throughput attained is 0.77Mbps. Fig.6.4 also shows that due to congestion, the throughput of network experiencing congestion fall short of the transmitted load. For example, the maximum throughput attained when the network is experiencing congestion is 0.55Mbps though the same load was transmitted. The congestion maybe due to weak signal strength that the CRN sensor could not detect. The throughput for network under attack is ≈ 0. This is because, during attack, the attacker is assumed to have gained access and able to change the CTS response emanating from CRN to NCTS thereby denying the SUs the opportunity to use the spectrum. Since the attacker denies the SU the chances to use the band, the throughput decreases as shown in Fig.6.4. To validate the results, the probability of loss and average queue length were also considered.

Fig.6.5 similarly shows that network under ideal working condition has moderate queue length. The queue length is due to the use of the band by the incumbent. This queue length decreases as the incumbent inter-arrival times increases as shown in Fig.6.5. As expected, the queue length for network experiencing congestion is highest. This is due to infrequent sensing by the CRN as shown in the input data in Table 6.1. The table shows that though the band has data rate of 10Mbps, however, the sensor may not detect when the band is idle due to infrequent sensing. This leads to increase in the number of SUs request in the queue. For network under attack, since SUs do not receive CTS signal from CRN due to attack, it defer its transmission and no load is transmitted, leading to zero request in queue as demonstrated in Fig.6.5.

There is similar behaviour when the probability of loss is considered. The SU packet lost when the network is experiencing congestion is highest. For network under ideal working condition, some SU requests are lost when the PU inter-arrival time is small, e.g. 0.5 ms, but decreases as the inter arrival time increases since there is no other constraint such as congestion or attack affecting the transmission of its requests. However, similar to the previous explanation, attack changes the CTS response to NCTS thereby leading to SU being denied the opportunity to transmit. This causes packet loss as shown in Fig.6.6. Note that packet drop is only possible where there is a transmission.

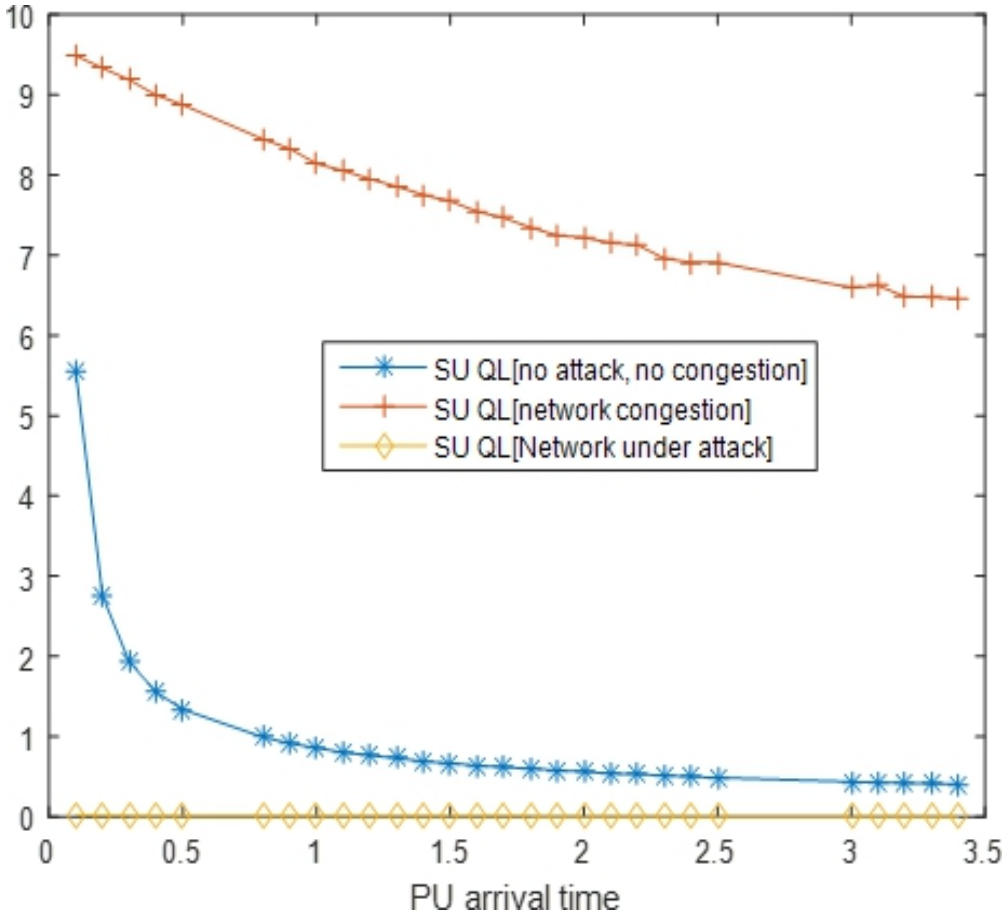

Figure 6.5: Queue length for network under different conditions

In addition to the above metrics, when a network is under attack, attackers could change the response from NCTS to CTS, eliciting transmissions from SU when the band is being occupied by PU. This results in SU interfering with the PU signal. One of the conditions listed by regulatory bodies before SUs are allowed to use licensed spectrum is that its signal must not interfere with PU signal (Bhagate and Patil [7]). Therefore any increase in the interference to SU signal is flagged as an attack. Fig.6.7 shows that when the inter-arrival time of PU decreases, then the probability of misdetection is expected to increase. This is because, with the service rate of 1.0, it will take much more service time to transmit PU request and if the network is under attack, the transmission could be affected by SU transmission. In contrast, if the service rate is 5.0, then it implies that it will take less service

