The Design and the implementation of the byzantine attack mitigation scheme in Cognitive Radio Ad Hoc networks

By

SEKGOARI SEMAKA MAPUNYA

[redacted]

Research Dissertation

Submitted in fulfilment of the requirements for the degree of

MASTER OF SCIENCE

In the

Faculty of Science and Agriculture

(School of Mathematical and Computer Sciences)

At the

University of Limpopo

SUPERVISOR: Prof M Velempini

April 2019

DECLARATION

I, Sekgoari Semaka Mapunya, hereby declare that **The design and implementation of the Byzantine attack mitigation scheme in cognitive radio ad hoc networks** is my original work and that all sources that have been used are fully acknowledged and correctly referenced. I further declare that this work has not previously been submitted to any other university for a qualification.

Signature: ____________________________

Date : _____________________________

ACKNOWLEDGMENTS

Firstly, I would like to honour and appreciate the sovereign God, the creator of heaven and earth who gave me life and wisdom throughout the research period and beyond. All the honour and glory are directed to Him, now and forever more. Without him I am nothing.

Secondly, I would like to acknowledge the man who guided me and worked hard to bring the best out of me, my supervisor Prof Mthulisi Velempini.

Finally, I want to thank my wife Dimakatso Mapunya for the prayers she continually makes unto God concerning my life. They are much appreciated and recognised. These are prayers which kept me going throughout the research period.

ABSTRACT

Cognitive radio network, which enables dynamic spectrum access, addresses the shortage of radio spectrum caused by ever-increasing wireless technology. This allows efficient utilisation of underutilised licenced spectrum by allowing cognitive radios to opportunistically make use of available licenced spectrum. Cognitive radios (CR), also known as secondary users, must constantly sense the spectrum band to avoid interfering with the transmission of the licenced users, known as primary users. Cognitive radios must cooperate in sensing the spectrum environment to avoid environmental issues that can affect the spectrum sensing. However, cooperative spectrum sensing is vulnerable to Byzantine attacks where selfish CR falsify the spectrum reports. Hence, there is a need to design and implement a defence mechanism that will thwart the Byzantine attacks and guarantee correct available spectrum access decisions.

The use of extreme studentized deviate (ESD) test together with consensus algorithms are proposed in this study to combat the results of the availability of Byzantine attack in a cognitive radio network. The ESD test was used to detect and isolate falsified reports from selfish cognitive radios during the information sharing phase. The consensus algorithm was used to combine sensing reports at each time k to arrive at a consensus value which will be used to decide the spectrum availability. The proposed scheme, known extreme studentized cooperative consensus spectrum sensing (ESCCSS), was implemented in an ad hoc cognitive radio networks environment where the use of a data fusion centre (DFC) is not required. Cognitive radios make their own data fusion and make the final decision about the availability of the spectrum on their sensed reports and reports from their neighbouring nodes without any assistance from the fusion centre. MATLAB was used to implement and simulate the proposed scheme. We compared our scheme with Attack-Proof Cooperative Spectrum Sensing to check its effectiveness in combating the effect of byzantine attack.

Table of contents

List of tables

List of figures

Chapter 1

1.1 Introduction

An increase in number of devices which utilize wireless network has led to a problem of spectrum overcrowding. Dr Joseph Mitola proposed the concept of cognitive radio network (CRN) as a promising solution to this problem [1]. This type of a network allows the cognitive nodes (CN) considered as secondary or unlicensed users to dynamically use the spectrum band which is licensed to be used by primary or licensed users at a certain time. Spectrum sensing is an initial and important requirement of CRN; it is where CN learns about its environment.

Cooperative spectrum sensing(CSS) was proposed as an efficient method to avoid interference of SU and PU as it can reduce hidden node problem, false alarm, accurate signal detection [2] Etc. CSS and allocation on spectrum can be achieved by either centralized or decentralized technique. In contrast, centralized approach sensed information from the cognitive users about the environment is channeled to a central focal point while in decentralized environment referred to as cognitive radio ad hoc networks (CRAHN) and cognitive users share the information among themselves [3]. Despite the benefits of CSS, CRAHN due to its distributed nature is vulnerable to many security attacks. The presence of malicious user in the network can paralyze the entire network by reporting wrong sensed information about the radio environment. Byzantine (Spectrum sensing data falsification) attack is the most detrimental type of an attack which target CSS. There is a great need to address this type of an attack as it is under-researched in CRAHN.

A number of schemes [4] [5] [6], have been proposed to combat security threats associated with spectrum sensing, most of the proposed schemes are based on centralized model of CSS and there is less work done in infrastructure less CRN.

Therefore, there is a need for researchers to focus on infrastructure-less networks and address the corresponding security issues. The existing spectrum sensing techniques, such as energy detection [7] and matched filter detection [8], the security issues where not considered in their design. We propose a scheme which complements such spectrum sensing techniques and effectively combat byzantine attack. The scheme makes use of the generalized extreme studentized deviate test and consensus algorithm to detect malicious user whom are broadcasting false data and those data is excluded from spectrum access decision making.

1.2 Problem statement

There are many security issues in relation to wireless networks (WN) due to the openness of the communication channels, information is transmitted on a logical connection over a radio channel and it makes it easy for attackers to intercept data in transit. CRN as a subset of WN, it is also susceptible to the same security issues which are common in the WN community. Furthermore, due to CRN capabilities, like spectrum sensing and spectrum decision, new security challenges have emerged. If false spectrum sensing results are broadcasted by malicious user or an attacker, spectrum access decision will be taken based on false data which affects the usage of the spectrum.

This security challenge requires more attention since one failure in the cognitive cycle can lead to PU interference. Malicious nodes known as byzantine nodes can report false data to be used in spectrum access decision. The byzantine node can report that a spectrum is occupied while it is idle or vice versa. This leads to the underutilization of the spectrum and to PU interference. As a result, the main objective of CRN to address the underutilization of the spectrum is not realized.

1.3 Hypothesis

The use of generalized extreme studentized deviation test can address the effects of byzantine attack in CRAHN through the implementation of an intelligent and trusted scheme.

1.4 Objectives

The aim of this study is to design and implement a defence mechanism optimised for CRNs. This is broken down into the following objectives:

i. To evaluate the effectiveness of the existing schemes designed to combat the Byzantine attack.
ii. To investigate the design challenges and shortcomings of existing Byzantine attack countermeasures in cognitive radio ad hoc networks (CRAHNs).
iii. To design and implement a defence scheme to counter the effects of the Byzantine attack.

1.5 Research questions

The following research questions will help devise the best countermeasures and will be answered throughout the study.

i. How significantly can Byzantine attacks cripple the network?
ii. How effective are the existing spectrum sensing data falsification attacks countermeasures?
iii. Which is the most effective countermeasure?
iv. Does our proposed scheme outperform the best current scheme?

1.6 Motivation

CRNs were proposed to solve the problem of spectrum scarcity by allowing the secondary users (SUs) to use licensed spectrum opportunistically. SUs are allowed to utilise idle spectrum without causing interference to PUs. However, this is threatened by the behaviour of malicious SUs which mislead other users in cooperative spectrum sensing paradigm. The Byzantine attack has been widely studied in infrastructure-based networks; however, there is a need to explore the attack in an infrastructure-less environment. This research is motivated by a need to design countermeasures optimised for infrastructure-less networks such as CRNs.

1.7 Scientific contribution

The Byzantine attack has been addressed in the infrastructure-based CRNs however, it is still a challenge in the infrastructure-less CRNs. This study provides a Byzantine solution to address its effects in the infrastructure-less CRNs.

1.7.1 Publications generated from the dissertation

A. Book chapter

1. S. Mapunya and M. Velempini, "Investigating spectrum sensing security threats in cognitive radio networks," in *Ad Hoc Networks*, Niagara falls, Canada, Springer, 2018, pp. 60-68.

B. Conference proceeding

1. S. Mapunya and M. Velempini, "The Design of Byzantine Attack Mitigation Scheme in Cognitive Radio Ad-hoc Networks," in *2018 International Conference*

on Intelligent and Innovative Computing Applications (ICONIC), Plaine Magnien, Mauritius, 2018.

1.8 Dissertation review

This dissertation is organised into six chapters. In Chapter 2, an overview of cognitive radio networks is presented and its security threats are also discussed briefly. Chapter 3 presents an extensive literature review, specifically existing countermeasures, which are proposed by other researchers to act against Byzantine attacks. Chapter 4 presents the methodology and design of the proposal. This proposed scheme is explained in detail and, in Chapter 5, an explanation of a simulation run to assess its effectiveness is discussed. In Chapter 6, a conclusion of the findings is drawn and recommendations are given for possible future research.

Chapter 2

2.1 Objective

Cognitive radio networks (CRNs), different kind of architecture and spectrum sensing techniques are introduced in this chapter.

The ever-increasing demand of wireless communication technologies has led to drastically increasing demand for radio spectrum. Available radio spectrum were allocated and licenced for permanent use by different applications. Cognitive radio networks were seen as a potential solution to the problem of the high-demand of radio spectrum. This problem is solved by allowing unlicensed users, known as secondary users (SU), to opportunistically utilise the licenced spectrum. It has presented an opportunity for secondary users to utilise the licensed spectrum without causing any interference to licensed users, or primary users (PU). As this technology is about to be fully deployed for use, a major problem of its advancement is security threats and attacks. Security threats sometimes attack the main aspect of this network which is spectrum sensing. There are two types of attacks which focus on spectrum sensing: byzantine attack, and primary user emulation attack.

Primary user emulation attack is an attack that acts against spectrum access by secondary users. In this case, an attacking node mimics the characteristics of primary users in order to mislead legitimate sensing nodes to conclude that a primary user is in use of the spectrum [9].

Spectrum sensing data falsification attacks occur when attacking nodes sends false information about the surrounding radio spectrum.

Since spectrum shortage in wireless communications can be alleviated by cognitive radio networks, new security issues evolved. However, traditional network security attacks are also a challenge to cognitive radio networks. The only unique factor that occurs between classic and new threats to cognitive radio networks come from the opportunistic spectrum access capability of this new technology [10]. Byzantine attacks and primary user emulation attacks are some of the examples of cognitive radio networks attacks.

A primary user emulation attack is an attack that acts against spectrum access by secondary users. In this case, an attacking node mimics the characteristics of primary users in order to mislead legitimate sensing nodes to conclude that primary user is in use of the spectrum [9].

Medium access control spoofing and hello flood attacks are some of the security issues inherited from conventional wireless networks. Cognitive radios, cognitive radio networks and the security threats associated with cognitive radio networks will be discussed in this chapter.

2.2 Cognitive radio and cognitive radio networks

In 1999, Mitola and Maguire came up with the term ‘cognitive networks’ [11]. Since then, their work has received attention from other researchers and in-depth research was done on this area.

Software defined radio is the basis of cognitive radio. Software defined radio is a radio communication system that can get any modulation across a large frequency spectrum by tuning into a frequency band and processing those signals though its software. Efficient usage of the spectrum band can be observed when secondary users are granted permission to utilise the observed unused spectrum which is permanently licensed to be used by primary users. Implementation of this technology enables secondary users to observe, or sense, the surrounding radio spectrum, select the available channel and utilise the available spectrum channel if they vacate the channel when the primary user reclaims their spectrum usage rights. Figure 2-1 presents the main functions of cognitive radio.

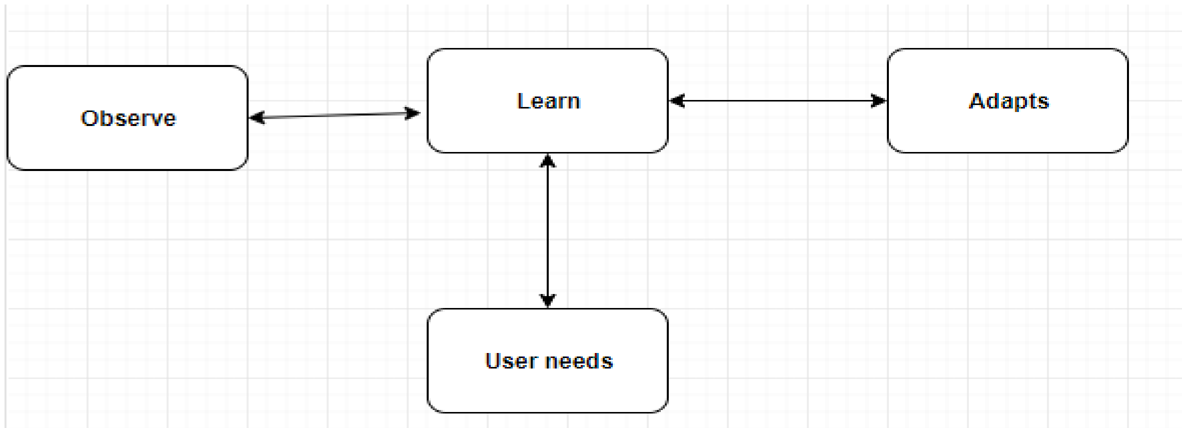

Figure 2-1: Main functions of cognitive radio

What distinguishes cognitive radio from traditional networks is its key functions as shown in Figure 2.1. Cognitive radio is able to sense the surrounding radio frequency and detect the unused radio spectrum band. This function is performed during the observation stage of cognitive radio. Based on past decisions and observations, cognitive radio is able to learn the surrounding radio environment. This device can be trained by neural network techniques and support vector machines to predict changes in the radio frequency environment. A cognitive radio can adapt its operating parameters, such as frequency, transmission power, modulation type, etc., to the varieties of the surrounding radio environment. It makes these adaptions during the adaption stage. Enhanced communication quality is achieved by the choice of radio interface used for communication, or tuning the communication system's parameters to suit the user by cognitive radio. This is achieved during users' needs functionality of cognitive radio.

