THE DEVELOPMENT OF NOVEL PHYSICAL LAYER SECURITY ALGORITHMS TO MITIGATE COGNITIVE RADIO ATTACKS

Sasa Maric

Doctor of Philosophy (PhD)

MACQUARIE University

Department of Electronic Engineering
Macquarie University

March 2018

Supervisor: Associate Professor Sam Reisenfeld

ACKNOWLEDGMENTS

It has been a long journey, with many ups and downs. It is my great pleasure to acknowledge my deepest gratitude to Associate Professor Sam Reisenfeld for his guidance and help throughout my research. He has always advised me with wisdom and patience, even when I repeated my mistakes multiple times. Without his guidance this thesis would never have been complete.

I would like to thank my family for their continual support throughout my schooling and PhD journey. It has been a long journey and I could have never got anywhere without them.

Lastly, I would like to thank my beautiful girl Lana for always keeping a smile on my face. For always sticking by me, even when things did not go the way I had imagined. Your support means the world to me. You have always pushed me to be better and try harder.

STATEMENT OF CANDIDATE

I, Sasa Maric, declare that this report, submitted as part of the requirement for the award of Doctor of Philosophy at Macquarie University, is entirely my own work unless otherwise referenced or acknowledged. This document has not been submitted for qualification or assessment in any academic institution.

Student's Name:

Student's Signature:

Date:

ABSTRACT

Since the implementation of the first public-access networks, attackers have looked to take advantage of vulnerabilities in network security to gain an unfair advantage. In recent times, wireless networks have increasingly been integrated in our everyday lives. Science-fiction style automated homes and societies have increasingly become a reality. Today's wireless devices possess high cognitive ability, they dynamically adjust according to their environment and user preferences to ensure maximum comfort for their users. As a result, a global network of interconnected wireless devices has been growing exponentially for the past few decades. Previous radio-frequency spectrum allocation has failed to predict this growth, which has resulted in extreme congestion in some bands and low utilisation of others. Cognitive Radio, a collection of intelligent methods, is seen as the most promising solution. To increase efficiency they allow secondary users (users that do not have a regulatory right to use a frequency channel) to utilise allocated frequency bands when they are not being utilised by paying users (primary users). However, cognitive radio implementation has been delayed several times because of its susceptibility to a number of security attacks, specifically in the physical layer. As such, a taxonomy of new attacks has been identified, which could not be mitigated by standard security algorithms that were developed for conventional wireless networks. The primary aim of this thesis is to mitigate the effects of physical layer attacks in Cognitive Radio Networks(CRN). In particular, two attacks have been identified as the most serious threats to cognitive radio

security. These are a Primary User Emulation Attack (PUEA), which involves an attacker emulating the properties of primary users in order to gain an unfair advantage over other secondary users and a Spectrum Sensing Data Falsification Attack(SSDFA), during which an attacker intentionally manipulates messages containing spectrum sensing information in order to trick secondary users into miss-diagnosing the status of a primary user. In this thesis, we present a number of algorithms to combat the vast array of attacks within the physical layer. In particular we present a number of novel, highly effective, low computational complexity algorithms that can be implemented to completely eradicate these attacks and render them ineffective. Since many of the devices that make up a cognitive radio network have battery and computational complexity constrains, our objective was to develop mitigation algorithms that they are lightweight and can be implemented effectively.

Contents

List of Figures

Chapter 1

Introduction

1.1 Motivation

Advancements in wireless technology have led to revolutions in a number of disciplines. Scientists are able to track and monitor animal behaviour, predict the weather and monitor pollution among other things. Doctors are able to monitor the various vital signs of patients remotely, allowing for fast response in cases of emergency. Wireless sensors enable homes to form complicated networks dedicated to making us as comfortable as possible at all times. As we become increasing reliant on wireless technology in our everyday lives, concerns for privacy and safety become prevalent. In the past, we have seen the development of systems with little or no consideration for security aspects. These systems often rely on updates and revisions to rectify and patch up security concerns. This method of system design has serious implications in todays rapidly advancing world. As a result, many systems now require reliability and data integrity. Therefore, powerful algorithms need to be developed to effectively deal with these issues.

The radio-frequency spectrum is a finite resource. As such, as wireless technology continues to grow , congestion within the radio frequency spectrum becomes a serious issue. Part of the reason is that the spectrum allocation methods that were used in the early days of wireless network development were inadequate and did not take into consideration future growth. A study by the Federal Communications Commission (FCC) determined

that the free-to-use ISM bands are extremely congested, while the vast majority of licensed bands are severely under-utilised [4]. The Federal Communications Commission (FCC) has found that the licensed radio-frequency bands are idle almost 80% of the time [5]. These findings prove that the real problem lies in under-utilisation rather than spectrum scarcity. Therefore, to effectively solve this problem we must find more effective ways to utilise the available licensed spectrum bands. Cognitive Radio, a collection of intelligent methods designed to use the radio spectrum in an efficient and dynamic manner, has been proposed as a promising solution for the spectrum utilisation problem we are faced with as a result of the increase number of wireless devices around the world. However, its full implementation in practical systems has continuously been delayed because of a wide range of security concerns.