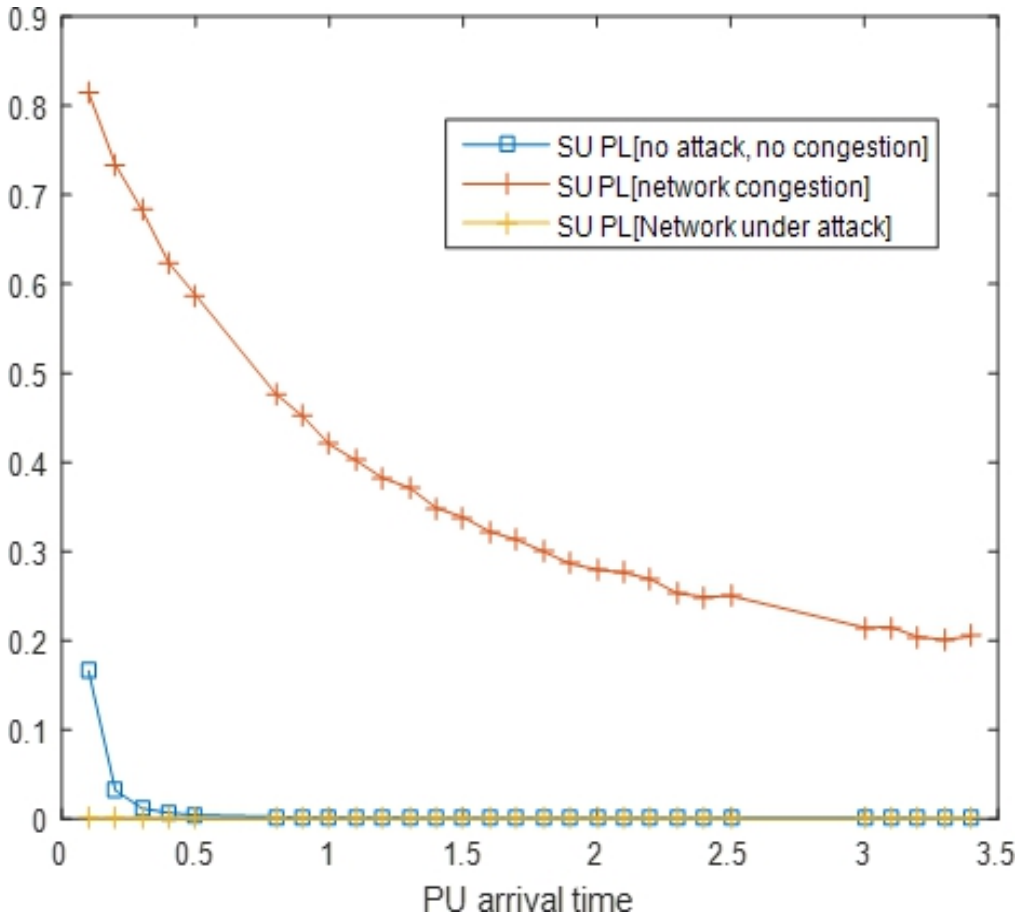

Figure 6.6: Probability of loss for network under different conditions

time to transmit PU requests. In this case, the band will be idle for about 50% of the time, resulting in decrease in the interference to PU transmission if the network is under attack. To demonstrate the solution to network congestion as highlighted in section 6, it is established here that increasing the number of SU requests when the spectrum is idle leads to significant increase in the throughput. For example, at any given slot, S_i, i= 1, 2,...n SU sends its requests in 3 per slot. Let

$$S_i = \{x_1, x_2, x_3\} \tag{6.10}$$

be the requests the SU sends per slot, then the total number of the requests for all the slots will be expressed as