2.3 Cognitive radio network architecture

CRNs is not just a connection of cognitive radios but CRNs are made from different sort of networks and systems that can be seen as a different network. Cognitive radios have the ability to observe the surrounding radio environment and to find an available spectrum hole. CRN environment also consists of primary users which are licensed to use certain spectrum band. The goal cognitive radio network is to optimise network utilization, rather than dealing with spectral efficiency issues only.

Deployment of CRNs spans across different types of network architecture. The fundamental components of CRNs are cognitive/secondary/unlicensed users, the primary/licenced users, base stations/cognitive tower and core networks. These four principal components make two different kinds of network architecture which are infrastructure, infrastructure-less (ad hoc and mesh) architectures [12].

2.3.1 Infrastructure architecture

In an infrastructural-based architecture as shown in Figure 2-2 (a), the cognitive radio tower controls the activities of secondary users. The cognitive radio tower controls the usage of both the licensed and unlicensed bands by secondary users, this is done by collecting all the information about the surrounding radio spectrum from the secondary users.

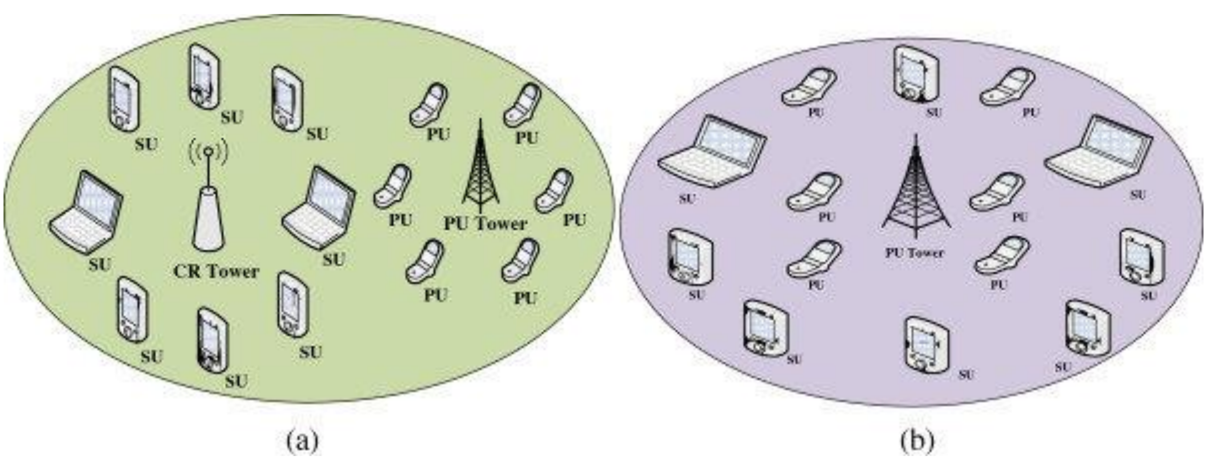

Figure 2-2: CRN architecture (a) Infrastructure (b) Ad-hoc . [13]

Based on the collected information, the CR tower makes spectrum access decisions for all the cognitive users. The secondary users can only access the cognitive radio tower in a one-hop manner. SUs under the transmission range of the same CR tower/base station communicate with each other through that base station. We have two different communication channels in CRN, sensing channel and the reporting channel. The sensing channel is the channel between the primary user and the secondary user and the reporting channel is the channel between the CR user and the CR tower.

2.3.2 Ad hoc network architecture

As shown in Figure 2-3(b), Ad hoc network architecture has no central CR tower support. The secondary users communicate directly with each other in an ad hoc manner and information is shared between the secondary users who fall within this communication range. Cognitive radio users can either communicate with each other using existing communication protocols or by dynamically using spectrum holes. The cognitive radio users do not have direct communication channels with the primary user and rely on their local observation during their operation.

2.4 Spectrum sensing in cognitive radio networks

Due to the ever increasing number of wireless devices, radio spectrum demand has drastically increased. It is necessary to propose methods to propel effective utilisation of radio spectrum as it has gradually become a scare resource. Spectrum sensing is one of the cognitive capability of CR. This basic function helps secondary users to learn about the radio environment. In cognitive radio networks, spectrum sensing is performed by secondary users to locate spectrum holes for use without causing interference to the primary user.

As explained in literature [14] and [15], there are several existing spectrum sensing techniques. These techniques can be classified into non-cooperating spectrum and cooperative spectrum sensing techniques. The non-cooperative sensing technique make use of the physical layer characteristics of primary user transmissions such as energy, spectral density modulation and cyclostationary properties [16]. Secondary users are allowed to relay spectrum observation information to each other, this phenomenon is known as cooperative sensing technique which is an improvement of non-cooperative spectrum sensing technique. The local spectrum sensing technique is further categorised into energy detection, cyclostationary feature detection and matched filter detection based on the sensing method employed in the signal detection process.

2.5 Byzantine attack

Byzantine attack is one of the most prominent attacks which can degrade the performance of dynamic spectrum access. In a typical dynamic spectrum access, PUs have the upper hand as they are able to use the spectrum at any point in time, while secondary users must relinquish the privileges gained when they concluded that a primary user is not using the spectrum band. All SUs have equal rights to use available spectrum. Malicious users can mislead genuine users to conclude that a spectrum is occupied for them to have all spectrum resources to them self. These malicious users can also mislead genuine users, causing them to conclude that a spectrum band is not in use by the primary users while in fact the band is occupied and lead to interference between the PU and SU. This cognitive radio network security issue is known as a Byzantine attack.

Therefore, we can define a Byzantine attack as an attack in both centralised and decentralised cognitive radio network where malicious users change information and report false data about the nature of the surrounding radio environment. Since legitimate secondary users are misled by these attackers, the entire network becomes untrustworthy.

Byzantine attacks can be launched in the process of spectrum occupancy data sharing among cognitive users and spectrum sensing using any type of spectrum sensing technique. Energy detection is the most popular and simple way to implement a spectrum sensing technique. There are several types of Byzantine attack namely:

2.5.1 Always yes

The aim of this attack is to decrease the probability of detection and maximise the attacker's bandwidth by preventing other SU's from using the available channel. When the malicious user detects spectrum holes, they prevent other users from using that hole by falsifying the actual sensed data, and report that the primary user is currently using the channel.

2.5.2 Always no

This type of attack aims to increase the probability of false alarms and causes interference between the SU and PU. This is achieved by reporting that a channel is not in use.

2.6 The Impact of Byzantine attack in cognitive radio ad hoc network

A Byzantine attack on CRAHN can influence the functioning of the entire network. CRNs which is well functional can be affected by the presence of byzantine malicious nodes which can cause legitimate cognitive user to collide with primary users during spectrum access phase.

2.6.1 Cognitive radio ad hoc network in the absence of an attacking nodes

Cognitive radio networks were proposed without taking into consideration the issue of security which can severely degrade its performance and affect the already existing wireless network. Figure 2-3 shows a typical cognitive radio ad hoc network in the absence of attacking nodes.

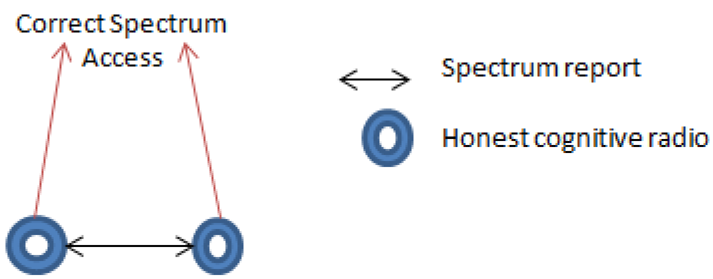

Figure 2-3: Cognitive radio ad-hoc network without Byzantine attack

Correct spectrum access decision is cooperatively taken by individual cognitive radios in an ad hoc network if there is no attacking cognitive radio in the network. Cognitive radios share the observed spectrum observations among themselves as shown on Figure 2-3 and the reported information is legitimate since all of the radios in the network are legitimate, hence it leads to correct spectrum access decision making. Therefore, the observed spectrum holes are utilised efficiently without causing any interference to the primary user by secondary users.

2.6.2 Cognitive radio ad hoc network in the presence of an attacking nodes

If the cognitive radio ad hoc network exists and operates in the presence of an attacking node, the spectrum access decision making of the honest cognitive radios will be misled and the wrong decision will be made. Figure 2-4 shows a cognitive ad hoc network where an attacking node / dishonest cognitive radio is present.

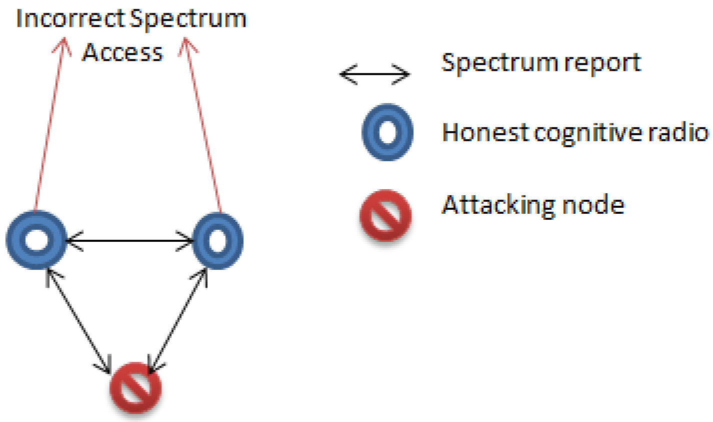

Figure 2-4: Cognitive radio ad-hoc network with Byzantine attack

Attacking node relays falsified observed radio environment observations to its neighbours in an ad hoc cognitive radio network as shown in figure 2-4. Therefore, there is a need to design a mitigation scheme to identify falsified data.

2.7 Conclusion

This chapter introduced and reviewed cognitive radio and its architecture and primary functionality. Cognitive radio promises to be one of the more favourable solutions to spectrum scarcity in wireless networks. Spectrum sensing techniques, a major operational aspect of CRNs were briefly looked at. The security threats known as Byzantine attack which is associated with cognitive radio networks was also studied.

Chapter 3

3.1 Introduction

This chapter analyses and reviews published research, industry guidance, and current research activities related to Byzantine attack countermeasures. Furthermore, this chapter highlights the shortcomings the counter measures have in addressing the attack.

3.2 Review

Several schemes have been proposed to combat security threats associated with spectrum sensing. Most of these proposed schemes are based on a centralised model of cooperative spectrum sensing. However, gaps still exist in the infrastructure-less CRNs.

Performance of various algorithms, based on the use of a fusion centre were evaluated in [4]. Spectrum sensing data falsification (SSDF) attacking nodes is being proven to be very difficult to be detected by those schemes. The standard and p-nom energy detector algorithm was assessed under the supposition that a Gamma and Gaussian distribution of the test statistics was implemented. The comparative results demonstrate that the Gaussian assumption for distribution of test statistics performs better in fighting the SSDF attack when compared to the Gamma assumption. The experiment was carried out with the assumption that the network is populated with a very small percentage of attacking nodes. It is not guaranteed that the algorithm will perfume better in a network with higher percentage of malicious users.

In [17], SSDF attack mitigation scheme which is based on the hard decision technique is proposed. The scheme uses the Gaussian approximation of Binomial distribution to detect and isolate MUs participating in cooperative spectrum sensing (CSS). The scheme is evaluated in a network populated with 50 nodes; hence its robustness may be evaluated in larger networks. The scheme might not function very well in a less-populated network. Our work looked at a network topology with a population ranging from 10 to more than 50 nodes.

In [6], schemes designed to counter a number of different classes of attacks which are based on the prior knowledge of the cognitive radios are proposed. The schemes detect and isolate the malicious reports. The use of the weighted sensing fusion mechanism in CRNs can reduce the impact of attacks in cognitive radio [6]. The assumption that the network has only five adversary nodes does not assess the effectiveness of the scheme when the number of MUs is increased.

extension of generalised extreme studentised deviate test algorithm is proposed by Srinu and Mishra [18], to combat the effects of malicious secondary users in the cognitive radio network environment. The proposed scheme can only function in the network with a fusion centre. The scheme detects MUs using the Shapiro–Wilk test and it is effective in detecting and isolating the Byzantine attacks, however, it is a centralised CSS based scheme. We are trying to close the gap which exists in completely decentralized network environment by addressing the problem of Byzantine attacks on a decentralised CRN. This proposed algorithm is the base of our research as they have used extreme studentised deviation test approach to solve the problem.

Novel multi-attribute trust-based framework which facilitates dependable spectrum sensing and priority-based spectrum access allotment to enhance delay sensitive data transmissions, is proposed in [19]. The effectiveness of this scheme in combating the SSDF attack was assessed. The simulation results has proven that the effectiveness of the scheme is 91.42%. The network is assumed to be populated with always-on attack and no any other kind of attackers. The reliability of the proposed solution when the attack possesses different attack behaviour might be unreliable. Our study will also use MATLAB to evaluate the projected solution under different kind of attacks.

In [20], a distributed cooperative spectrum sensing, and cheat-proof spectrum allocation strategy is proposed. Dynamic reputation model and the Vickrey-Clarke-Groves where combined and unfolded this strategy. It was proven using through the analytical and simulation results that the proposed scheme can detect and isolate SSDF attack in

CRAHNs. The performance of the proposed strategy was evaluated against a distributed random scheme and the results show that it is superior [21].