At the moment, spectrum allocation ensures that licenced users are assigned channels, exclusively. We denote this type of user as a primary user (PU). Unlicensed users who look to opportunistically use idle channels are denoted as secondary users (SUs) [4]. Within the Cognitive Radio framework, a secondary user is able to utilise any radio-frequency band as long as the primary user is idle. As soon as a primary user becomes active on a channel, all secondary users using that channel must immediately cease all transmission and vacate the band. It is essential that secondary users do not interfere with primary users. In fact, primary users must remain oblivious to the activities of the secondary users, with a minimal acceptable performance degradation. To prevent interference with the primary user, secondary users must continuously monitor primary user activity. Each secondary user periodically performs spectrum sensing, during which it scans the channel (using one of a number of spectrum sensing techniques) to determined whether the primary user is still idle. If the primary user is transmitting on the channel, all secondary users must vacate the band immediately. By allowing unlicensed use to utilise radio-frequency bands that were previously exclusively reserved for primary users, we are able to reduce congestion

and utilise unused spectrum effectively.

The dynamic nature of cognitive radio means that secondary users are able to monitor, sense and adopt to changes in the environment. Their flexibility allows them to harmoniously coexist with primary users. Successful implementation of cognitive radio rests on its ability to continuously monitor the radio frequency band and act quickly if primary users become active. This fundamental feature of cognitive radio is susceptible for exploitation by security attacks. If an adversary was able to mimic the properties of a primary user, they could trick secondary users into thinking that a primary user is active. According to protocol, secondary users would immediately vacate the channel making it available for the primary users. This would allow the attacker to use the entire radio-frequency band, uncontested. This type of attack is called a Primary User Emulation Attack (PUEA).

Attackers are able to reduce the overall throughput of a network very quickly by continuously performing a PUEA on a number of radio-frequency bands. Attacks on multiple channels can be done as part of a team or as a single attacker who is able to optimally distribute power over a number of channels. Similarly, the best methods for identifying and mitigating against PUEAs are based on cooperation between secondary users. It is very difficult for a single secondary user to reliably identify the presence of a primary user because of various transmission degradation factors such as channel fading and shadowing. With a number of secondary users working together we able to observe a number of perspectives which help develop an overall picture. Identification of the primary user can achieved a number of ways, but the most popular methods are based on localisation. Techniques using the Receive Signal Strength (RSS), Angle of Arrival (AOA), Time of Arrival (TOA) and Time Difference of Arrival(TDOA) are some of the most popular. Each has positive and negative aspects associated with it, the choice of localisation technique is largely dependent on the type of environment and the resources available.

Cooperative spectrum sensing is key in the mitigation of PUEAs. However, it too is susceptible to attacks by adversaries that look to gain an unfair advantage over legitimate users. Spectrum sensing data falsification attacks (SSDFAs) involve an attacker, posing as a legitimate secondary user, and falsifying spectrum sensing results in an attempt to trick legitimate users into misdiagnosing the status of the primary user. The effect of an SSDFA is twofold; either secondary users decide that the primary user is idle when the primary user is actually active, which causes interference, or secondary users vacate the channel thinking that the primary user is active, which allows the attacker to use the radio-frequency band uncontested. The mitigation of SSDFAs is seen as extremely important because of cognitive radio's reliance on cooperative exchange of information. The spectrum sensing phase is essential in ensuring that cognitive radio fulfills its mission. Therefore, it is often seen as a point of vulnerability. In order to achieve a high level of reliability and accuracy, secondary users must exchange information with each other. When information is falsified intentionally by an attacker or during transmission, the legitimacy of spectrum sensing results degrade almost instantaneously. In addition, the effects of SSDFA attacks are often propagated throughout the entire network causing a long lasting impact.

The distributed nature of cognitive radio networks often means that users have strict power constraints. Many of the devices that make up cognitive radio networks are limited in size, which means that they often have limited computational capacity and battery energy storage capacity. Therefore, developers must keep this in mind when developing algorithms. Algorithms must have low computational complexity in order for them to be practical for implementation. In this thesis we develop algorithms to mitigate PUEA and SSDFA in Cognitive Radio networks. To mitigate against Primary-User Emulation attacks we use a combination of belief propagation and localisation of a transmitter to calculate a probability that corresponds to a belief about whether or not a transmitter is