$$X = \{S_1 + S_2 +, \ldots, + S_n\} \tag{6.11}$$

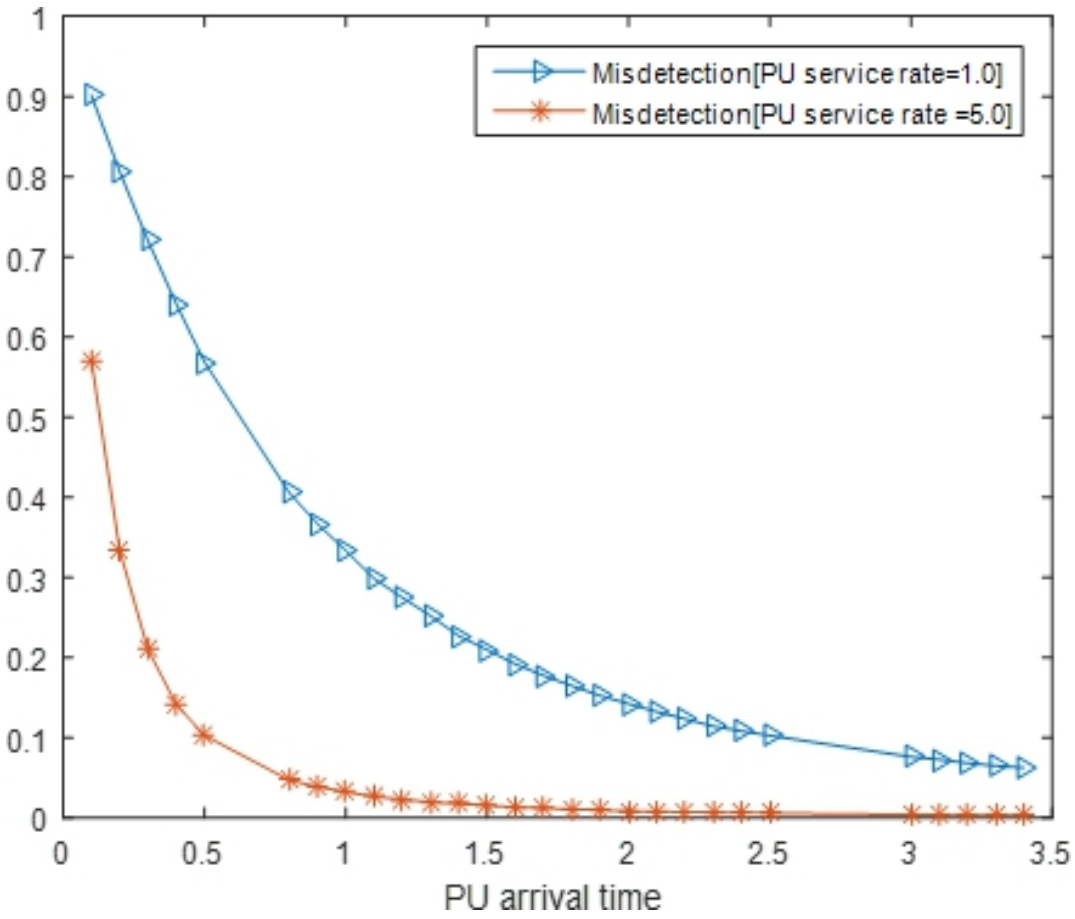

Figure 6.7: Probability of miss detection for network under different conditions

In this case, SU will continue to send this requests in 3 per slot until it gets to the predetermined transfer length of 9 requests at which it reduces to 1 per slot in order to avoid losses. This experiment was also carried out but with 2 requests in a slot and similarly until it gets to the transfer length of 9 requests at which it reduces to 1 request per slot. As shown in Fig. 6.8, there is an increase in SU throughput if more requests are transmitted in a slot. This increase in performance is because since the encryption node has an encryption rate of 10, then it implies that the greater the number of requests forwarded to it, the greater the throughput. Reducing the number in a slot leads to decline in throughput. To validate this assertion, the same experiment is carried out but with a transfer length of 9 and 20 and buffer size of 10. It started with 2 requests in a slot which reduces to 1 after the transfer

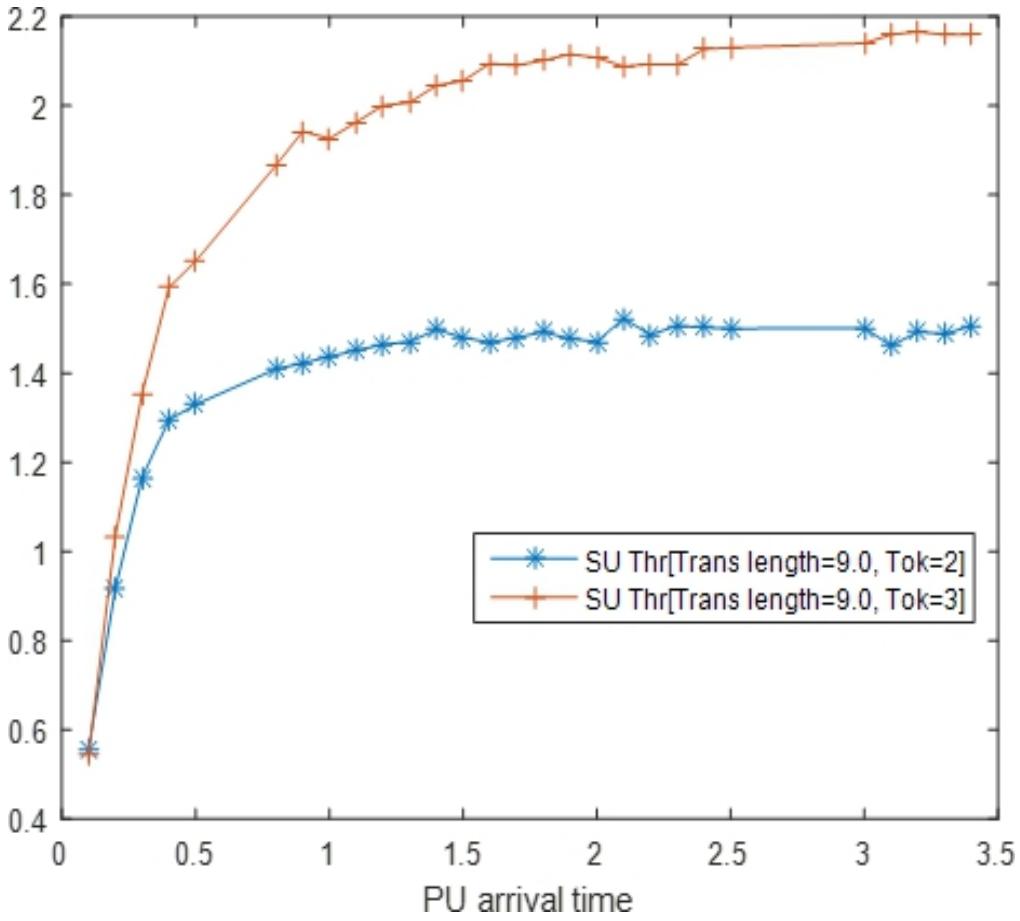

Figure 6.8: Throughput for the solution for network congestion

length. The results in Fig. 6.9 shows that though in both cases, the number of requests in a slot is 2, however, the probability of loss is greater when the transfer length is 20. This is because, at transfer length of 9, the SU reduces the number of requests in a slot to 1 to avoid losses. For transfer threshold of 20, SU will continue to send the same number of token with no consideration to the buffer size, thereby resulting in more losses as demonstrated in Fig. 6.9.

Fig. 6.10 also confirmed the assertions. In the figure, the experiment was carried out with same transfer length of 9 and initial 2 and 3 requests per slot respectively and queue capacity of 10. As demonstrated, the experiment with 3 requests per slot losses slightly more because it has more in the queue before it reduces sending.