Novel trust-aware gossip-based scheme is proposed to work in a distributed cognitive radio networks and it is Sayed to improve significantly CSS in the presence of malicious users [22]. Push-sum protocol is the bases of this scheme and it is a novel consensus-based [23]. Using gossip, the average of the values stored by each node is calculated and the storing of these values is achieved by push-sum protocol. Gossip protocols are distributed algorithms where every node transmit its value to a random node at a given time step. They incorporated trust score into the original push-sum algorithm to make it resilient to SSDF attack.

The goal of every node is to detect its neighbour's trustworthiness and ignore the report from them. Furthermore, the study proved that consensus-based systems are more vulnerable to SSDF attacks. It is evident that the proposed scheme significantly improves the detection performance in the presence of malicious nodes. This scheme might cause delay due to the convergence process. The proposed scheme was simulated considering a location area within a range of single primary users. We were also assuming and evaluating our proposed scheme considering a location area within a range of single primary users.

Two block outlier detection methods, based on Tietjen-Moore (TM) and Shapiro-Wilk (SW) tests, are proposed to mitigate the effect of malicious users in CSS [24]. box plot and median absolute deviation (MAD) tests are compared to the proposed mitigation scheme. The robustness of TM and SW against statistical and random attack is proven against box plot and MAD tests. A new type of attack was proposed, called cooperative SSDF attack, which involves cooperation among malicious users. Monte Carlo simulations is used to show that the largest gap and clustering method fail to precisely estimate the number of outliers in cooperative attack. Thus, to overcome this shortcoming, they propose a modified largest gap method which can accurately estimate the number of outliers under cooperative attack.

Cooperative spectrum sensing (CSS) scheme according to an identity-based threshold key management for MANET is presented in [25] to combat SSDF attack in CR-MANET and it is named S-CRAHN. The proposed scheme doesn't need continual repetition and long convergence time like in consensus-based schemes. Also, it is shown through simulation that by selecting threshold in S-CRAHN, false alarm probability is reduced when compared to the consensus-based scheme suggested in [26]. Due to the fact that C-CRAHN uses binary string instead of contributing signal transmission with various distribution: delay, energy consumption and common control channel are decreased due to this procedure. S-CRAHN is seen to be a good scheme since it can combat the attack and at the same take into consideration energy consumption. [27] emphasised the fact that previous work in literature did not consider the preservation of energy when designing their schemes.

Ref. [28] proposed a neighbour detection-based spectrum sensing algorithm in CRAHN to defence against SSDF attack. The algorithm is optimised to detect malicious users by the help of neighbours during spectrum sensing to improve decision making accuracy. The algorithm removes the suspicious nodes based on their data variation and adjusts trusted neighbour nodes when the set is being altered to maintain the connectivity. The good part of this algorithm is that it also solves the issue of connectivity after they have removed a suspicious user from the network topology and it can reach unified sensing results quickly. They have used energy detection as their spectrum sensing technique and focused on CRAHN, that's what makes their work complementary our work. Our proposed scheme makes use of energy detection spectrum sensing technique, because of its simplicity.

A threshold-based detection strategy, named collaborative detection strategy (CODES) is proposed in ref. [29] to act against SSDF attack in centralised CRN. CODES can detect SSDF attacks in the network with varying SU density, malicious user density and PU activity. PU activity probability is being utilised by the algorithm to set the threshold to detect malicious users. CODES stand out in contrast to state-of-the-art strategies, it uses simple strategy for setting up a threshold values by the help of PU activity probability, it does not make use of any prior knowledge about the current network.

In [30], the discovery of mutual-aid collusive (MAC) attacks as the basis of their augment that securing CSS with only trust mechanism is reported be inadequate, and presented DMAC to thwart this kind of an attack. MAC attack falsifies sensing data to mislead spectrum availability decisions, by indicating that the PU is in use of its licenced spectrum band although the band is idling. A quick recovery to trust can be employed by MAC attackers to avoid being detected by trust mechanism. DMAC use “0-1” similarity measure to avoid such monopolization of the spectrum band. If the mechanism notes an irregularity in the trust values of SUs then the node is rendered as an attacker. The pros of this mechanism lie in the fact that it is not proven how effective it would be and whether it would thwart other types of SSDF attack. Our proposed scheme also takes in consideration the existence of always yes SSDF attack known as MAC attack in [30].

Joint spectrum sensing and resource allocation (JSSRA) scheme is proposed in [31] to deal with SSDF attack and to motivate secondary users to behave appropriately. The JSSRA scheme is being utilised in a centralised CSS. It is argued that the resource-allocating problem in the CRN with SSDF attacks is still an open issue. Hence, that forms the basis of the proposed scheme, which combats SSDF attacks and improves SUs sensing reliability which leads to fair resource allocation.

conditional frequency check (CFC) to counter Byzantine attack is proposed in [32], and the method is based on a Markov Spectrum Model. With the help of one trusted cognitive radio and a long detection window they claim that this global independent proposed scheme can accurately detect any malicious users, regardless of the number of attacking ones in the network. The is no need of prior knowledge of the radio spectrum for the scheme to function effectively.

The challenge within this method, is that when there is no sufficient detection window it does not perform very well. In our work, we are also making use of hard-decision malicious user detection.

In [33], a decision fusion technique is proposed in which all local spectrum sensing results are gathered and summed then it is contrasted to a threshold to detect an attack. Threshold value will be in the middle of 1 and the quantity of sensing terminals if the total is greater than or equal to the threshold then the result will be "Occupied" i.e., it indicates the presence of the licensed user. Otherwise, the outcome will be "free" i.e., it indicates the nonappearance of the licensed user. The issue with this technique is that using of fixed thresholds, expanding and decreasing the threshold has a major effect on the decision. Moreover, the method is ineffective in numerous situations that incorporate multiple attackers.

In [34], Weighted Sequential Ratio Test (WSRT) is utilised and the solution comprises of this 2 stages: a reputation maintenance step and a hypothesis test. In the reputation maintenance step, at first every node is assigned a reputation value equalling to 0, upon each accurate spectrum report the reputation value incremented by one. The second step depends on the Sequential Probability Ratio Test [35]. Different from ordinary SPRT, this WSRT approach utilises a trust-based information fusion scheme. The disadvantage is that there are no analytical studies which have being done, however performance is good.

In [36] , a weight based fusion scheme is utilized to encounter the malicious node which transmits false detecting signals. It uses trust approach and pre-sifting procedures. They looked at two types of SSDF attacks, for example, "Always Yes" and the "Always No". The "Always Yes" type falsify the observed state of the spectrum and relay the information with says the is a presence of the licensed users and in this way increasing the likelihood of false alert. The other sort "Always No" advertises the absence of the licensed users and in this way decreasing the likelihood of identification. pre-filtering of the information of the relayed information is utilized to detect the presence of attacking nodes and assigning the trust factor to every user. It exhibits good performance result.

In [37] a detection mechanism that keeps running in the FC is proposed. The FC distinguishes the attacker by checking mismatches between their local decision and the worldwide decision and removes them from the information FC. It is strong against Byzantine attack and removes the Byzantine attacks in a short time-frame; however, it works only when an FC exists.

In [38] a Bayesian detection mechanism that requires the knowledge of prior restrictive probabilities of the local spectrum sensing results and furthermore, the knowledge of prior conditional probabilities of the last sensing results. There are a few combination cases that exist between these two cases either right or wrong and cost are assigned. A large cost is assigned to the wrong ones and a little cost is assigned to the right ones. The overall cost is calculated by the sum of every cost weighted by the probabilities of the corresponding cases. The disadvantage of this scheme is that when there exist an SSDF attacker initially the prior knowledge becomes untrusted, and thus the suggested detection mechanism becomes no longer optimal in terms of minimizing the overall cost. The simulation conducted on this paper they did not consider the case when is SSDF attacker dominate the network, our research is meant to check cases like when malicious users dominate the network.

In [39] a Neyman-Pearson Test that does not require the prior probabilities of final sensing or any cost related to each decision case is proposed. It needs to define either the maximum acceptable probability of a false alarm or the maximum acceptable probability of a missed detection. Another probability is minimised and the defined probability is acceptable. Yet, it requires a prior conditional probability of the local sensing.

In [40], the Correlation Based Secondary User Authentication is proposed; the proposed scheme validates the number of trusted users at the FC only and by so doing it becomes immune to spectrum sensing data falsification attacks. This security scheme assumes that there are two sorts of SUs; a trustful SU which shares the same sensing metric with the FC and a malicious SU which has no knowledge of the sensing metric and sending random falsified data to the FC. The idea of the proposed scheme is to verify the trustful

SU if its correlation with the sensing matric is greater than a specific threshold. However, the success of the proposed scheme is built upon the assumption that the global decision is correct, which may not be true when malicious sensors dominate the network.

In [41] identification technique of Byzantines Attack called Pinokio is proposed. The Misbehaviour Detection System (MDS) that keeps up a profile of the network's normal behaviour based on training data is utilized. The MDS identifies trouble making nodes by checking the bit rate behaviour. By protocol, the bit rate ought to change occasionally furthermore, be balanced by a node alongside, the bit rates between two nodes ought to demonstrate some correspondence, and the utilization of a low bit rate ought to happen over a narrow channel. Nodes not showing these characteristics are not acting in a way helpful for spectrum efficiency, as results they are suspect. They have assumed that the mobile nodes moves at a lower speed which is a challenge with this scheme, what if they move at a faster rate their association with the access point will changes quickly. This results in unstable traffic request of AP. It along these lines makes the systems default behaviour vacillate at a quicker speed, and statistical algorithms of MDS that rely upon default system behaviour might not work correctly.

In [42] authors propose a technique to react against control channel saturation with an alternative decision-making strategy based on gathered negotiation to ensure user's communication coordination. Basically, the paper presents a mathematical study of the resources required for channel negotiation for the network based upon the quantity of unlicensed users present and the current channel throughput. At the point when the common control channel usage approaches the point at which the extra allotment of resources to rendezvous channel negotiation will create a saturation condition, the network moves to the period of gathered channel negotiation. This method avoids the circumstance in which common channel saturation is reached, and there are no resources accessible for extra channel gathered transaction. Hence, the early channel examination and begin of negotiation keep the misuse of data transmission resources while the common control channel is saturated.

In [43] a detection mechanism is utilized to detect the attacker and it is based on the past reports. This algorithm detects the suspicious level of the unlicensed nodes in light of their past reports. It computes the trust values and the consistency values. Trust value indicator can viably differentiate honestly and the malicious user. At the point when a client turns bad then the trust value pointer reduces the trust value. In the event that the client acts gravely for few times then after a large number of good practices the trust esteem gets increased. If the bad behaviour is carry's on, then it is impossible to recover. The main disadvantage is that the scheme cannot be applied to multiple malicious users' scenario.

In [44], authors propose a unique robust algorithm to mitigate spectrum sensing data falsification attack, the algorithm engage SVDD in sensing procedure. The SVDD is a sort of one-class classification method based on Support Vector Machine which was proposed by Tax & Duin [45], this algorithm picks out attacking nodes from network and isolate them from spectrum assess decision making.It tries to differentiate the boundary around the target data by enclosing the target data within a minimum hyper-sphere. Motivated by the support vector machine the SVDD decision boundary is described by a couple of target objects, known as support vectors. Then the algorithm votes between trusted nodes to decide whether the spectrum is empty malicious node reports presence of PU, when the PU is absent. The algorithm is very memory consuming because it employs SVDD to help in the sensing procedure. On their simulation, they kept the number of node constant throughout the experiment which may lead to the wrong conclusion. This paper leads us to the use of different scenarios.

Paper [46] proposed consensus-based cooperative spectrum sensing scheme to counter SSDF attacks in CR-MANETs. The scheme is based on recent advances in consensus algorithms [47], that which was magnified by a self-organizing behaviour of animal groups such as fish. Unlike the existing schemes, there is no need for a common receiver to do the data fusion for reaching the final decision to counter SSDF attacks. Concerning the secure spectrum sensing models, the basic requirement is for the secondary users to collectively filter out falsified data inserted by SSDF attacks and make the correct decision about the presence of primary users, which can be viewed as a typical multi-agent coordination situation. Using the consensus of secondary users, the proposed scheme can differentiate the trustworthiness of spectrum sensing terminals, which makes it more robust against SSDF attacks. Moreover, a common receiver is not needed for the final decision in the proposed scheme.

The limitation of this scheme is that it won't function well when SU's fails to collectively filter out falsified data inserted. In their paper, they simulated the proposed scheme and centralised decision fusion scheme after they found that the proposed one is performing best which is the focus of our research to compare the recently proposed schemes.

Authors of paper [48], collaborative malicious user detection during spectrum observation stage is proposed. BL value which indicate the trustworthy of cognitive radio to participate in sensing phase is attached to SUs. Cognitive nodes relay their spectrum observation information to their neighbours and cluster head (CH). The sensing behaviour of cognitive radios are monitored and reported to CH where there is superior authority to cut off misbehaving cognitive radios. Normal behaving cognitive radios are allowed to participate in spectrum observation phase and to use the available spectrum band, hence alleviate spectrum underutilization.