an attacker. Essentially, when a transmitter (unknown user) becomes active on a channel, each secondary user performs local observations to determine the transmitter's identity. They then exchange their beliefs with other secondary users to determine a consensus about whether the transmitter is a primary user or a spoofer. This is similar to a decision made by a committee. We use a highly accurate, low computationally complex method that uses Received Signal Strength (RSS) measurements to localise a transmitting node. It is assumed that primary user locations are known. Using this information, we are able to determine with a high degree of accuracy whether the transmitter is a legitimate primary user based on the location of the transmitter. To mitigate against Spectrum Sensing Data Falsification Attacks, we employ a dynamic reputation function. A reputation function is a representation of the reliability of a secondary users observations. If the reputation of a secondary user is low, the user is seen as unreliable. If the users reputation is high, the user is seen as highly reliable. We develop a method for secondary users within the network to develop trust with each other. This helps secondary users determine the validity of an incoming messages, as trusted secondary users with a higher reputation have a higher probability of sending out valid spectrum sensing reports. In conjunction with the development of SSDFA mitigation schemes, this thesis introduces two new types of attacks: a reputation mining attack and a reset attack. These are prevalent attacks in reputation based algorithms. These are rarely contemplated, and algorithms to mitigate against them have been seldomly explored. A lightweight algorithm is introduced that is able to diagnose and mitigate these attacks effectively. Used in conjunction with our reputation scheme, the new algorithm is the most complete SSDFA mitigation method.

The development of algorithms to mitigate physical layer attacks must take into account possible system trade-offs. Naturally, the introduction of any new algorithm into an existent system creates additional functional and computational complexity. A trade-off between the level of security of the network and the additional complexity must be evalu-

ated. A new algorithm must ensure that the throughput of the network is not significantly affected by the introduction of algorithms which mitigate jamming and spoofing attacks. If the throughput is degraded significantly, then the introduction of the algorithm is no effective. In this thesis we address the question of whether it is possible to develop a unified algorithm to combat both PUEAs and SSDFAs that achieves a high level of security while having a minimal effect of the performance of the network.

1.2 Background and Previous Work

In the past decade, we have seen an increase in the number of wireless devices around the world. As a result, we have seen increased interested in a number of research fields related to wireless technology. Currently, research into 5G technology is the gaining a huge amount of attention [6]. Cognitive radio devices are considered by many to be one of the key technologies for the development and successful implementation of future 5G technology [7] [8]. Cognitive radio allows for higher utilisation of the radio spectrum, making it a key technology within 5G networks [9]. Throughout this thesis, we focus on the development of algorithms to mitigate against physical-layer attacks in Cognitive Radio Networks. In particular we focus on data and user authentication, emulation attacks, denial of service attacks and man in the middle attacks. Cognitive Radio implementation has been halted a number of times due to its poor resilience against a number of types of security attacks. Primary user emulation attacks, where a secondary user impersonates a primary user, and spectrum sensing data falsification attacks, where one or many secondary users spread falsified spectrum sensing reports in order to deceive other users in the network or gain an unfair advantage, are seen as the two most serious types of attacks. Similarly, with the Internet of Things, user emulation attacks are seen as extremely dangerous. A simple example of how dangerous this form of attack can be is

demonstrated within a smart home. If an attacker were to emulate the resident of the house, they would be able to control a number of appliances within the house and cause serious damage, not only to the appliances but also to the occupants. In this section we present a brief overview of some of the previous work presented by researchers around the world, in particular a number of algorithms that are directly related to what we have done throughout our work.

1.2.1 Primary-User Emulation Attacks

Primary-user emulation attacks are considered to be the most serious physical layer attack in Cognitive Radio networks. In a primary-user emulation attack, a secondary user impersonates the primary user to make it look like the primary user is active when the user is not (A primary user is said to be active if they transmitting on the channel). This enables the malicious node to take control of the frequency band, as other secondary users must vacate any radio frequency band. A number of methods have been proposed to combat primary user emulation attacks. The most popular methods are based on localisation of the transmitter. They use the location of the transmitter to identify whether the signal has originated from the primary-user or from a secondary user impersonating a primary user. Below we present a number of algorithms developed to stop primary-user emulation attacks.

In [10] the author presents a technique based on belief propagation. This technique uses cooperation between secondary users to localise a transmitter. Comparing this to the known location of a primary user, each secondary user is able to determine with a certain probability of the transmission originally at a primary user location. The author denotes this probability as a belief. Secondary users in the network calculate their own local beliefs and exchange them with their neighbours. Then, each secondary user calculates a final belief using their own beliefs and all the beliefs from their neighbours.

This algorithm suggests a useful procedure for determining whether the received signal originates from an attacker or not. This thesis presents substantial improvements to the algorithm described in [?] in terms of computational complexity, scalability and accuracy.