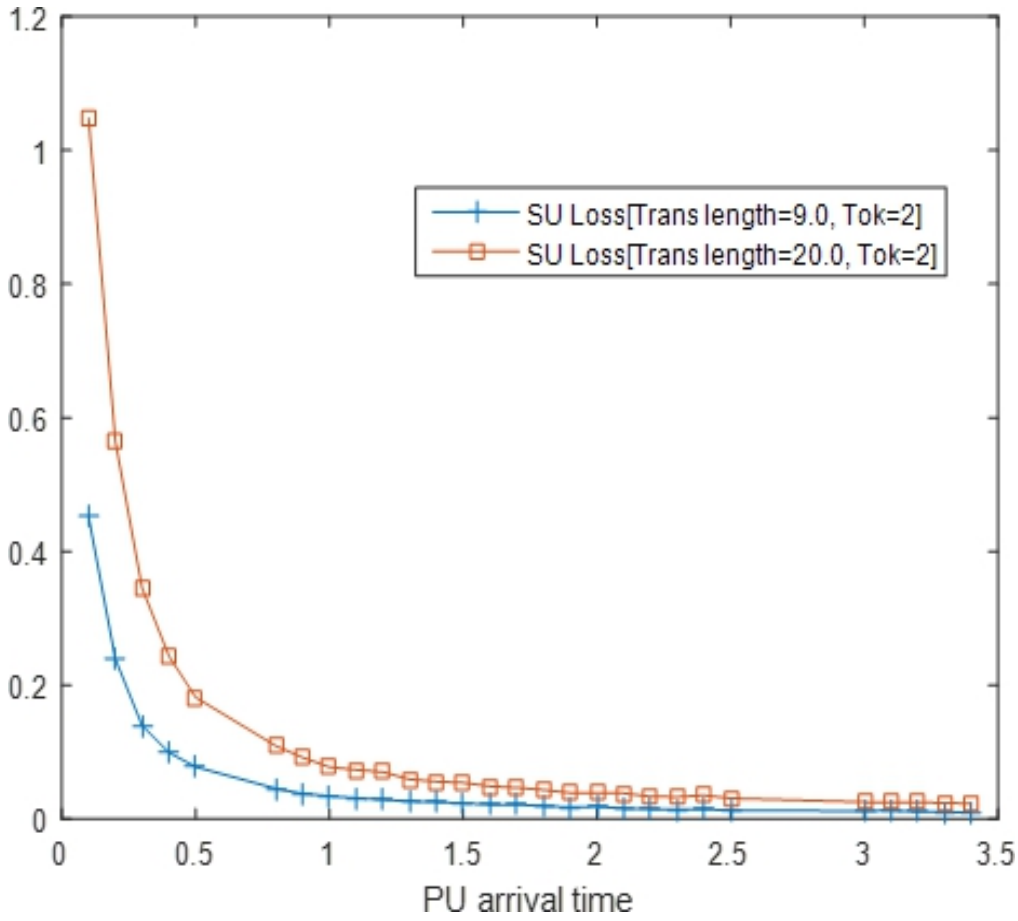

Figure 6.9: Probability of loss for the solution for network congestion

6.9 Summary

In the context of CRNs, it is essential to comprehend the actual cause of underutilization of idle spectrum space. In this research, an experiment was carried out aiming to distinguish a network under DoS attack from one experiencing network congestion so that an appropriate solution can be devised. The analysis of the proposed model shows that a network is under DoS attack if the throughput of the transmitter, average queue length and packet loss probability are approximately zero. However, in a congested network, all the metrics of the transmitter are greater than zero but less than the expected value. This analysis shows that DoS attacks can be detected as shown in Fig. 6.3.

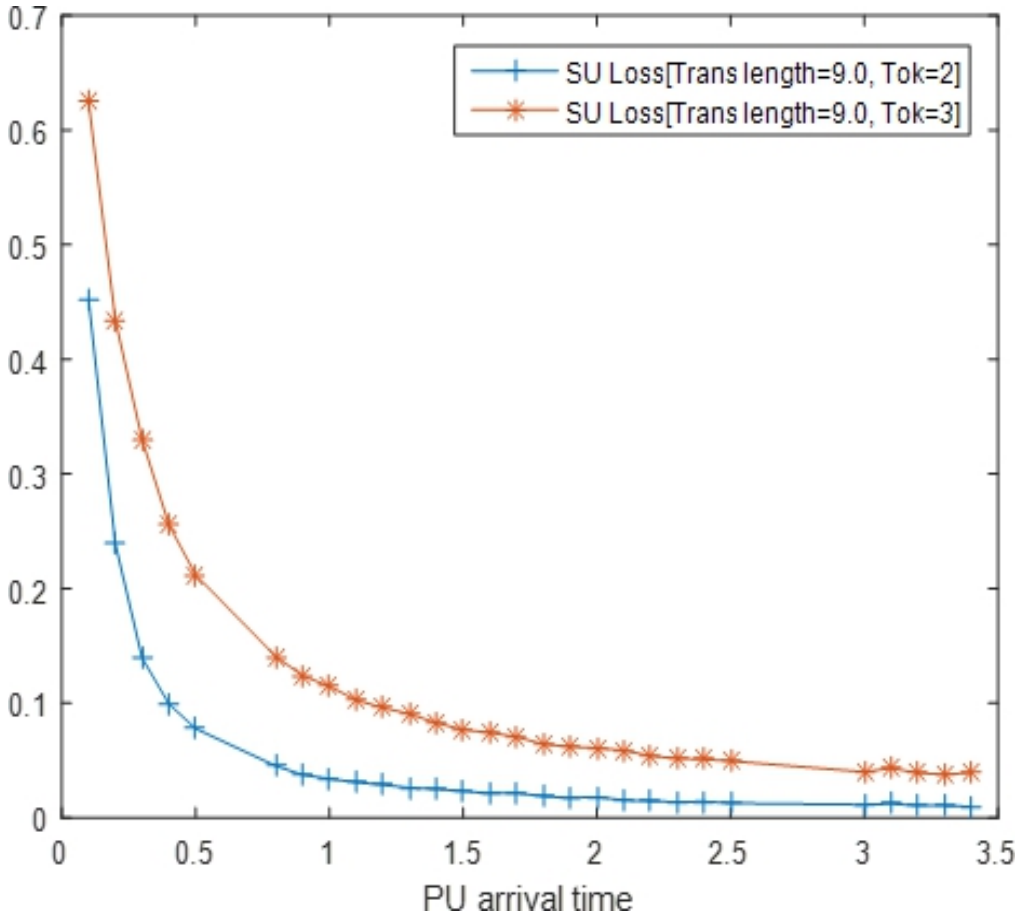

Figure 6.10: Probability of loss for the control of network congestion with transfer length of 9 and token size of 2 and 3 respectively

Chapter 7

Conclusions

A developed new formalism was proposed based on a SAN sub-model to determine 'optimal' sensing, security and performance trade-offs in SCRNs and UCRNs. In this context, an experiment-based assessment was carried out to quantify the improvement of scalability in comparison with UCRNs. The proposed redundant service channel was used to determine the optimum throughput achievable in SCRN in comparison with that of UCRNs. A further extension of the work included the use of a SAN model for the abstraction of the real system behaviour in order to establish if a CRN is under DoS attack and differentiate it from a network experiencing congestion.

In this context, an investigation was carried out focusing on a CRN, subject to 'optimal' sensing, security and performance trade-offs. The proposed CRN model with two classes of requests with priorities under a random selection discipline was used to abstract the behaviour of CRN with respect to sensing, security and performance. Specifically, a proposed new CRN model with intrusion detection control mechanism was introduced in Chapter 4, where the encryption rate was correlated with the rate of security incidents. Both sensing delay and the interplay between the encryption key lengths and rate of security incidents were used in conjunction with Poisson arrival process of SU requests. To this end, 'optimal' sensing vs security vs performance trade-offs in CRNs with the encryption and transmission times being exponential. Note that the input parameters were selected to imitate the real network behaviour, as appropriate.