3.3 Conclusion

Research in cognitive radio networks has received great attention recently. A major thrust in this research area is the development of spectrum sensing mechanisms which are capable of accurately detecting the existence of licensed users or spectrum opportunities. From our extensive literature survey, we conclude that the cognitive radio ad hoc networks need more research in the area of security to achieve dynamic spectrum access and alleviate the inefficient spectrum utilization. In dynamic spectrum access networks, the sharing of spectrum occupancy information improves the spectrum access efficiency and minimizes the interference to the primary users. However, it is also important to detect and assess the trustworthy of nodes and the received data is not compromised, while facilitating the main operational objectives of cognitive radio networks.

Chapter 4

4.1 Introduction

In this research, a quantitative experimental approach was chosen whereby the experiments are performed using a simulator. In the experiments, several countermeasures designed to combat Byzantine attacks in cognitive radio adhoc network environments were simulated. The simulation experiments were conducted using a high-performance language for technical computing called MATLAB version R2015a [49]. MATLAB is configured to run on a Windows operating system (OS).

In the next section we present the design of our proposed scheme, followed by the system model and simulation environment. The network performance metrics used to evaluate the countermeasure in the simulation scenario are presented in the last section of this chapter.

4.2 PROPOSED COUNTERMEASURE: EXTREME STUDENTIZED COOPERATIVE CONSENSUS SPECTRUM SENSING (ESCCSS)

Having investigated a number of Byzantine attack countermeasures and evaluating their weaknesses and strengths, we proposed a new scheme called the Extreme Studentized Cooperative Consensus Spectrum Sensing (ESCCSS) scheme. Its name is adopted from the fact that extreme studentized deviate test was implemented in order to make the scheme more robust. Its robustness was evaluated and compared to the robustness of Attack-Proof Cooperative Spectrum Sensing (APSCC) against Byzantine attacks.

Our proposed extreme scheme is based on a cooperative spectrum knowledge whereby each node in the network is responsible for observing and constructing information about its immediate surroundings and sharing it with the rest of the nodes in the network through a common control channel.

A consensus algorithm assists in the sharing of data and the making of decisions about the availability of the spectrum band. ESCCSS is a cooperative spectrum sensing and a consensus-based scheme. Distributed spectrum sensing was proposed to address the problem of link and node failure.

Each SU shares its spectrum observations with its neighbours and the final decision about the availability of the spectrum are made by each SU based on the combined shared spectrum observations and its own observations through a consensus algorithm.

Hence, without any support from cognitive radio tower SUs unite in taking accurate global conclusion about the availability of the radio spectrum band. Spectrum observations are shared amongst SUs. Upon the termination of the algorithm, each SU individually makes a final decision about the availability of the spectrum, based on the final converged value obtained from the combining of the received observations from neighbouring nodes by the consensus algorithm. The proposed scheme can be summarised as follows:

1) At the first time step $k = 0$, each SU initially transmits its local observation to its neighbours that are connected to it at this time step. Resulting to this vector $b(k) = [b_1(k) \dots, b_m(k)]$

2) The received local observations are sorted in ascending order.

3) Each node estimates the number of falsified data denoted by u, at $k = 0$.

4) Each node computes the mean $\bar{x}$ and standard deviation s of the received local observation and its own observation.

5) Compute

$$R_j = \max_i \frac{|x_i - \bar{x}|}{s} \quad j = 1,2 \dots, u \tag{1}$$

6) After computing R_j, find the value of x_i that maximises $|x_i - \bar{x}|$

7) Remove x_i from the sorted local observations and repeat steps 2 to 6 with estimated outliers $j = u$ and k=1,…,K

8) exclude isolated data from participating in step 9 after declaring them (x_i's) as suspicious data

9) Subsequent to secluding adulterated data at each successive time step $(0 < k < \mathrm{K})$, each SU couple these observations, along with the received observations from past time steps, through a combining function which generates a new observation $b(k)$ [50]. This new observation is transmitted to neighbouring nodes at the current time step k. This can be mathematically expressed as:

$$b(k) = F(b(n), n = 0, \dots, k-1), \qquad 0 < k < \mathrm{K} \tag{2}$$

where $F(.)$ is the combining function.

10) When ($k = K$) consensus algorithm terminates, at this point each SUs takes a final decision individually about the availability of the spectrum. $b(K)$ is compared to a threshold value. This can be expressed as:

$$G = \begin{cases} 0, & b(K) < \alpha \\ 1, & otherwise \end{cases} \tag{3}$$

Where α is a threshold value.

At this stage SUs can correctly make use of the available spectrum, if the final decision is 0 it means the spectrum is available and unavailable otherwise. Figure 4-1 gives a graphical representation of the proposed scheme.

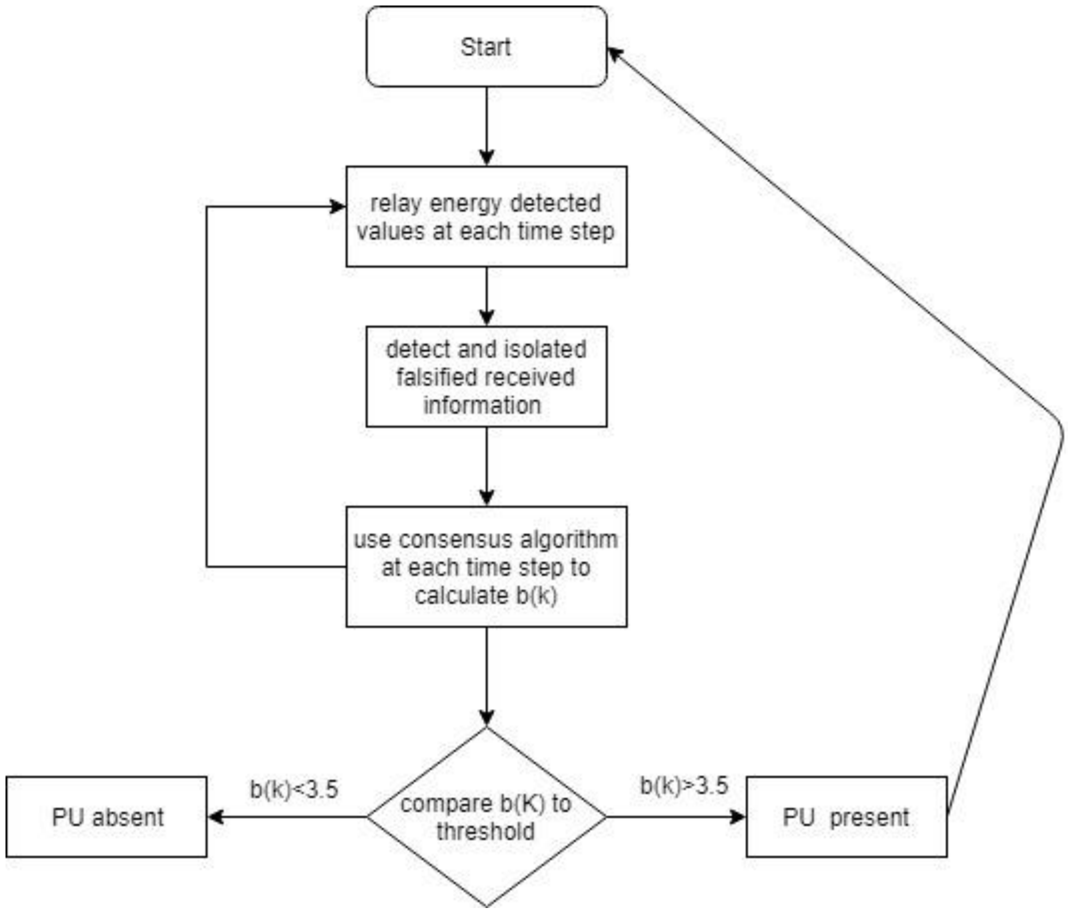

Figure 4-1: spectrum access decision making in the presence of malicious users

Figure 4 -1 present the flow chart of the spectrum access decision making by cognitive radios. Cognitive radios start by sensing the radio environment trying to locate spectrum holes. As the spectrum observation information sharing amongst cognitive radios commences the proposed scheme is triggered. The falsified information is detected and isolated while the consensus algorithm is running and combining all the information received by each cognitive radio, allowing all the secondary users to arrive at a consensus state. Finally, the converged information is compared to a threshold value resulting to a cooperative spectrum availability decision. Hence, if the spectrum is available the secondary users can transmit in that available band else the spectrum observation restart.

4.3 Evaluation plan

The network size and the number of malicious nodes in the network were considered in the simulation of this proposed scheme. The evaluation was done using different network sizes, from a small-sized network to a large-sized network, choosing the malicious nodes from 10%, 15%, 25%, and 40%. Simulation parameters are presented in table 1.

Table 4-1: List of parameters

Parameter	Setting
Antenna type	OmniAntenna
MAC protocol	IEEE 802.11 with extension to support CR networks
Data channel	8
Common control channel	1
Channel data rate	11 M bits/s
Number of Sus	10, 15, 25,50,100
Number of selfish SU	10%,15%,25%,40%
Propagation model	TwoRayGround
Grid size	1000m * 1000m
Primary user detection type	Energy detection
Mobility type	Random waypoint model
Sensing type	Cooperative spectrum sensing
Threshold α	3.5

The MATLAB simulation tool was used in this research because it has been effectively used by previous researchers in similar areas of study. It had the necessary tools needed to effectively simulate the proposed scheme. MATLAB works best with Windows operating systems; thus it was installed on a computer with a Windows 10 operating system.

Spectrum sensing can be conducted in one of two ways, cooperatively or non-cooperatively. Cooperatively is where the SUs sense the spectrum band and share the information with each other before making the final transmission decision. Non-cooperatively, where a SU senses the spectrum band and makes the decision on its own. In this research, we focused on cooperative spectrum sensing because it is more effective than non-cooperative spectrum sensing.

4.4 Performance Metrics

The metrics used to evaluate the proposed scheme were the success probability, missed detection probability and false alarm probability which are given by the following equations:

Let $DSUs$ be the detected SUs and $TSUs$ be the total number of SUs. The false alarm probability is given by:

$$\boldsymbol{FAp} = \frac{DSUs}{TSUs} \tag{4}$$

Let TA be Total attack and AD be attacks detected. The missed detection probability is given by:

$$MDp = \frac{TA - AD}{TA} \tag{5}$$

Let AD be the attacks detected. The success probability is given by:

$$Sp = \frac{AD}{TA} \tag{6}$$

The probability of false alarm is the probability that a channel is occupied by PUs $(H0)$ while it is not. This is denoted by:

$$Pf \text{ or } P(H1|H0) \tag{7}$$

The probability of missed detection is the probability that a channel which is occupied by PUs is detected to be idle $(H1)$. This is denoted by the following:

$$Pd \text{ or } P(H0|H1) \tag{8}$$

4.5 Conclusion

This chapter has discussed the simulation tools and simulation parameters that were used. Extreme studentized cooperative consensus spectrum sensing where elaborated along with performance metrics that were used to test the robustness of the proposed scheme. The number of nodes chosen for simulation were 10, 15, 25,50 and 100. This varying number has been chosen to evaluate the performance of the proposed scheme in a small-sized network, a medium-sized network and a large-sized network. Matlab was chosen as the simulation tool. Different scenarios considered for the simulations are discussed in next chapter

Chapter 5

5.1 Introduction

The main objective of this chapter is to evaluate the performance of the proposed Byzantine attack mitigation scheme, the ESCCSS, with Attack-Proof Cooperative Spectrum Sensing (APSCC) [51]. APSCC is a scheme which is closely related to our work. They have designed it utilizing the consensus algorithm and it is optimised to work in an ad hoc cognitive radio networks. It is proven to be the best scheme compared to its simulated equivalent. Hence, we chose to compare it to our proposed scheme.

A number of simulation scenarios were considered in this evaluation. The size of the different networks and the percentages of attacking nodes ranged from 10 to 100 nodes and 10% to 40% respectively. We evaluated their performance based on the following metrics: probability of false alarm, missed detection and success probability.

The performance of our scheme when combating different kinds of Byzantine attacks in different sizes network was extensively examined.

The evaluations were carried out using the following procedure:

1. MATLAB 2015b was installed on a Windows 8.1, 64-bit operating system.
2. The network was designed on an area of 1000 square metres.
3. Results were recorded, analysed, and graphically represented using MATLAB.

5.2 False Alarm Probability

In this section we present and discuss the probability of false alarm obtained through MATLAB experiments. The results show that our proposed mitigation scheme significantly reduces false alarm probability (FAP) compared to the APCSS scheme. The main interest was evaluating how much FAP the proposed mitigation scheme can achieve in combating Byzantine attacks as the network size increases compared to the APCSS scheme. Fig 5-1 shows the probability of false alarm in the networks with 10,15,25,50 and 100 nodes, where 10% of total nodes were malicious nodes.