A number of mitigation techniques have been proposed to combat primary user emulation attacks. The most promising of these use localisation of the transmitter because primary users may be able to accurately replicate the signalling of a legitimate primary user. A number of methods exist for localisation of transmitters. These localisation methods can be classified into two categories: distributed localisation and centralised localisation. The first approach uses secondary user cooperation. This type of method is classified as the distributed method and involves secondary users trying to solve the localization problem individually using information from cooperating nodes. The second approach is the central approach. In this approach nodes are scattered around the network and collect snapshots of the transmitted signal. These measurements are sent to a central node that processes the information and makes a decision on whether the suspect is a legitimate user or an attacker. The advantage of the centralised approach is that the central node may have considerably more computing power than that of a secondary user.

Locdef is a localisation method that uses both localisation of the transmitter and signal characteristics to determine if the transmitter is a malicious user or not [11]. The Locdef scheme uses sensor nodes scattered around the network to take snapshots of the incoming RSS at different locations in the network. These measurements are sent to a central location for processing. By identifying peaks in the RSS, a central node is able to determine the location of the transmitted signal. Locdef uses a three-stage verification scheme to determine the validity of the incoming signal. The first stage of the Locdef scheme looks at the RSS of the signal to determine if it is coming from a primary user location or not. If the signal does not correspond to a primary user location, the transmitter is considered a malicious user and is ignored. If it does correspond to a known

location, the scheme moves on to the second verification point where the signal's energy is investigated. In the second stage the receiver looks at the energy of the received signal. The reason for this is that secondary users are not able to transmit at high power levels whereas primary users often are. If the receiver knows that it is close to a primary user the receiver would expect a signal with high energy to be received. If the incoming signal from the transmitter does not correspond to the expected received signal levels, the transmitter is considered a malicious user. If a suspect passes the first two stages, the scheme moves on to the last stage, where it compares the signal characteristics of the incoming signal with the known characteristics of the idle primary user. If the characteristics of the incoming signal do not match the known signal characteristics of the primary user, the transmitter is deemed to be a malicious user.

In [12], a scheme based on a combination of two signal-characteristic comparison methods is presented. This technique combines two methods called the Time Difference of Arrival (TDOA) and the Frequency Difference of Arrival (FDOA) to determine the location of the incoming signal. TDOA uses the differences in the time delay of signals arriving at secondary-user stations to determine the location of a transmitter. TDOA uses four receiving stations that use three dimensional time difference of four stations to get the positioning equations [12]. FDOA is used to estimate the location of target using the Doppler effect. As the transmitter moves their frequency changes which allows for other secondary users to track the direction of their movement [12]. Individually neither technique is capable of reliably locating the transmitter. However, when used together TDOA provides basic positioning points that are used by FDOA to determine the exact location of the transmitter. This technique is very accurate and works well with both stationary and moving targets, but it requires complex equipment at the receiving station. Its high level of complexity means that it is expensive and complicated to implement and run.

In [12] and [13], two primary user emulation attack mitigation schemes based on

authentication and encryption are presented. In [13], the author outlines a centralised scheme in which each primary user is given a unique ID number and a random variable by a centralised base station. Every time a suspect becomes active, the base station goes through a two-step authentication process to ensure that the suspect is a valid primary user. Before a primary user can access the network, the user must send their ID number to the BS for authentication. The primary-user ID is compared to a pool of identification numbers that correspond to all the primary users in the area. If the ID number corresponds to one of the ID numbers in the pool, the scheme moves on to step two of the authentication process. If it does not, the user is treated as a malicious user and is ignored. The second step of the process is called the information displacement step. In this step, the random variable (which each PU must know) is multiplied by an encryption matrix which returns a value M that is compared to a set of expected values (the expected values correspond to previously calculated values using the random variables of the PUs). If the value corresponds to the expected values, the transmitter is authenticated as a primary user. If it does not, the transmitter is treated as a malicious user and is ignored.

In [**?**], the author presents a technique based on belief propagation. This technique uses cooperation between secondary users to localise a transmitter. Comparing this to the known location of a primary user, each secondary user is able to determine with a certain probability whether the transmitter is a primary user. The author denotes this probability as a belief. Secondary users in the network calculate their own local belief and exchange them with their neighbours. Then each secondary user calculates a final belief using their own beliefs and all the beliefs from their neighbours. [**?**] describes a useful procedure for determining wether a transmitter is a primary user or an attacker. This thesis introduces substantial improvements to the algorithm and performance in [**?**].

In [14], a scheme to combat primary-user emulation in CRNs is presented. The authors use a Wals sequential probability ratio test (WSPRT) in an attempt to develop a

mathematical model for the PDF of the incoming signal. The probability density function (PDF) is used to develop a lower bound which is used to determine whether the incoming signal is a malicious user or a primary user. This method is fairly effective. However, it does not take into account the observations of the other secondary users in the network. The lack of cooperation with other secondary users means that the poor accuracy of the results obtained by this method make it unstable because of noise and other channel degradation factors such as fading and shadowing. Since every secondary user is essentially a stand alone node, the effects of degradation and the hidden node problem have a tremendous effect on results. A hidden node is one that is seen by the central node but not to the other nodes on the network. A hidden node that is visible to one node but not to the rest of the users on the network. When a hidden node is present, convergence of the algorithm is difficult.