Moreover, inhibitor arcs connected the performance model to security model whilst transition connected to the output place of the arrival node was used to model the sensing operation

of the network. This implied that sensing introduced some delay, which degraded the performance of the network. In this context, multiple classes of requests were used to model the sharing of spectrum by SUs as well as to represent the pre-emptions that occur whenever requests with higher priority appeared in the channel. Numerical simulation experiments were carried out, based on the use of the Mobius Petri Net Package, in order to determine the optimal value that offers no maximum but optimum values for sensing, security and performance parameters. The results of the simulations show that there exist an 'optimal' sensing time that maximizes the combined probabilities of 'spectrum detection', 'CRN being in secure state', and 'normalized throughput'. Simulation results were also presented to validate the analysis.

Chapter 5 focused on the analysis of a proposed SCRN, which withstood the surge in service demand, where the performance sub-model was connected to the security sub-model. This chapter provided a redundant service channel that acts as a back-up channel whenever there is an increase in service demand. This redundant service channel provided the same service with the dedicated server. This implies that even though redundant, it is still connected to security control model, which detects and freezes the channel in event of intrusion detection. The sensing time at which the scalable network has the highest throughput was quantified and compared with UCRN. This work was extended to include detection of PU arrival, detection and quantification of interference to PU signal. The outcomes of conducted experiments revealed that SCRNs require a shorter sensing time to achieve optimum performance and security than UCRNs.

Finally, Chapter 6 dealt with detection of DoS attacks, differentiating them from network experiencing congestion and their behavioural differences were assessed. Moreover, the investigation was extended to include a sub-model for detection of DoS attacks. The study adopted typical performance metrics for SUs such as packet loss probability, mean queue length and normalized transmission throughput. This led to the credible estimation of the PDR for SUs in order to determine whether or not the network was under DoS attack. The numerical experiments were conducted for a CRN, which was subject to i) Attacks ii) Normal working conditions and iii) Congestion. The results showed that a CRN under attack has near to zero throughput associated with SUs, which was distinguished from network

experiencing congestion as well as network under ideal working condition.

7.0.1 Future Work

An extension of this research could include the use of machine learning to predict the pattern of arrival of PU requests in order to reduce the sensing frequency of CRN and save the battery life. In this case, if it is discovered that during a period, the band is being consistently busy by PU requests, the CRN would be required to avoid sensing throughout this period, given that the probability of the band being occupied is high. This is in an effort to conserve the energy. Moreover, some spectrum opportunities would be missed by SUs during the period predicted to be busy by PUs. Thus, there is a need to determine 'optimal' trade-offs between energy conservation and missed spectrum opportunities.

When the network is under attack but not detected, it is also assumed to be insecure and not recovering as demonstrated in [10]. In this case, the network is vulnerable. Therefore, the future work could be extended to consider an additional state, namely a vulnerable state of the security detection control model aiming to protect the data during the period of vulnerability.

The work could be extended to include creation of group communication of CRN users in conjunction with intrusion detection system in order to protect the band from unauthorised users. For further protection and improvement of performance, batch rekeying technique could be used to identify the optimal settings that satisfy the performance and security requirements. In this case, any user in the group could sense and use the band with a shared access key.

Finally, further work will consider the extension of the thesis to include multiple spectrum bands and multiple CRN users. In this case, colour Petri nets could be used to identify users from different CRN users. The use of colours to represent requests from each participating CRN user is expected to improve the security because any user not in the accepted colour list would be flagged as malicious.

Bibliography

[1]Evans, D. (2012). The internet of things how the next evolution of the internet is changing everything (april 2011). White Paper by Cisco Internet Business Solutions Group (IBSG).

[2]Arjoune, Y., & Kaabouch, N. (2019). A comprehensive survey on spectrum sensing in cognitive radio networks: Recent advances, new challenges, and future research directions. Sensors, 19(1), 126.

[3]Sansoy, M., & Buttar, A. S. (2015, March). Spectrum sensing algorithms in Cognitive Radio: A survey. In 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) (pp. 1-5). IEEE.

[4] Lekomtcev, D., & Marsalek, R. (2015). Evaluation of Kolmogorov-Smirnov test and energy detector techniques for cooperative spectrum sensing in real channel conditions. Telfor Journal, 7(1), 31-36.

[5]Saad, W., Han, Z., Zheng, R., Hjorungnes, A., Basar, T., & Poor, H. V. (2011). Coalitional games in partition form for joint spectrum sensing and access in cognitive radio networks. IEEE Journal of Selected Topics in Signal Processing, 6(2), 195-209.

[6]Kyungate, K., Yan, X., and Sampath R., "Energy Detection Based Spectrum Sensing for Cognitive Radio: An Experimental Study," 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, 2010, pp. 1-5. doi: 10.1109/GLOCOM.2010.5683560

[7] Bhagate, S. V., & Patil, S. (2017, December). Maximizing spectrum utilization in cognitive radio network. In 2017 International Conference on Big Data, IoT and Data Science (BID) (pp. 82-90). IEEE.

[8]Bhattacharjee, S., Rajkumari, R., & Marchang, N. (2014). Cognitive Radio Networks Security Threats and Attacks: A Review. International Journal of Computer Applications, 975, 8887.

[9] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," in IEEE Communications Surveys & Tutorials, vol. 13, no. 2, pp. 245-257, Second Quarter 2011.

[10] Wolter, K., & Reinecke, P. (2010, June). Performance and security tradeoff. In International School on Formal Methods for the Design of Computer, Communication and Software Systems (pp. 135-167). Springer Berlin Heidelberg.

[11] Liang, Y. C., Zeng, Y., Peh, E. C., & Hoang, A. T. (2008). Sensing-throughput tradeoff for cognitive radio networks. IEEE transactions on Wireless Communications, 7(4), 1326-1337.