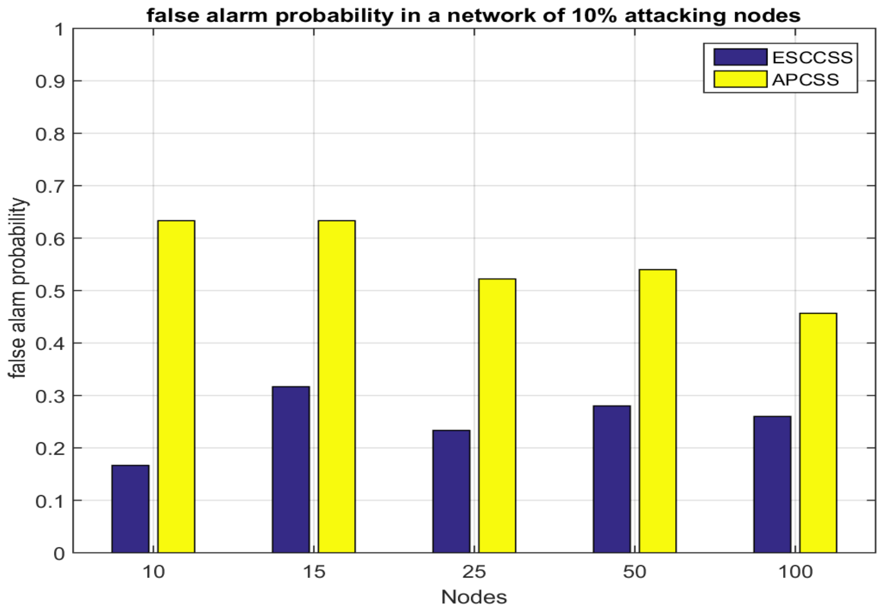

Figure 5-1: False alarm probability with 10% attacking nodes

In Figure 5-1, the alarm probability in a network with 10% malicious nodes is shown. The results show that in all the considered scenarios our proposed scheme significantly reduced FAP compared to APCSS. When N=10 and one of those nodes is an attacker, ESCCSS achieved a significant reduction of FAP. In Figure 5-2, where there 15% of the nodes are attacking nodes, ESCCSS also achieved good results. The proposed scheme isolate all the suspected falsified information from the final decision making, while APCSS isolated the suspected data based on the following expression $(\mu_i(k) - \gamma_c)(\mu_i' - \gamma_c)<0$ which sometimes failed to make correct decision which, ultimately result in failure to reduce FAP sufficiently.

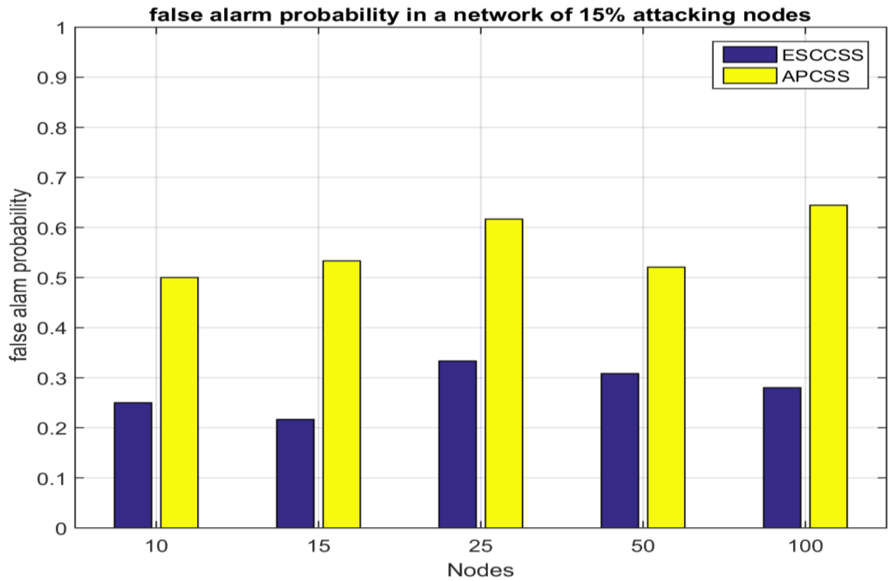

Figure 5-2: False alarm probability with 15% attacking nodes

As the number of attacking nodes were increased to 15% in scenarios with different network sizes, ESCCSS consistently reduced FAP when compared to APCSS, as shown in figure 5-2. The APCSS was outperformed by ESCCSS as it failed to reduce FAP significantly. FAP dynamically changes when the size of the network is increased. This is caused by the fact that our scheme isolates falsified data reported by malicious nodes. The performance results of our proposed scheme when the network is populated with 25% of the attacking nodes, are presented in figure 5-3.

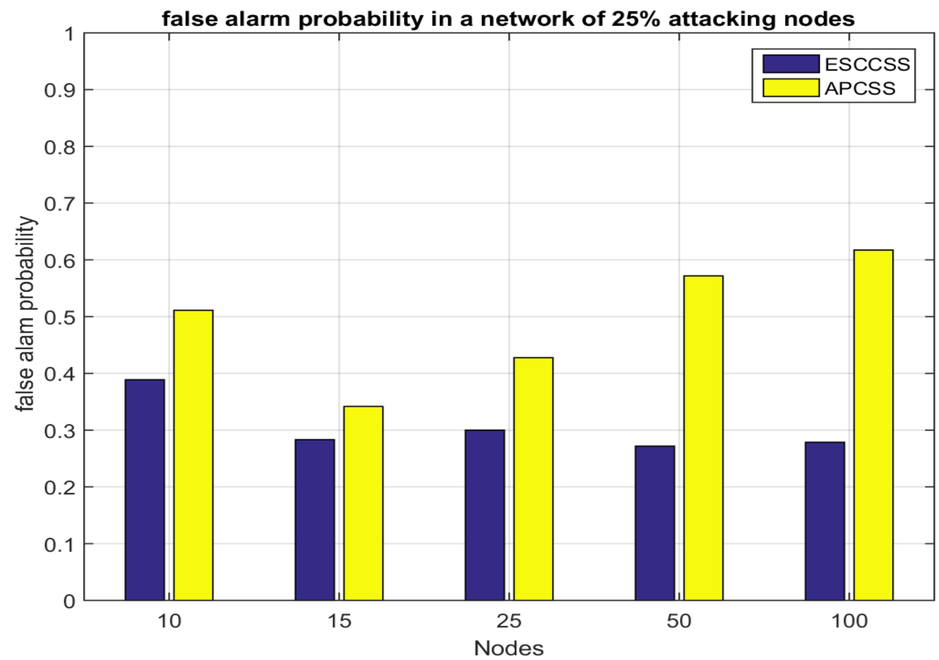

Figure 5-3: False alarm probability with 25% attacking nodes

The ESCCSS scheme outperformed the APCSS based on consensus algorithm scheme marginally in scenarios in networks with 10, 15, and 25 nodes. It outperformed the APCSS with a significant margin for network sizes with 50 and 100 nodes as shown in Figure 5-3. As the network size increased, FAP decreased for ESCCSS while it increased for APCSS. The poor performance of APCSS can be attributed to its failure to detect and isolate all the malicious data while ESCCSS was able to detect and isolate all the suspected data. Figure 5-4 shows that the performance of ESCCSS in the network with 40% of attacking nodes is degraded by the increasing number of attacking nodes.

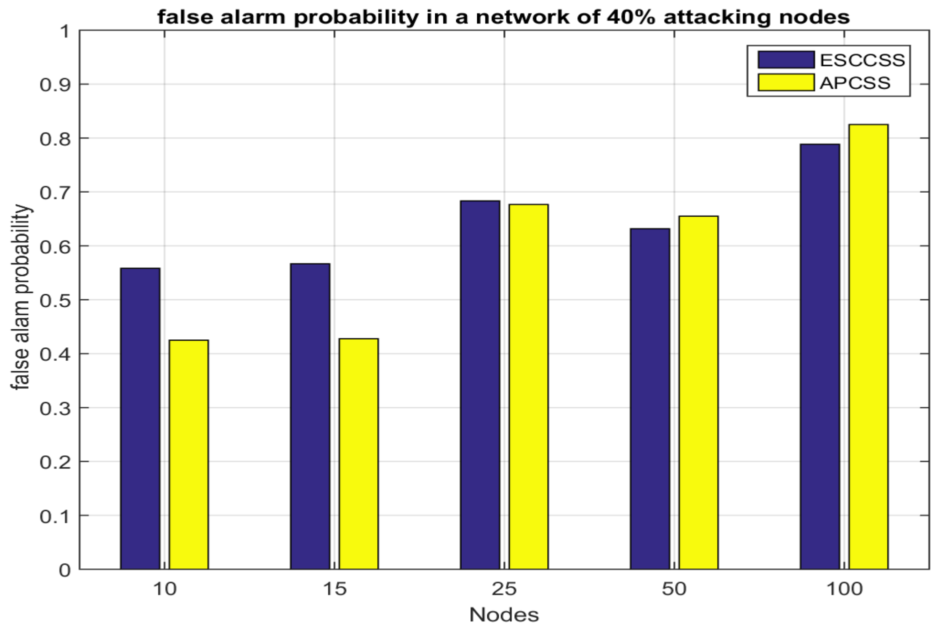

Figure 5-4: False alarm probability with 40% attacking nodes

Fig 5-4 shows that overall, the extreme studentized cooperative consensus spectrum sensing scheme was outperformed by APCSS when the network size was small (10,15 and 25 nodes) and with 40% of attacking nodes. The number of instructions to be executed has a fundamental role to the behaviour of ESCCSS in a network consisting of 40% attacking nodes. ESCCSS has less instructions to execute which enabled it to identify more falsified data and cut it from dissension making, while APCSS has more instructions to execute resulting in less false alarm reduction compared to ESCCSS in the network size of 50 and 100.

5.3 MISSED DETECTION PROBABILITY

Missed detection of malicious users by our scheme was compared to the attack-proof cooperative spectrum sensing (APCSS) scheme [42] and our findings are presented in this section. MD occurs when a primary user makes an actual transmission but SUs decide that the spectrum is idling. Figure 5-5 presents the missed detection probability in a network comprising of 10% of malicious users.

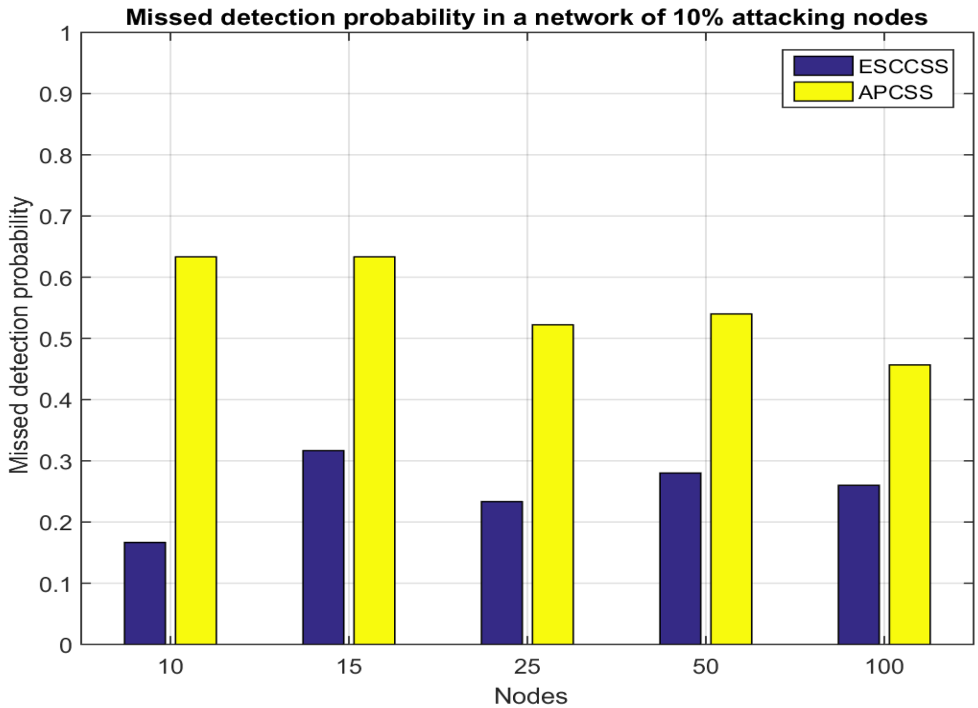

Figure 5-5: Missed detection probability in a network with 10% attacking nodes

A reduced missed detection probability is desirable for a good performing scheme as in Figure 5-5. ESCCSS significantly outperforms APCSS. As the network size increased, ESCCSS reduced the MDP when compared to APCSS. When the network size was too small (10 and 15), APCSS records a very high MDP (0.63) and ESCCSS significantly reduced MDP by 0.45 and 0.3 respectively. ESCSS does not record 0% missed detection, since the attacking nodes does not falsify all the sensed data, ESCCSS does not discard all the data from the malicious node, only the falsified data. Always yes attacks falsified the data in cases where it observed low primary user signal and always no falsified attacks sensed high primary user signal. The proposed records law missed detection probability because extreme studentized deviate test was implemented and it managed to detect all of the outlying data. Figure 5-6 presents the simulation results of extreme studentized cooperative consensus spectrum sensing compared to the simulation results of APCSS when looking into the probability of missed detection.