In [15], the authors present a mitigation algorithm based on hopping. The algorithm is based on a zero sum game where the goal for the legitimate users is to evade the attacker by predicting which channels they will attack. This method assumes that channel statistics are known for the entire network. This means that it is somewhat limited when such knowledge is not available. It is also fairly high in computational complexity, as its accuracy improves as more information becomes available. This means that it is best suited for centralised networks, where the computational burden rests with the central node.

In [16], an algorithm to mitigate against primary-user-emulation attacks is presented. The authors present an algorithm based on analysis of the received signal strength at a secondary user. Using a number of RSSs(Receive Signal Strength) power measurements, lower and upper thresholds are established and the RSS measurements are compared to the threshold. A flexible log-normal sum approximation is used to characterise the incoming RSS. This algorithm relies on a centralised topology, in which the central node handles

the bulk of computation. In order for this algorithm to be effective in its mitigation of primary user emulation attacks, it is essential that an accurate threshold is developed. This however could take some time when limited information is available. Trust between users is another aspect that is overlooked in this algorithm but the use of trust could help improve its performance.

In [17] an authentication algorithm based on one way hash functions is presented. The primary user initiates a hash chain that is used by secondary users to authenticate the primary user. One advantage of this method is there does not need to be any modifications to the transmitter. However, if the malicious node discovers the chain sequence(refers to the chain of hash functions), the malicious users would be able to successfully emulate the PU for extended periods.

Primary user emulation attacks have received increased attention within the research community over the past few years. Their impact on cognitive radio networks is apparent and has been a key deterrent to its implementation. A number of the methods to diagnose and combat primary user emulation attacks exist throughout the literature. Many are very effective but have shortfalls in key areas such as computational complexity and practicality. Others have poor authentication protocols and lack methods to establish trust between users. In this thesis, we present a practical physical layer protocol to combat primary user emulation attacks which we believe is the most complete and comprehensive solution to combat physical layer attacks.

1.2.2 Spectrum Sensing Data Falsification Attacks

SSDFAs can be devastating to the network if they are not considered. A large number of papers that propose schemes to combat SSDFAs do not take into account a trust factor. Trustworthiness of incoming information is extremely important in any network. Essentially, if we cannot trust the spectrum sensing information that is being relayed by

other secondary users, that information has limited usefulness. Therefore, it is essential that any scheme to combat SSDFAs is able to accurately and efficiently establish trust between secondary users within the network. This section summarises previous research conducted in the mitigation of spectrum sensing data falsification attacks in cognitive radio networks.

In [18], a modified "q out of m" scheme is proposed, where only a fraction of the secondary users in the network is polled for their spectrum sensing reports. Essentially, if there are m users in the network and if a subset of those users (q) report a 1 (corresponding to a primary user being active). Then, the final spectrum sensing report results will show that the primary user is actively transmitting on the channel, regardless of that the rest of the users report. In other words, the q can be seen as a threshold value. Once the enough users agree to the same results, that result is assumed to be valid. In [18], the author proposed a few simplifications of the previous "q out of m" schemes. However, the method presented is a centralised scheme that relies on a central control center to receive and process the reports. The high complexity of the algorithm means that it would be difficult to implement in a distributed network. Since the group of secondary users is selected randomly, there is a high chance that it could consist of a large percentage of malicious users. This would significantly reduce the accuracy of this method.

In [19], a Maximum Likelihood Estimator (MLE) based method is proposed. A central fusion centre is used to process data. This method uses an effective outlier algorithm. When an outlier is identified, their observations are discarded. Legitimate secondary users are rewarded with an increase in trust (reputation value). The proposed method has only been proven to work well with a small percentage of secondary users present in the network. The high complexity of the algorithm also makes it difficult to implement in distributed networks. There is no punishment (decrease in trust) for malicious nodes, which could cause a problem if malicious users act legitimate for a period of time to in-

crease trust and cause maximum damage.

In [20], an enhanced weighted sequential probability ratio test (EWSPRT) method is introduced. In EWSPRT, whenever a report is consistent with the global observations, it is rewarded with an increase in reputation. When it is not, it is punished with a decrease of reputation. Nodes with higher reputation are polled and have a higher weight in the overall consensus, since we assume that they are highly likely to be sending out legitimate reports. This method suffers from high complexity and is therefore not suitable for distributed networks. Its reputation algorithm is static and could be used by malicious users to build trust and cause maximum damage to the network. The low reputation punishment update values means that secondary users could cause serious damage throughout the network for extended periods of time. It lacks a comprehensive outlier test to stop malicious nodes from taking advantage of the reputation algorithm.