[12] Akin, S. (2014, March). Security in cognitive radio networks. In 2014 48th Annual Conference on Information Sciences and Systems (CISS) (pp. 1-6). IEEE.

[13] Kartheek, M., Misra, R., & Sharma, V. (2011, January). Performance analysis of data and voice connections in a cognitive radio network. In 2011 National Conference on Communications (NCC) (pp. 1-5). IEEE.

[14] Prashob, R. N., Vinod, A. P., and Krishna, A. K. (2010, November). An adaptive threshold based energy detector for spectrum sensing in cognitive radios at low SNR. In Communication Systems (ICCS), 2010 IEEE International Conference on (pp. 574-578). IEEE [impact of scalability].

[15] Ian F. Akyildiz, Won-Yeol Lee, Kaushik R. Chowdhury, CRAHNs: Cognitive radio ad hoc networks, Ad Hoc Networks, Volume 7, Issue 5, 2009, Pages 810-836, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2009.01.001.

[16] Taherpour, A., Gazor, S., & Nasiri-Kenari, M. (2008). Wideband spectrum sensing in unknown white Gaussian noise. IET communications, 2(6), 763-771.

[17] Torabi, N., Bhate, S., & Leung, V. C. (2013, September). Robust sensing strategy for dynamic spectrum access in the 2.4 GHz ISM band. In PIMRC (pp. 2713-2717).

[18] Kryszkiewicz, P., Kliks, A., & Bogucka, H. (2016). Small-scale spectrum aggregation and sharing. IEEE Journal on Selected Areas in Communications, 34(10), 2630-2641.

[19] Stotas, S., & Nallanathan, A. (2010, May). Overcoming the Sensing-Throughput Tradeoff in Cognitive Radio Networks. In ICC (pp. 1-5).

[20] Wang, B., & Liu, K. R. (2010). Advances in cognitive radio networks: A survey. IEEE Journal of selected topics in signal processing, 5(1), 5-23.

[21] Jain, P. C. (2013, December). Rural wireless broadband Internet access in Wireless Regional Area network using cognitive radio. In Signal Processing and Communication (ICSC), 2013 International Conference on (pp. 98-103). IEEE.

[22] You, C., Kwon, H., & Heo, J. (2011). Cooperative TV spectrum sensing in cognitive radio for Wi-Fi networks. IEEE transactions on consumer electronics, 57(1), 62-67.

[23] 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

[24] Gupta, M. S., & Kumar, K. (2019). Progression on spectrum sensing for cognitive radio networks: A survey, classification, challenges and future research issues. Journal of Network and Computer Applications.

[25] Zarrin, S., & Lim, T. J. (2009, June). Composite hypothesis testing for cooperative spectrum sensing in cognitive radio. In 2009 IEEE International Conference on Communications (pp. 1-5). IEEE.

[26] Rawat, D. B., Shetty, S., & Raza, K. (2012, September). Secure radio resource management in cloud computing based cognitive radio networks. In Parallel Processing Workshops (ICPPW), 2012 41st International Conference on (pp. 288-295). IEEE.

[27] Ahmed, K., Bashir, F., & ul Haq, M. E. (2010, July). Comparative study of centralized cooperative spectrum sensing in cognitive radio networks. In 2010 2nd International Conference on Signal Processing Systems (Vol. 3, pp. V3-246). IEEE.

[28] Attar, A., Tang, H., Vasilakos, A. V., Yu, F. R., & Leung, V. C. (2012). A survey of security challenges in cognitive radio networks: Solutions and future research directions. Proceedings of the IEEE, 100(12), 3172-3186.

[29] Fragkiadakis, A. G., Tragos, E. Z., & Askoxylakis, I. G. (2012). A survey on security threats and detection techniques in cognitive radio networks. IEEE Communications Surveys & Tutorials, 15(1), 428-445.

[30] Bhattacharjee, S., Sengupta, S., & Chatterjee, M. (2013). Vulnerabilities in cognitive radio networks: A survey. Computer Communications, 36(13), 1387-1398.

[31] Lamprecht, C., Van Moorsel, A., Tomlinson, P., & Thomas, N. (2006). Investigating the efficiency of cryptographic algorithms in online transactions. International Journal of Simulation: Systems, Science & Technology, 7(2), 63-75.

[32] Rizvi, S., Showan, N., & Mitchell, J. (2015). Analyzing the Integration of Cognitive Radio and Cloud Computing for Secure Networking. Procedia Computer Science, 61, 206-212.

[33] Wang, L., Wu, X., Zhang, S., Zhang, G., & Bao, Z. (2018, July). Cooperative Spectrum Sensing Algorithm Based on Phase Compensation in Cognitive Cloud Networks. In 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 143-147). IEEE.

[34] A. V. Kumar Kamal Chauhan, Amit K.S Sanger, "Homomorphic Encryption for Data Security in Cloud Computing," 14th Int. Conf. Inf. Technol., 2015.

[35] T. C. Chieu, A. Mohindra, and A. A. Karve, "Scalability and performance of web applications in a compute cloud," Proc. - 2011 8th IEEE Int. Conf. E-bus. Eng. ICEBE 2011, pp. 317âĂŞ323, 2011.

[36] N. R. A. DEEPIKA.Tenepalli, "Active Resource Provision in Cloud Computing Through Virtualization," IEEE Int. Conf. Comput. Intell. Comput. Res., 2014.

[37] J. Y. Lee and S. D. Kim, "Software approaches to assuring high scalability in cloud computing," Proc. - IEEE Int. Conf. E-bus. Eng. ICEBE 2010, pp. 300âĂŞ306, 2010.

[38] C. Colman-Meixner, C. Develder, M. Tornatore, and B. Mukherjee, "A Survey on Resiliency Techniques in Cloud Computing Infrastructures and Applications," IEEE Commun. Surv. Tutorials, vol. PP, no. 99, pp. 1âĂŞ1, 2016.

[39] A. Volokyta, I. Kokhanevych, and D. Ivanov, "Secure virtualization in cloud computing," 11th Int. Conf. Mod. Probl. Radio Eng. Telecommun. Comput. Sci., p. 395, 2012.

[40] S. P. Raj Jain, "Network Virtualization and Software Defined Networking for Cloud Computing: A Survey," IEEE Commun., 2013.