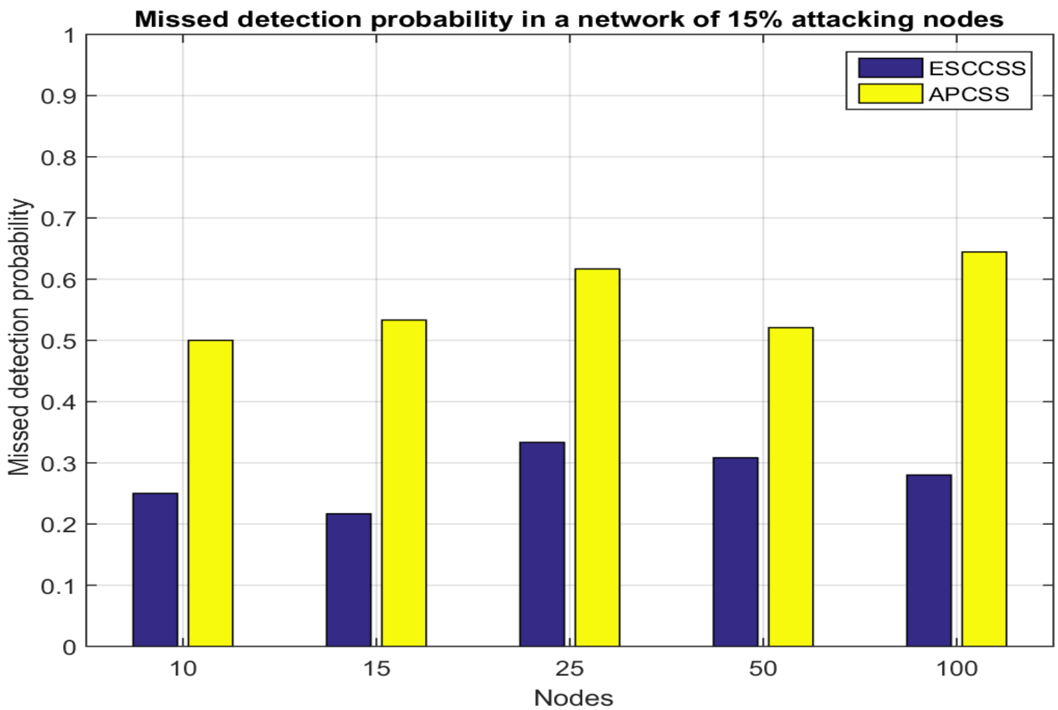

Figure 5-6: Missed detection probability in a network with 15% attacking nodes

Through simulations, positive results were achieved for extreme studentized cooperative consensus spectrum sensing compared to APCSS in a network comprising of 15% of malicious users as showed in figure 5-6. It is evident that as the network size increased, ESCCSS continued to have an upper hand when compared to APCSS. Throughout different network sizes, ESCCSS continued to record MDP less than 0.36 while APCSS recorded MDP above 0.49. APCSS failed to correctly isolate and identify all of the falsified data due to this criterion $(\mu_i(k) - \gamma_c)(\mu_i' - \gamma_c)$<0. When the network comprised of 15% attacking nodes, we can conclude that ESCCSS performed better. MDP recorded by ESCCSS is compared to APCSS in networks of different sizes with 25% of attacking nodes is presented in Figure 5-7.

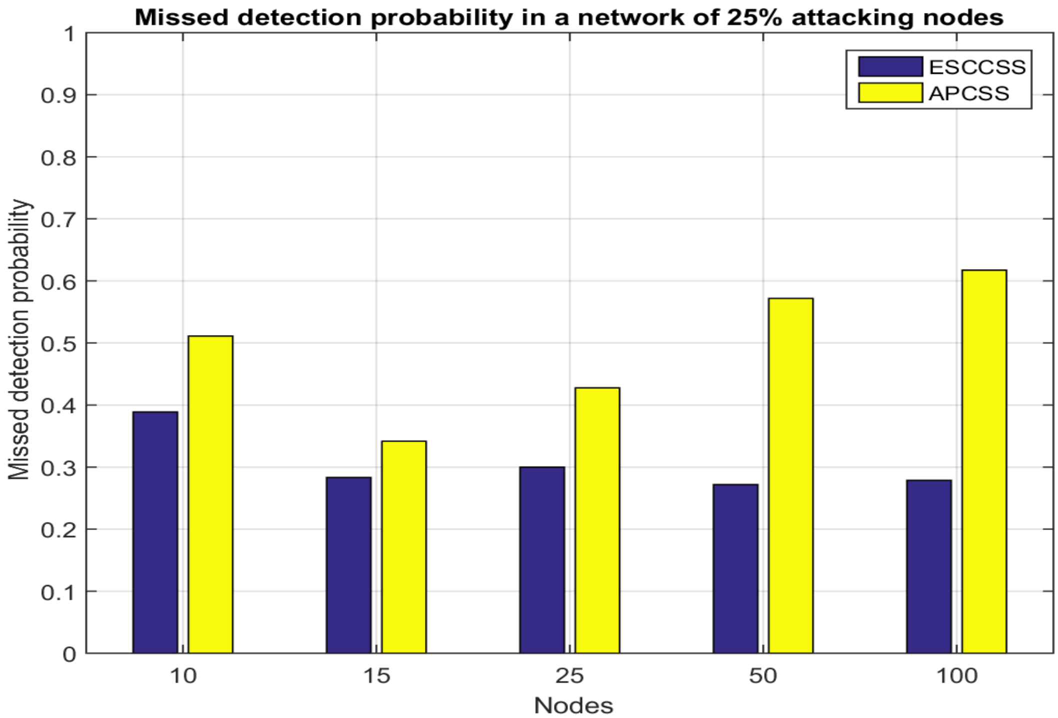

Figure 5-7: Missed detection probability in a network with 25% attacking nodes

When the network size is small (10 to 25 nodes) ESCCSS records a slight difference of MDP compared to APCSS as shown in Figure 5-7. As the network size is large, the proposed scheme reduced MDP with a high factor compared to the APCSS scheme. ESCCSS is more efficient when the network size is large and that network is comprised of 25% of attacking nodes. This is prompted by the fact that at this point, the proposed scheme can still detect and isolate most of the falsified data while APCSS fails to detect even at least 50% of falsified data. Outliers are more visible in the case where there is a larger data set and the extreme studentized deviate test is able to detect those outliers easily. Figure 5-8 presents the performance results of our proposed scheme in networks comprising of 40% of attacking nodes.

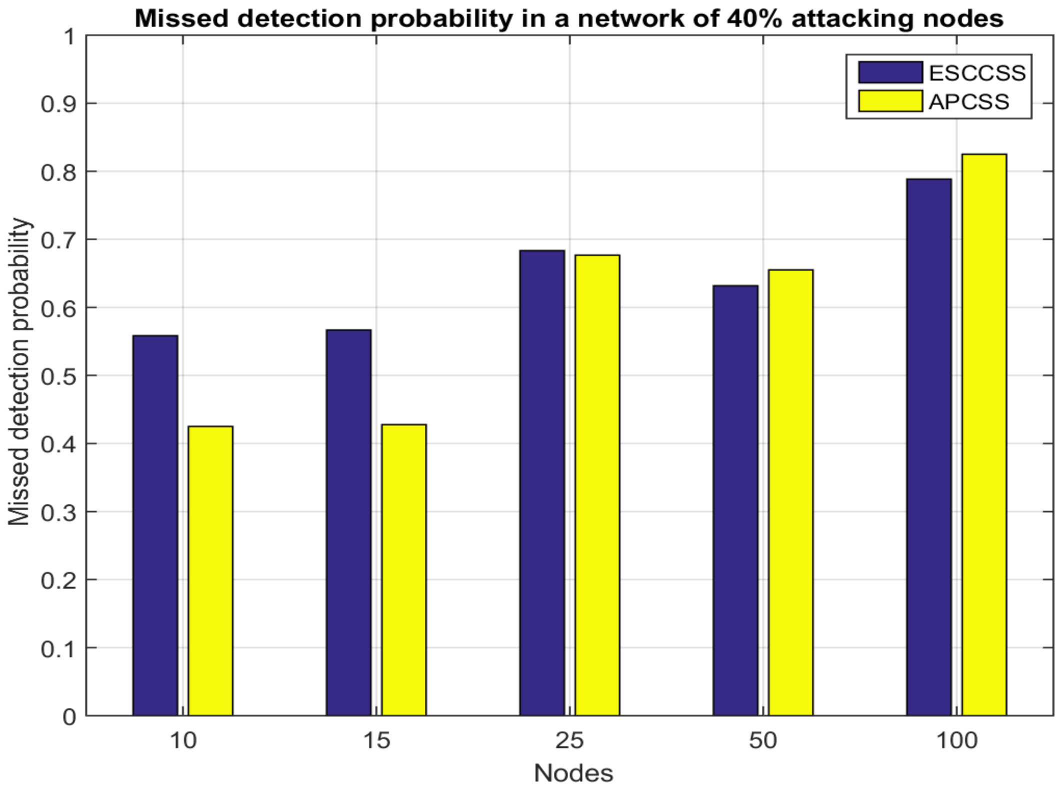

Figure 5-8: Missed detection probability in a network with 40% attacking nodes

When the network size is small (10-25 nodes) and the malicious nodes make up 40% of the total nodes, extreme studentized cooperative consensus spectrum sensing was out-performed by APCSS evident in figure 5-8. In large networks with 40% of malicious users, ESCCSS performed marginally better than APCSS. The lesser the instruction executed, the better the performance of ESCCSS in a large network size with 40% of malicious users. ESCCSS has a fewer instruction to execute compared to APCSS.

5.4 SUCCESS PROBABILITY

This section presents the detection rate of the proposed scheme in detecting the malicious users. Figures 5 -9 to Figure 5 -12 shows the comparative results of extreme studentized cooperative consensus spectrum sensing and attack-proof cooperative spectrum sensing based on consensus algorithm schemes. Figure 5-9 presents the success probability results of ESCCSS in networks with varying number of nodes. The number of attacking nodes was kept constant.

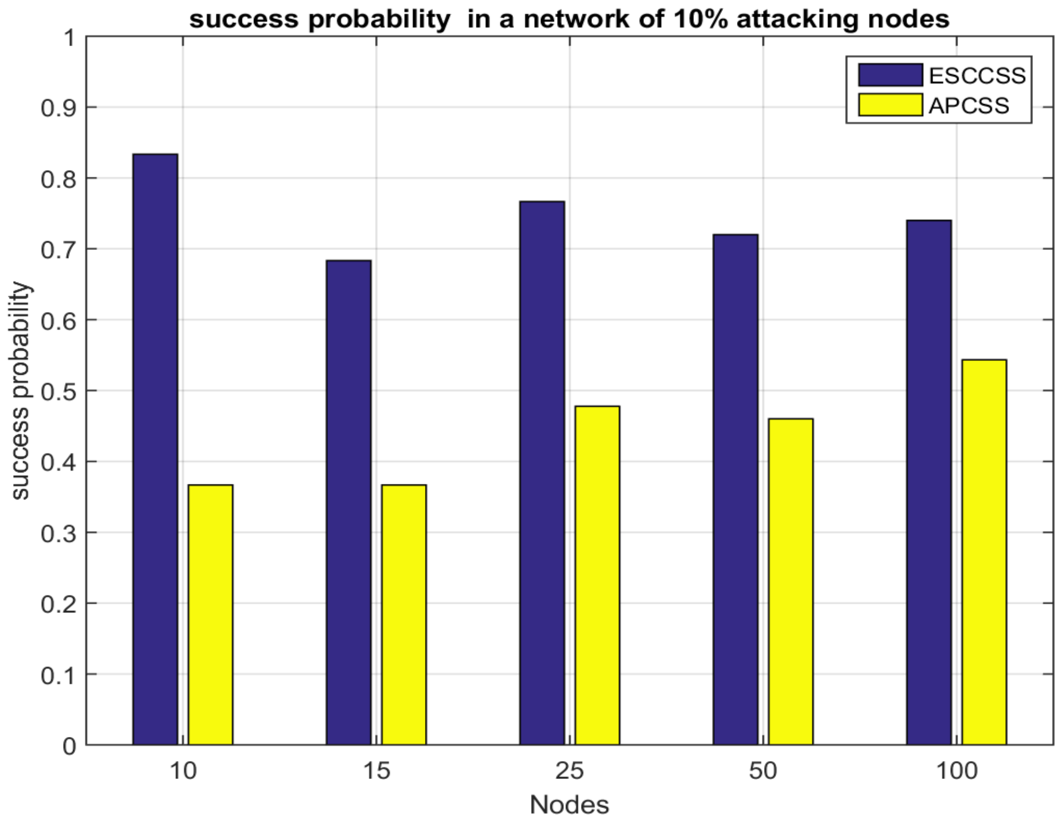

Figure 5-9: Success probability in a network with 10% attacking nodes

In a small network, the ESCCSS scheme detected a higher number of attacking nodes compared to APCSS as shown in Figure 5-9. As the network size was increased, the success probability of ESCCSS in general decreased, while APCSS's success probability increases. ESCCSS detected all falsified data and isolated them from spectrum availability decision making. The success probability was also investigated in a network scenario with 15% of attacking nodes. The results are presented in Figure 5 -10 for both ESCCSS and APCSS.