In [21], an RSS (Received Signal Strength) based method is presented. The proposed method relies on localisation of the transmitter along with the spectrum-sensing results to determine whether or not the transmitter is a malicious node. An increase in reputation is given to secondary users who report legitimate information. This is a simple scheme that can be implemented in distributed networks. It is robust and is able to mitigate against SSDF attacks effectively. However, there is no punishment for secondary users who report falsified information, and relies on RSS measurements that can be unreliable in noisy environments. It also lacks an outlier identification method.

In [22], each secondary user calculates their own local observation. Incoming messages are analysed and reputation values are updated according to the validity of the message. Extreme outliers are discarded using z-scores. Z-scores are a method to identify statistical outliers from an arbitrary set of data. This method is simple and is well suited for distributed networks. However, the reputation scheme does not have a threshold, which means that malicious users could act as legitimate users for an extended period of time

to accumulate reputation. It doesn't consider shadowing or noise on the channel, making it unreliable in practical implementation.

In [23], the authors present an SSDFA reputation-based method. The algorithm works in a three-step process. The first step is called the preliminary step; at this point the secondary user's reputation is compared to a threshold. If the reputation is above the threshold, the user's results are used in the final decision. If not their observations are discarded. In the next step, a cluster is formed containing a subset of secondary users. In the third and final step the central node uses the majority rule to determine what the result of the spectrum sensing are going to be. The performance of the algorithm is compared to [24]. In comparison to that algorithm described in [23] it presents a significant improvement.

In [25], the authors present a method to alleviate the effects of SSDFAs in cognitive radio networks. A similarity factor is used to establish the validity of incoming spectrum sensing information. Essentially, after each secondary user performs their spectrum sensing, they forward this information to the fusion centre which compares those results with their own and computes a similarity. If the two results are similar to a degree, the spectrum sensing results are added to the overall result. If not, they are discarded. This method is effective, however it has several disadvantages. Namely, if the results that are being used as the baseline for comparison are wrong, the entire scheme is nullified.

In [26], a reputation based algorithm is proposed. The algorithm uses a maximum likelihood estimator to determine the distribution of secondary user reports. This is used to evaluate the trustworthiness of each incoming signal. If the signal falls within the calculated range, the reputation of the sender is increased. If not, the reputation is decreased. The authors have shown that this method performs on par when about 16% of users are malicious. However, when 30% of secondary users are malicious, there is a significant advantage to be gained with this method as opposed to simple averaging. One of the

main problems with this type of algorithm is the lack of a punishment for secondary users that do the wrong thing.

The authors in [27] propose a method with two algorithms to combat spectrum sensing data falsification attacks in Cognitive Radio Networks. The first algorithm is based on the identification of the attacker. After the attacker has been identified their spectrum sensing results are discarded. To further increase the efficiency of the method, the second algorithm introduces a punishment function that is used to punish users that send falsified results. The punishment ensures that malicious nodes are identified quickly, with a reduced reputation function. The algorithm presents an effective method to mitigate spectrum sensing data falsification attacks. It is however vulnerable to malicious nodes that adopt more advanced attack methods such as the replay attack, which involves an attacker resetting their reputation after their reputation is decreased and reputation mining attacks, where attackers report legitimate results for a period to increase their own reputation so they have a greater impact.

A method called Attack-Aware Cooperate Spectrum Sensing (ACSS) is introduced in [28]. This method uses the strength of the incoming signal to determine whether a transmitter is a malicious node or not. The ACSS method uses a k-out-of-N rule to derive the optimum value of the parameter k to minimise the Bayes risk. k out of n refers to a threshold regarding the observations. If there are n users in the network and if a subset of those users (k) report a 1 (corresponding to a primary user being active). Then, the final spectrum sensing report results will show that the primary user is actively transmitting on the channel, regardless of that the rest of the users report. This is very similar to the p out q method. This method is lightweight(low computational complexity) and in the right circumstances is very effective. However, determining whether a transmitter is a malicious node or not using only RSS information can lead to poor results, especially if secondary users are not stationary in location. This is due to a number of degradation

factors such as noise and shadowing.

A biologically inspired mechanism is introduced in [29]. This algorithm is inspired by self-organising behaviour that occurs in nature with fish and birds. The proposed algorithm is a distributed algorithm, where each secondary user performs localised spectrum sensing. Each secondary user then passes this information around the network until a general consensus is reached. When the final spectrum sensing results are calculated, they are compared to a predefined threshold. This method is a self-learning graph based method similar to belief propagation. A particular shortfall of this algorithm is that it fails to establish a trust function that can be used to detect malicious users. Instead, using this method, a malicious user can continuously transmit falsified information which significantly degrades the cognitive radio network performance.