[41] S. Hassan, "Analysis of Cloud Computing Performance, Scalability, Availability, & Security," 2014.

[42] N. Anja, Fiegler; AndrÃľ Zwanziger; Niko, Zenker; Reiner, Dumke; Robert, "Advanced Quality Measurement for Cloud Services," IEEE Sixth Int. Conf. Cloud Comput., 2013.

[43] Rackspace, "The Economics of Cloud Computing," 2011.

[44] Z. Cao, J. Lin, C. Wan, Y. Song, Y. Zhang, and X. Wang, "Optimal Cloud Computing Resource Allocation for Demand Side Management," IEEE Trans. Smart Grid, pp. 1âĂŞ13, 2016.

[45] A. Vig, R. S. Kushwah, and S. S. Kushwah, "An Efficient Distributed Approach for Load Balancing in Cloud Computing," 2015 Int. Conf. Comput. Intell. Commun. Networks, pp. 751âĂŞ755, 2015.

[46] W. Liu, "Research on cloud computing security problem and strategy," 2012 2nd Int. Conf. Consum. Electron. Commun. Networks, CECNet 2012 - Proc., pp. 1216âĂŞ1219, 2012.

[47] F. Sharevski, "Digital forensic investigation in cloud computing environment: Impact on privacy," 2013 8th Int. Work. Syst. Approaches to Digit. Forensics Eng., pp. 1-6, 2013.

[48] C. Yan, "Cybercrime forensic system in cloud computing,"Proc. 2011 Int. Conf. Image Anal. Signal Process. IASP 2011, no. Dc, pp. 612-613, 2011.

[49] C. A. V. Qingling Wang, "Impact of Cloud Computing Virtualization Strategies on Workloads' Performance," 2011 Fourth IEEE Int. Conf. Util. Cloud Comput., 2011.

[50] P. Jogalekar, M. Woodside, and S. Member, "Evaluating the Scalability of Managed Distributed Systems," IEEE Trans. Parallel Distrib. Syst., vol. 11, no. 6, pp. 589-603, 2000.

[51] Netto, M. A., Cardonha, C., Cunha, R. L., & Assuncao, M. D. (2014, September). Evaluating auto-scaling strategies for cloud computing environments. In 2014 IEEE 22nd International Symposium on Modelling, Analysis & Simulation of Computer and Telecommunication Systems (pp. 187-196). IEEE.

[52] E. Biersack, "Cloud Computing Challenges and Opportunities," Fr. Summer Sch. 2011 Jr. Sci., pp. 34-38, 2011.

[53] V. R. Kanakala, V. K. Reddy, and K. Karthik, "Performance Analysis of Load Balancing Techniques in Cloud Computing Environment," 2015.

[54] A. Goswami and R. P. Patel, "Service Migration In Cluster Based Cloud Computing Environment," Icip 2015, pp. 468-471, 2015.

[55] C. J. D. D. L. Jens, Myrup, Pedersen; M. Tahir, Riaz; Joaquim, "Assessing Measurements of QoS for global Cloud Computing Services," Ninth IEEE Int. Conf. Dependable, Auton. Secur. Comput., 2011.

[56] M. M. Falatah and O. A. Batarfi, "Cloud Scalability Considerations," Int. J. Comput. Sci. Eng. Surv., vol. 5, no. 4, pp. 37-47, 2014.

[57] Chuku, E. E., & Kouvatsos, D. D. (2018). Impact of scalability on the performance of secured cognitive radio networks. Electronic Notes in Theoretical Computer Science, 340, 123-135.

[58] Kakalou, I., Psannis, K. E., Krawiec, P., & Badea, R. (2017). Cognitive radio network and network service chaining toward 5G: Challenges and requirements. IEEE Communications Magazine, 55(11), 145-151.

[59] Khan, A. A., Rehmani, M. H., & Rachedi, A. (2017). Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions. IEEE wireless communications, 24(3), 17-25.

[60] H. C. Massimo Ficco, Christian Esposito, "Live Migration in Emerging Cloud Paradigms," 2016.

[61] Balbo, G. (2000, July). Introduction to stochastic Petri nets. In School organized by the European Educational Forum (pp. 84-155). Springer, Berlin, Heidelberg.

[62] Mobius Tool: MÂÍobius Manual Version 2.4 Rev. 1. Copyrightc 2012 William H. Sanders and The Board of Trustees of the University of Illinois. Accessed on: June. 21, 2019. [Online].Available:https://www.mobius.illinois.edu/wiki/index.php/Building-ModelsSAN

[63] Wang, J. (2007). Petri Nets for Dynamic Event-Driven System Modeling. Handbook of Dynamic System Modeling, 1.

[64] Zhang, L., Yu, J., & Wu, Z. (2015, August). Secured chaotic cognitive radio system using advanced encryption standard. In Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015 IEEE 26th Annual International Symposium on (pp. 7-11). IEEE.

[65] Sanyal, S., Bhadauria, R., & Ghosh, C. (2009, December). Secure communication in cognitive radio networks. In Computers and Devices for Communication, 2009. CODEC 2009. 4th International Conference on (pp. 1-4). IEEE.

[66] Lim, C. H. (2012). Adaptive energy detection for spectrum sensing in unknown white Gaussian noise. IET communications, 6(13), 1884-1889.

[67] Bhowmick, A., Das, M. K., Biswas, J., Roy, S. D., & Kundu, S. (2014, February). Throughput optimization with cooperative spectrum sensing in cognitive radio network. In Advance Computing Conference (IACC), 2014 IEEE International (pp. 329-332). IEEE.

[68] Duan, D., Yang, L., & Principe, J. C. (2010). Cooperative diversity of spectrum sensing for cognitive radio systems. IEEE transactions on signal processing, 58(6), 3218-3227.

[69] Nekovee, M. (2010, April). Cognitive radio access to TV white spaces: Spectrum opportunities, commercial applications and remaining technology challenges. In New Frontiers in Dynamic Spectrum, 2010 IEEE Symposium on (pp. 1-10). IEEE.

[70] Alamgir, M., Faulkner, M., Gao, J., & Conder, P. (2008, October). Signal detection for cognitive radio using multiple antennas. In 2008 IEEE International Symposium on Wireless Communication Systems (pp. 488-492). IEEE.