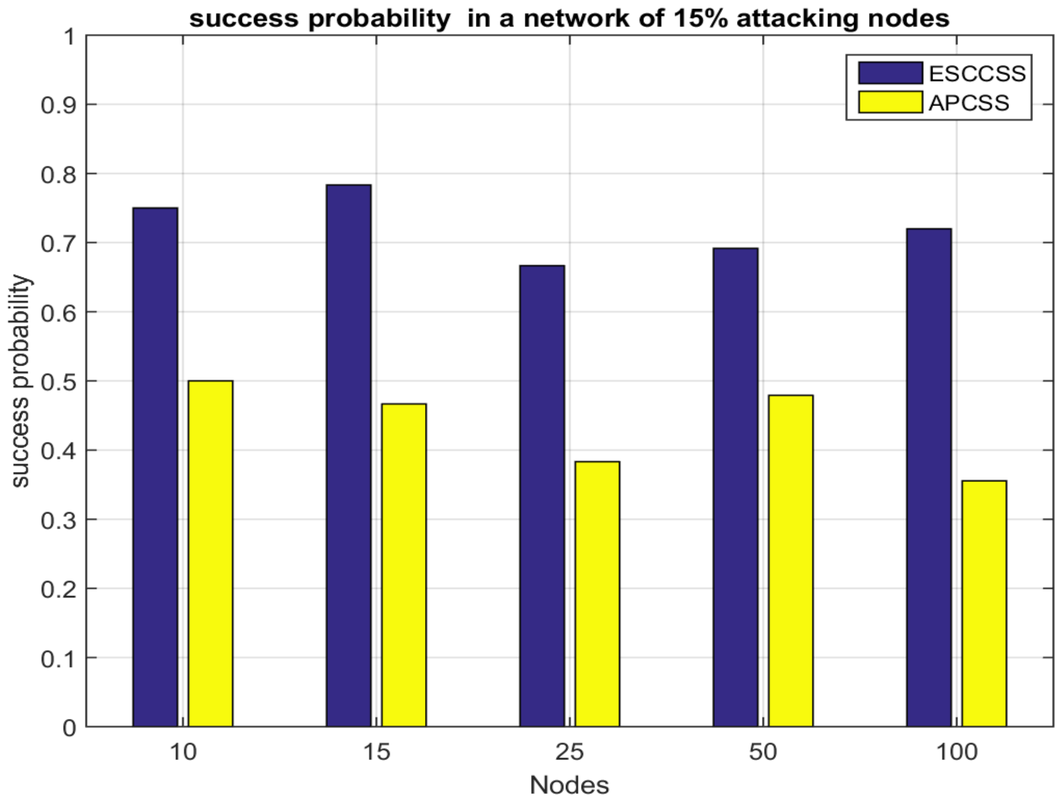

Figure 5-10: Success probability in a network with 15% attacking nodes

Figure 5 -11 shows that ESCCSS performed better in comparison to the APCSS. ESCCSS recorded the highest success probability when the number of nodes in the network were 15, and 2 of those nodes were malicious. The network size was populated with a reasonable number of malicious users and they were quickly detected by ESCCSS since it is configured to quickly detect the suspicious nodes. Fig 5-11 presents the results of the schemes when the percentage of malicious nodes were increased to 25% of attacking nodes.

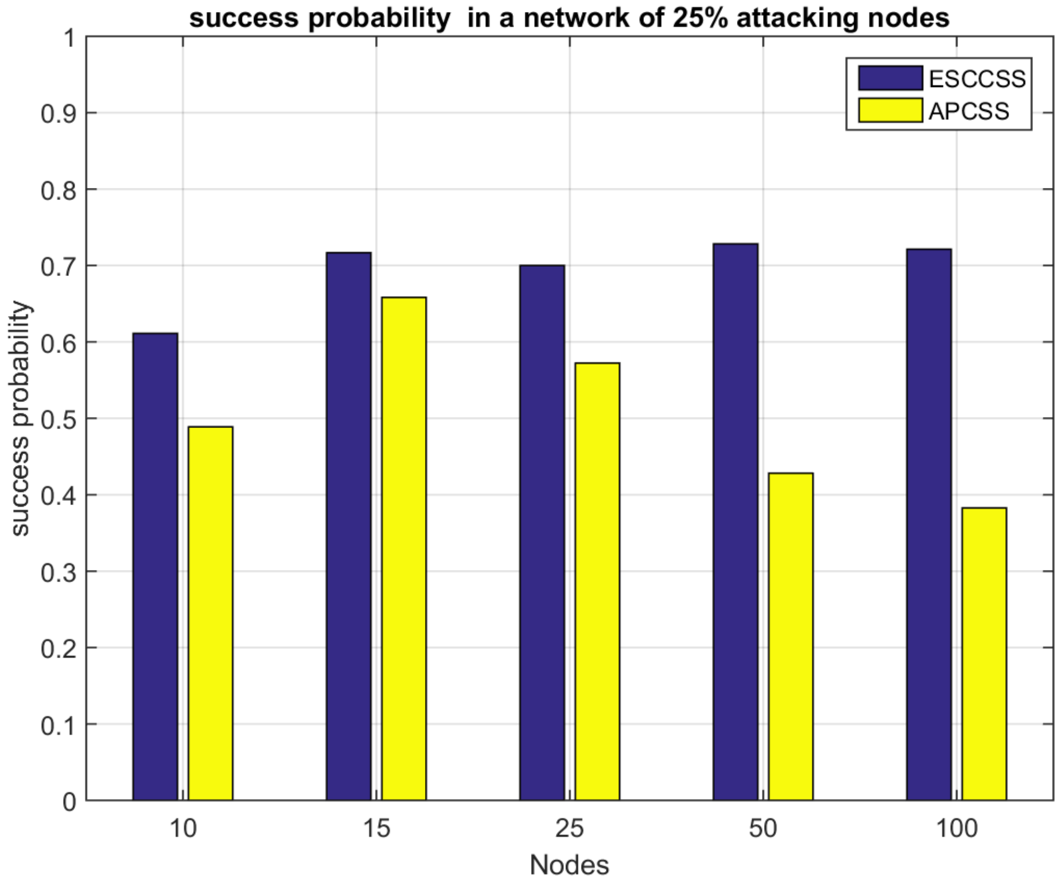

Figure 5-11: Success probability in a network with 25% attacking nodes

Fig 5 -11 shows that as the network size increases, the success probability also increases. It can be seen that when the network size is small, the performance of the two schemes is almost the same. In Fig 5-12, percentage of malicious nodes 40%.

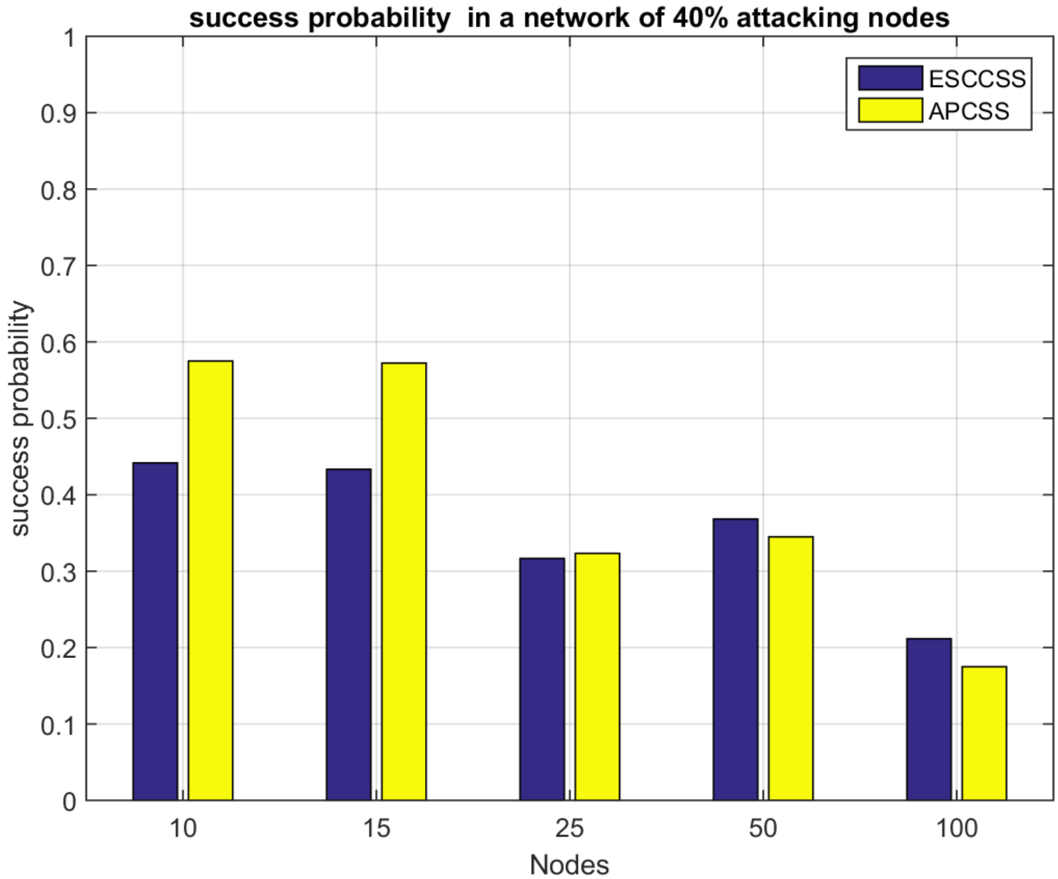

Figure 5-12: Success probability in a network with 40% attacking nodes

In fig 5-12, it can be seen that in the network size ranging from 10 to 25, the ESCCSS was outperformed by the APCSS. In larger networks, ESCCSS outperformed APCSS. We can conclude that as the network size is increases, the performance of the ESCCSS improves. Large network size allows ESCCSS to operate effectively because of the fact that the instructions to be executed are less compared to its simulated equivalent.

5.5 Explanation on the behaviour of Attack-Proof Cooperative Spectrum Sensing in a network populated with 40% of malicious nodes.

Figure 5-13 bellow fives a thorough explanation on the reason why the proposed scheme is performing badly in a network with 40% of malicious users.

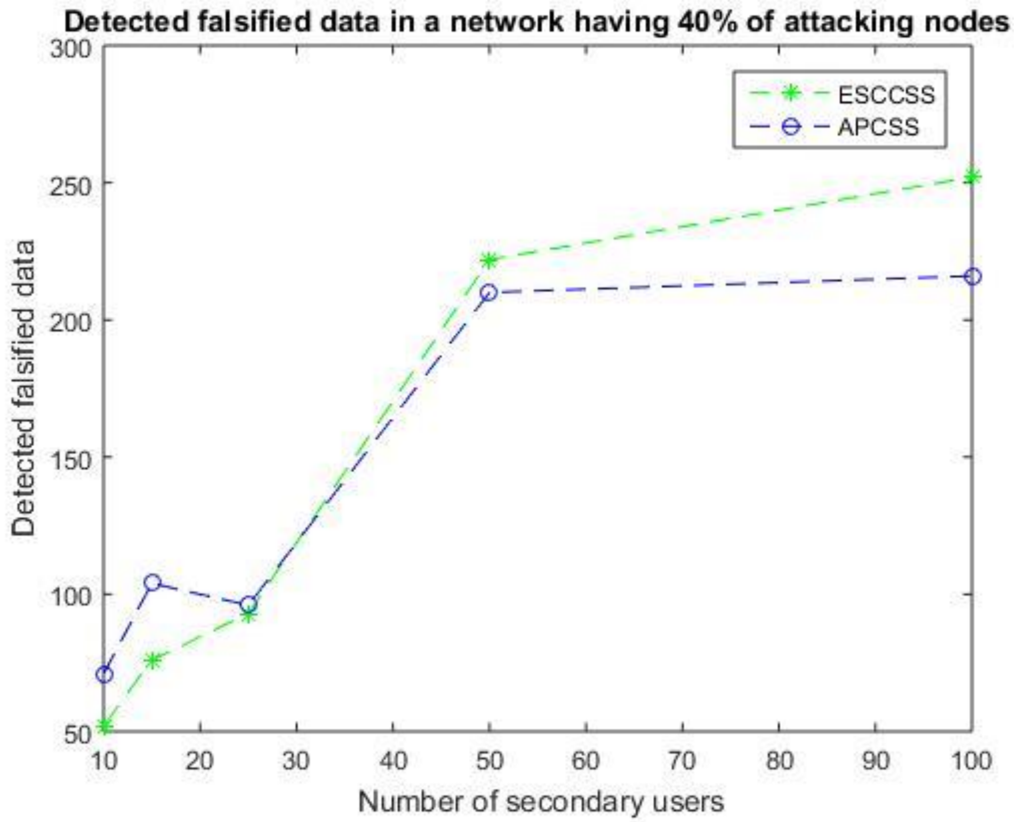

Figure 5-13: Undetected falsified data in a network having 40% of attacking nodes

Figure 5-13 proves what exactly transpires in a network populated with 40% attacking nodes. In a small network size, the numbers of instructions to be executed has no significant impact on the strength of the schemes, but the moment the size of the network increases, which means the number of attacking nodes also increases, APCSS becomes overloaded. This leads to reduction in its strength of detecting the falsified data. It is evident in figure 5-13 that as the network size become large ESCCSS detect more falsified data than APCSS because APCSS have more instructions to execute than APCSS.

5.6 Conclusion

The performance of ESCCSS was evaluated against the performance of the attack-proof cooperative spectrum sensing scheme. The two schemes were optimised to detect and isolate the malicious nodes. The simulation results show that ESCCSS performs better than the APCSS scheme when the percentage of malicious nodes is, at most, 25%. In networks with higher percentages of malicious nodes, ESCCSS only outperforms APCSS when the number of nodes in a network is at least 50.

Chapter 6

CONCLUSION AND FUTURE WORK

6.1 Introduction

The summary of the findings, contributions and final conclusion are presented in this chapter. There is a great notable improvement in technology and wireless systems. The advancement of wireless technology has led to spectrum scarcity. Thus, wireless communication devices need to share the available radio spectrum in an efficient manner without causing interferences to the PUs. Therefore, some regulatory bodies have had to revisit the spectrum allocation principles and allow SUs to opportunistically utilise the available spectrum allocated to licensed users by employing cognitive radios. Cognitive radio networks sense the radio spectrum, capture the information, and identify unutilised spectrum bands using cooperative spectrum sensing. Cooperative spectrum sensing is the process of identifying and sharing the unutilised spectrum bands cooperatively in ad hoc cognitive radio networks. However, traditional cooperative spectrum sensing techniques are vulnerable to Byzantine attacks which interfere with the cognitive cycle and mislead nodes for selfish reasons.