In order to diagnose and mitigate spectrum sensing data falsification attacks we must consider as many possible scenarios as possible. We must assume that the malicious node is not going to launch the same type of attack every time, but randomise their strategy to ensure maximum effectiveness. Therefore, we must develop an algorithm that is lightweight (with low computational complexity) and flexible. Throughout the literature, we have seen a number of very effective algorithms. However, all have vulnerabilities that can be exploited by a smart adversary. The majority of algorithms include a reputation function to develop a trust between secondary users. However, most do not consider punishment as part of the reputation function. It is essential that punishment for falsified results is established within any algorithm that hopes to be effective. Another aspect that is often missing is a defence against data mining attacks. In this type of attack, the malicious user sends out legitimate results to increase their reputation to a point where they are trusted by all other secondary users. Then, they start falsifying results causing increased damage to the network because of their high reputation. In this thesis, we not only identify but also develop a method that is able to defeat attackers using reputation

mining and reset attacks. Reset attacks are used when the reputation of the attacker drops below a certain value. Instead of sending out legitimate results, the attacker then pretends that they are new to the network and their reputation is automatically reset to the default value. This greatly increases the effectiveness of the attacks because the attacker has relatively high default reputation value.

1.3 Contributions

This thesis introduces a number of algorithms to mitigate physical layer attacks in Cognitive Radio Networks. More specifically, the research contributions of this thesis are summarised as follows.

- A fundamentally new simplified belief propagation based algorithm to identify and mitigate against primary user emulation attacks. The convergence time of the algorithm was decreased significantly relative to the time reported in previous literature, with the introduction of a new local function. This is especially true when there is a large number of secondary users in the network. In some cases the convergence time was decreased from hours to seconds.

- Development of a novel single iteration belief propagation algorithm to combat primary user emulation attacks. Previous belief propagation algorithms were iterative in nature and required as much as 10 iterations to reach a satisfactory result. The new algorithm presents a fundamental improvement and is able to achieve the same level of accuracy with a single iteration. This significantly reduces the complexity of the algorithm, which enables easier implementation. This algorithm is most effective in large networks, where many secondary users are exchanging information.

- An algorithm to combat spectrum sensing data falsification attacks in cognitive radio

networks. Using the belief propagation framework in conjunction with a reputation based compatibility function, we are able to mitigate the effects of SSDFAs. This novel hybrid method increases detection rates, and outliers are identified using a modified Z-scores based function [30]. This algorithm is well rounded, fast, accurate and easy to implement.

- A revolutionary hybrid compressive sensing belief propagation algorithm that greatly improves the accuracy. Compressive sensing increases the localisation accuracy of the transmitter. This allows for better comparison with the primary user location, greatly increasing accuracy. This algorithm can be implemented in both a centralised and distributed architecture.

- A highly accurate novel Belief Propagation Based Statistical Reputation Function (BPBSRF) algorithm to combat Spectrum Sensing Data Falsification Attacks in Cognitive Radio Networks. We use a dynamic reputation function that can be adjusted to reflect the degree of punishment and reward to be given out to secondary users. This is the best and most complete algorithm to combat SSDFAs. It is a complete mitigation algorithm that completely neutralised SSDFAs.

- The identification of a novel type of attack called a reputation mining attack. A reputation mining attack involves an attacker pretending to be a legitimate user to build up its reputation to the point where they are trusted by other secondary users. Then it begins to transmit falsified results with maximum impact on the network. We characterise this new type of attack and present a method to alleviate it. To combat this a three strike policy was introduced(where users are only allowed to send out falsified results three times before being excluded), with a mandatary suspension to users who report falsified reports.

- The identification of a novel attack, called a reset attack. a probation function is

introduced to deal with this type of attack. A reset attack involves an attacker sending out falsified results until their reputation is low, at which point they reset and are given a default reputation. This type of attack is characterised within this thesis and a method to mitigate its effects is presented.

- A unified physical layer algorithm able to effectively mitigate both SSDFA and PUEAs. This novel unification approach to the mitigation of physical layer attacks simplifies implementation and decreases the overall complexity of processing to mitigate these attacks by the secondary user.

Chapter 2

Cognitive Radio Networks

Officially, the International Telecommunications Union (ITU) defines a cognitive radio as a "radio system employing technology that allows the system to obtain knowledge of its operational and geographical environment, established policies and its internal state, to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives, and to learn from the results obtained" [31]. Since then, cognitive radio has been redefined a number of times throughout the literature. In this thesis, we define cognitive radio simply as a collection of intelligent device methods designed to use the radio spectrum in an efficient manner. Cognitive radios increase spectrum efficiency by allowing unlicensed users to utilise channels when they are not being used by primary/licenced users. In the CR terminology, a licensed user is often denoted as a primary user (PU) and an unlicensed user is referred to as a secondary user (SU). Secondary users scan sections of the spectrum looking for bands that are not being used. When an idle band is identified by a SU, it can be used by the SU as long the primary user remains idle. The secondary users must continually monitor the status of the channel being used. If a primary user was to become active, SU would have to vacate the channel immediately.