[71] Naeem, M., Illanko, K., Karmokar, A., Anpalagan, A., & Jaseemuddin, M. (2013). Energy-efficient cognitive radio sensor networks: Parametric and convex transformations. Sensors, 13(8), 11032-11050.

[72] Maleki, S., Pandharipande, A., & Leus, G. (2011). Energy-efficient distributed spectrum sensing for cognitive sensor networks. IEEE sensors journal, 11(3), 565-573.

[73] Ejike, C., Demetres, K.(2017). Combined Sensing, Performance and Security Tradeoff in Cognitive Radio Networks. 2017 IEEE International Symposium on Network Computing and Applications (NCA)

[74] Chieu, T. C., Mohindra, A., & Karve, A. A. (2011, October). Scalability and performance of web applications in a compute cloud. In e-Business Engineering (ICEBE), 2011 IEEE 8th International Conference on (pp. 317-323). IEEE.

[75] Lee, J. Y., & Kim, S. D. (2010, November). Software approaches to assuring high scalability in cloud computing. In e-Business Engineering (ICEBE), 2010 IEEE 7th International Conference on (pp. 300-306). IEEE.

[76] E.E Chuku, A., & D.D Kouvatsos (2016). Performance Evaluation of Service Channel Scalability on Cloud Platforms. In 32nd UK Performance Engineering Workshop, University of Bradford.

[77] Vilaplana, J., Solsona, F., TeixidÃş, I., Mateo, J., Abella, F., & Rius, J. (2014). A queuing theory model for cloud computing. The Journal of Supercomputing, 69(1), 492-507.

[78] Lorido-Botran, T., Miguel-Alonso, J., & Lozano, J. A. (2014). A review of auto-scaling techniques for elastic applications in cloud environments. Journal of Grid Computing, 12(4), 559-592.

[79] Allen, A. O. (2014). Probability, statistics, and queueing theory. Academic Press.

[80] Abdulsattar, M. A., & Hussein, Z. A. (2012). Energy detection technique for spectrum sensing in cognitive radio: a survey. International Journal of Computer Networks & Communications, 4(5), 223.

[81] Saleem, Y., & Rehmani, M. H. (2014). Primary radio user activity models for cognitive radio networks: A survey. Journal of Network and Computer Applications, 43, 1-16.

[82] A., Censki (n.d). Reliability Modelling and Analysis with Free and Open Source Software.

[83] Balbo, G., Bruell, S. C., & Ghanta, S. (1988). Combining queueing networks and generalized stochastic Petri nets for the solution of complex models of system behavior. IEEE Transactions on Computers, 37(10), 1251-1268.

[84] Marsan, M. A., Balbo, G., Conte, G., Donatelli, S., & Franceschinis, G. (1994). Modelling with generalized stochastic Petri nets. John Wiley & Sons, Inc.

[85] Balapuwaduge, I. A. M. (2016). Channel access and reliability performance in cognitive radio networks: Modeling and performance analysis.

[86] Clancy, T. C., & Goergen, N. (2008, May). Security in cognitive radio networks: Threats and mitigation. In 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008) (pp. 1-8). IEEE.

[87] Esraa M. G., Mohamed A., Ahmed M., Spatiotemporal diversification by moving-target defense through benign employment of false-data injection for dynamic, secure cognitive radio network, Journal of Network and Computer Applications, Volume 138, 2019, Pages 1-14, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2019.02.020.

[88] Chuku, E. and Demetres K., "Combined sensing, performance and security trade-offs in cognitive radio networks," 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, 2017, pp. 1-4. doi: 10.1109/NCA.2017.8171335

[89] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005, May). The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (pp. 46-57). ACM.

[90] Mehr, K. A., Niya, J. M., & Akar, N. (2018). Queue management for two-user cognitive radio with delay-constrained primary user. Computer Networks, 142,

[91] Kurose, J., & Ross, K. W. (2010). Computer networking: International version: A top-down approach. doi: 10.1109/SURV.2011.041110.000221-12.

[92] Kulkarni, S. S., Gouda, M. G., & Arora, A. (2006). Secret instantiation in ad-hoc networks. Computer Communications, 29(2), 200-215.

[93] Syed R, Nathan S, John M, "Analyzing the Integration of Cognitive Radio and Cloud Computing for Secure Networking" Procedia Computer Science, Volume 61,2015, Pages 206-212,ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.09.195.

[94] Cho, J. H., Chen, R., & Feng, P. G. (2008, March). Performance analysis of dynamic group communication systems with intrusion detection integrated with batch rekeying in mobile ad hoc networks. In Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on (pp. 644-649). IEEE.

[95] I. Ngomane, M. Velempini and S. V. Dlamini, "The detection of the spectrum sensing data falsification attack in cognitive radio ad hoc networks," 2018 Conference on Information Communicatnd Society (ICTAS), Durban, 2018, pdoi: 10.1109/ICTAS.2018.8368742

[96] Pathan, A. S. K., Lee, H. W., Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In 2006 8th International Conference Advanced Communication Technology (Vol. 2, pp. 6-pp). IEEE.

[97] Y. Yang, Q. Zhang, Y. Wang, T. Emoto, M. Akutagawa and S. Konaka, "Multi-strategy dynamic spectrum access in cognitive radio networks: Modeling, analysis and optimization," in China Communications, vol. 16, no. 3, pp. 103-121, March 2019. doi: 10.12676/j.cc.2019.03.010

[98] Thamilarasu, G., Mishra, S., & Sridhar, R. (2011). Improving reliability of jamming attack detection in ad hoc networks. International Journal of Communication Networks and Information Security, 3(1), 57.

[99] Chelli, K. (2015, July). Security issues in wireless sensor networks: attacks and counter-measures. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 1-3).

[100] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," in IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, Jan.-March 2008. doi: 10.1109/MPRV.2008.6

[101] Balbo, G., Bruell, S. C., & Ghanta, S. (1988). Combining queueing networks and generalized stochastic Petri nets for the solution of complex models of system behavior. IEEE Transactions on Computers, 37(10), 1251-1268.

[102] Marsan, M. A., Balbo, G., Conte, G., Donatelli, S., & Franceschinis, G. (1994). Modelling with generalized stochastic Petri nets. John Wiley & Sons, inc