6.2 Summary of the Findings

The goal of this work was to design and implement a Byzantine attack mitigation scheme in cognitive radio ad hoc networks. The focus was to isolate nodes sharing falsified data regarding spectrum availability to mislead SUs in their spectrum access decision making.

The proposed statistical approach of isolating falsified data was integrated with cooperative spectrum sensing. The extreme studentized deviate test isolate data of outliers from the shared data set from all nodes at time K.

Based on the results of this study, we can conclude that the extreme studentized deviate test is a suitable candidate in combating Byzantine attacks. The simulation results shown that ESCCSS achieved a lower false alarm probability when compared to APCSS except for the scenario where the network is populated with 40% of MUs. The proposed scheme therefore successfully detects malicious data and outperforms the APCSS scheme. ESCCSS also achieved the lower missed detection probability when compared to APCSS.

6.3 Recommendations

There is a need for more research on the strategies which can be used to mitigate the effects of Byzantine attacks in order to allow cognitive radio networks to be deployed in situation where malicious users exist. In addition, there is a need to investigate other security issues which can be considered concurrently with Byzantine attacks, such as the primary user emulation attack in order to improve the performance of this technology. Forthcoming work should be based on designing mitigation schemes that can address the effect of Byzantine and primary user emulation attacks concurrently.

6.4 Final Conclusion

The core objective of this work was to design and implement the Byzantine attack mitigation scheme in cognitive radio ad hoc network. Although the scope of this research was limited to a network consisting of 10%, 15%, 25% and 40% attacking nodes, there is enough evidence from the simulation results which show that the extreme studentized cooperative consensus spectrum sensing scheme performs better than APCSS.

References

[1] J. Mitola and G. Maguire, “Cognitive radio: making software radios more personal,” *IEEE Personal Communications,* vol. 6, no. 4, pp. 13 - 18, 1999.

[2] R. Kaur and P. Chawla, “Analysis of Spectrum Sensing based on Cyclostationary Feature Detection and Access using OFDM and OWDM,” *International Journal of Engineering Development and Research ,* vol. 5, no. 1, pp. 466-474, 2017.

[3] A. E. Omer, “Various Sensing Techniques in Cognitive Radio Networks: A Review,” in *2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE)*, Khartoum, Sudan, 2015.

[4] N. Lavanis and D. Jalihal, “Performance of p-Norm Detector in Cognitive Radio Networks with Cooperative Spectrum Sensing in Presence of Malicious Users,” *Wireless Communications and Mobile Computing,* vol. 2017, no. 2, pp. 1-8, 2017.

[5] J. Lu, P. Wei and Z. Chen, “A Scheme to Counter SSDF Attacks based on Hard Decision in Cognitive Radio Networks,” *WSEAS TRANSACTIONS on COMMUNICATIONS ,* vol. 13, pp. 242-248, 2014.

[6] S. Sodagari, A. Attar, V. Leung and S. G. Bilén, “Combating channel eviction triggering denial-of-service attacks in cognitive radio networks†,” *TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES,* vol. 23, no. 5, pp. 454-465, 2012.

[7] H. Reyes and N. Kaabouch, “Improving the Reliability of Unmanned Aircraft System Wireless Communications through Cognitive Radio Technology,” *Communications and Network,* vol. 5, no. 3, pp. 225-230, 2013.

[8] F. Salahdine, E. H. Ghazi, . N. Kaabouch and F. W. Fihri, “Matched Filter Detection with Dynamic Threshold for Cognitive Radio Networks,” in *2015 International*

Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakech, Morocco, 2015.

[9] M. Sharifi, A. A. Sharifi and M. J. Niya, “Cooperative spectrum sensing in the presence of primary user emulation attack in cognitive radio network: multi-level hypotheses test approach,” *Wireless Networks,* vol. 24, no. 1, pp. 61-68, 2018.

[10] A. Attar, H. Tang, A. Vasilakos, R. Yu and V. Leung, “A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions,” *Proceedings of the IEEE,* vol. 100, no. 12, pp. 3172 - 3186, 2012.

[11] J. Mitola and G. Q. Maguire, “Cognitive radio: making software radios more personal,” *Cognitive radio: making software radios more personal,* vol. 6, no. 4, pp. 13-18, 1999.

[12] K. C. Chen, Y. J. Peng, N. Prasad, Y. C. Liang and S. Sun, “Cognitive radio network architecture; Part 1 – General structure,” in *Proceedings of the ACM International Conference on Ubiquitous Information Management and Communication*, Seoul, 2008.

[13] S. Aslam and G. K. Lee , “CSPA: Channel Selection and Parameter Adaptation scheme based on genetic algorithm for cognitive radio Ad Hoc networks,” *EURASIP Journal on Wireless Communications and Networking 2012(1),* pp. 1-15, 2012.

[14] T. Yucek and . H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” *IEEE Communications Surveys & Tutorials,* vol. 11, no. 1, pp. 116-130, 2009.

[15] Y. Zeng, Y. C. Liang, A. T. Hoang and R. Zhang, “A review on spectrum sensing for cognitive radio: challenges and solutions,” *EURASIP Journal Advances in Signal Process,* vol. 20, no. 1, pp. 1-15, 2010.

[16] D. Cabric, S. M. Mishra and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," *IEEE Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers,* vol. 1, pp. 772-776, 2004.

[17] J. Lu, P. Wei and Z. Chen, "A Scheme to Counter SSDF Attacks based on Hard Decision in Cognitive Radio Networks," *WSEAS TRANSACTIONS on COMMUNICATIONS,* vol. 13, pp. 242-248, 2014.

[18] S. Srinu and A. K. Mishra, " Efficient elimination of erroneous nodes in cooperative sensing for cognitive radio networks," *Computers and Electrical Engineering,* vol. 52, p. 284–292, 2016.

[19] U. S. Premarathne, I. Khalil and M. Atiquzzaman, "Trust based reliable transmissions strategies for smart home energy consumption management in cognitive radio based smart grid," *Ad Hoc Networks,* vol. 41, pp. 15-29, 2016.

[20] H. Lin, J. Hu, C. Huang, L. Xu and B. Wu, "Secure Cooperative Spectrum Sensing and Allocation in Distributed Cognitive Radio Networks," *International Journal of Distributed Sensor Networks,* 2015.

[21] L. Luo and S. Roy, "Analysis of search schemes in cognitive," *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor,Mesh andAdHoc Communications and Networks (SECON'07),* pp. 647-654, June 2017.

[22] A. Vosoughi, J. Cavallaro and A. Marshall, "A Cooperative Spectrum Sensing Scheme for Cognitive Radio Ad Hoc Networks based on Gossip and Trust," in *Signal and Information Processing (GlobalSIP), 2014 IEEE Global Conference on. IEEE*, Georgia, 2014.

[23] . D. Kempe, D. Alin and G. Johannes , "Gossip-based computation of aggregate information," in *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on. IEEE*, 2003.

[24] S. S. Kalamkar, K. P. Singh, and A. Banerjee, “Block Outlier Methods for Malicious User Detection in Cooperative Spectrum Sensing,” in *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th. IEEE*, 2014.

[25] Y. Cheng and J. Zhou, “S-CRAHN: A Secure Cognitive-Radio Ad-Hoc Network,” *HCTL Open Science and Technology Letters (HCTL Open STL),* vol. 6, 2014.

[26] H. Tang, R. Yu, M. Huang and Z. Li, “Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks,” *IET communications,* vol. 6, no. 8, pp. 974-983, 2012.

[27] V. Sucasas, S. Althunibat, A. Radwan, H. Marques, J. Rodriguez, S. Vahid, R. Tafazolli and F. Granelli, “Lightweight Security Against combined IE and SSDF Attacks in Cooperative Spectrum Sensing for Cognitive Radio Networks,” *Security and Communication Networks,* vol. 8, no. 18, pp. 3978-3994, 2015.

[28] P. Qingqi, L. Hongning and L. Xianjun, “Neighbor Detection-Based Spectrum Sensing Algorithm in Distributed Cognitive Radio Networks,” *Chinese Journal of Electronics,* vol. 26, no. 02, pp. 399-406, 2017.

[29] A. Taggu, C. Chunka and N. Marchang, “CODES: A COllaborative DEtection Strategy for SSDF in cognitive radio networks,” in *Proceedings of the Third International Symposium on Women in Computing and Informatics. ACM*, 2015.

[30] J. FENG, G. LU, Y. ZHANG and H. WANG, “Avoiding monopolization: mutual-aid collusive attack detection in cooperative spectrum sensing,” *Science China Information Sciences,* vol. 60, no. 5, 2017.

[31] H. Chen, M. Zhou, L. Xie, K. Wang and J. Li, “Joint Spectrum Sensing and Resource Allocation Scheme in Cognitive Radio Networks with Spectrum Sensing Data Falsification Attack,” *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY,* vol. 65, no. 11, pp. 9181-9191, 2016.

[32] H. Xiaofan and Huaiyu Dai, “A Byzantine Attack Defender in Cognitive Radio Networks: the Conditional Frequency Check,” in *IEEE International Symposium on information theory*, cambridge, 2012.

[33] Pandharipande, K. J.-M, M. D and J. B, “Wireless RANs: Technology Proposal Package for IEEE 802.22,” *IEEE 802.22 WG on WRANs,* 2005.

[34] C. Ruiliang, P. Jung-Min, H. Thomas and H. Jeffrey, “Toward Secure Distributed Spectrum Toward Secure Distributed Spectrum,” *IEEE Communications Magazine,* pp. 50-55, April 2008.

[35] Su, S. Yeelin and T. Yu, “A sequential test based cooperative spectrum sensing scheme for cognitive radios,” in *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, Cannes, 2008.

[36] P. Kaligineedi, M. Khabbazian and V. Bhargava, “Secure Cooperative Sensing Techniques for Cognitive Radio Systems,” in *2008 IEEE International Conference on Communications*, Beijing, 2008.

[37] A. S. Rawat, P. Anand, H. Chen and P. K. Varshney, “Countering byzantine attacks in cognitive radio networks,” in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, Dallas, TX, 2010.

[38] L. Lu, S.-Y. Chang, J. Zhang, L. Qian, J. Wen, V. K. N. Lau, R. S. Cheng, R. D. Murch, W. H. Mow and K. B. Letaief, “Technology Proposal Clarifications for IEEE 802.22 WRAN Systems,” *IEEE P802.22 Wireless RANs,* May 2006.

[39] J. Hillenbrand, T. Weiss and F. Jondral, “Calculation of detection and false alarm probabilities in spectrum pooling systems,” *IEEE Communications Letters,* vol. 9, no. 4, pp. 349 - 351, 2005.

[40] H. Jorg, W. Timo and J. Friedrich, “Calculation of detection and false alarm probabilities in spectrum pooling systems,” *IEEE Communications Letters,* vol. 9, no. 4, pp. 349 - 351, 2005.

[41] K. Tan, S. Jana, P. Pathak and P. Mohapatra, “On insider misbehavior detection in cognitive radio networks,” *IEEE Network,* vol. 27, no. 3, pp. 4-9, 2013.

[42] B. Reza, F. Mahmood, M. Seyed and N. Mirhoseni, “COMMON CONTROL CHANNEL SATURATION DETECTION AND ENHANCEMENT IN COGNITIVE RADIO NETWORKS,” *International Journal of Distributed and Parallel Systems,* vol. 3, no. 1, pp. 15-25, 2012.

[43] W. Wang, H. Li, Y. Sun and Z. Han, “Attack-proof collaborative spectrum sensing in cognitive radio networks,” in *Information Sciences and Systems*, Baltimore, MD, 2009.

[44] F. F, J.-A. Abbasi and B. R, “Detection of SSDF Attack using SVDD Algorithm in Cognitive Radio Networks,” in *Third International Conference on Computational Intelligence, Communication Systems and Networks*, 2011.

[45] D. Tax and R. Duin, “Support Vector Data Description,” *Machine Learning,* vol. 54, no. 1, pp. 45-66, 2004.

[46] Y. Richard, T. Helen, H. Minyi, L. Zhiqiang and M. Peter, “Defense against Spectrum Sensing Data Falsification Attacks in Mobile Ad Hoc Networks with Cognitive Radios,” 2009.

[47] W. Ren, R. Beard and E. Atkins, “A survey of consensus problems in multi-a gent coordination,” in *in Proc. American Control Conference 05*, Portl and, OR, June 2005.

[48] K. Mahmoud and A. Anjali , “A Collaborative Approach towards Securing Spectrum Sensing in Cognitive Radio Networks,” in *Procedia Computer Science 94*, 2016.

[49] E. Kaur and H. Kaur, “MATLAB as a Development Environment for Mathematics Functions & Graphs in GUI,” *International Journal of Computer Science and Communication Engineering,* vol. 1, no. 2, pp. 65-67, 2012.

[50] M. Seif, T. ElBatt and S. Karim , “Sparse Spectrum Sensing in Infrastructure-less Cognitive Radio Networks via Binary Consensus Algorithm,” in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Valencia, Spain, 2016.

[51] Q. Liu, J. Gao, Y. Guo and S. Liu, “Attack-Proof Cooperative Spectrum Sensing Based on Consensus Algorithm in Cognitive Radio Networks,” *KSII Transactions on Internet and Information Systems (TIIS),* vol. 4, no. 6, pp. 1042-1062, 2010.