This chapter provides an overview of some of the key concepts of CR technology. It presents an introduction to the basic concepts and theories associated with the function and operation of cognitive radio networks. The primary objective of cognitive radio is to provide a means to utilise the radio frequency spectrum more efficiently than fixed assigned networks. This is achieved by allowing secondary users access to frequency bands that were originally designated for primary users. This increases efficiency as previously under-utilised spectrum is being used, while congestion in over-utilised bands is eased. An essential aspect of cognitive radio is its dynamic nature. Each device must ensure that it is continually monitoring the environment to ensure that a primary user has not become active on the band. If a primary user does become active, all secondary users on that channel must immediately vacate the channel. In addition, it is important that secondary users are able to distinguish between a primary user becoming active and secondary users trying to use the band or high variants of noise in the environment.

In order to perform to its maximum capacity, it is important that secondary users within the cognitive radio network are able to communicate with each other [32]. Cognitive radios are intended to operate in a highly dynamic distributed topology. Therefore, for effective and accurate results, secondary users must cooperate with each other. Cooperation is defined as a paradigm that allows distributed terminals in a wireless network to communicate through some distributed transmission or signal processing so as to realise a new form of space diversity to combat the detrimental effects of fading channels upon the determination of available channels [33]. Cooperation is an essential part of cognitive radio. It is therefore important that users able to communicate in an effective and efficient manner. In a typical network, each secondary user does some localised observations of the environment. These observations are then propagated throughout the network to

ensure that different perspectives are considered. Just like many problems in life, the more information from different perspectives is available the more accurate the decision becomes.

The rest of this chapter is organised into seven distinct sections. In the first section, we explain how cognitive radios operate. The cognition cycle is used by secondary users to learn and adapt from their environment. These key concepts are the basis of cognitive radio networks. The next section details different spectrum sensing techniques. Energy detection, matched filter detection and cyclo-stationary detection are introduced. These form the basis for all other spectrum sensing methods. We also present some of the more advanced hybrid techniques. The next section gives an introduction into machine learning, which is an essential part of the cognition cycle. Techniques such as Q-Learning, which is a form of reinforced learning, that uses a reward function to optimise future actions are used as tools to increase the efficiency of cognitive radio devices by predicting changes in the environment. The next section presents a key enabling technology for cognitive radio networks, software defined radios. These allow for highly flexible receiving and transmitting configurations which enable cognitive radios to effectively operate. The next section presents the two main network topologies used in cognitive radio networks, the distributed and the centralised architectures. The last section presents the different localisation methods used in networks to localise a transmitting node. We use these methods as a way of identifying whether the signal is coming from a primary user, or a non authorised transmitter.

2.1 Cognition Cycle

A primary objective of cognitive radios is to perceive the environment that they are operating in and learn from events that occur to generate plans for future action [34] [35]. This essentially means that cognitive radios must continually monitor their radio environment and ensure that they adapt to changes in that environment, in an effective and efficient manner. Fig. 2.1 is an illustration of a typical cognition cycle used by cognitive radio devices. CR operations are split into four distinct phases. In order for a cognitive radio to effectively achieve its mission, it must ensure that each phase is completed accurately. The four phases are characterised as: the sensing phase, the analysis phase, the decision phase and finally the adaptation phase. It is important to note that even though each phase can be thought of as being independent, in order for cognitive radio to achieve its mission, it is essential that the information gathered in the previous phase is carried over into the next phase. This process is repeated in a never ending cycle by each secondary user within the network.

The cognition cycle is applied to spectrum sensing phase where each secondary user scans parts of the spectrum looking for possible idle bands that they can use. They sense to see if there is a channel idle, they analyse the channel to determine its capacity, user occupancy and channel quality. Then, they decide on whether they are going to use the channel or if they have to go back to the sensing phase based on the information they have gathered. Finally, in the last step the secondary user either chooses to use the channel that they found or goes around and begins another cycle, starting with sensing [36].

The initial phase in the cognitive radio cycle is called the sensing phase. During the sensing phase each secondary user within the network performs some preliminary sensing to determine whether a channel is actively being used or not. During this phase, it is important that secondary users are very flexible and as soon as they identify a primary user within the band they move on to another band. It is also important to ensure that

Figure 2.1: Functional Architecture of a Cognitive Radio

spectrum sensing results are accurate. If a primary user is within the band it is important that the secondary user does identifies this and does not begin to send out data, interfering with the primary user [36]. On the other hand, it is also important that when the primary user is not active, the secondary user is able to identify this. Otherwise, critical resources such as time and frequency are wasted. To perform spectrum sensing a cognitive radio can employ a number of techniques. However, most are based on one of the following: energy detection, matched filter detection and cyclostationary detection. The decision on which to use depends largely on the environment in which the network is operating, the amount of resources available, and the processing capabilities of the secondary users. Spectrum sensing techniques are discussed in more detail in the next section of this chapter.

At the conclusion of the sensing phase, we begin the analysis phase, during which the information that was gathered in the sensing phase is analysed. During the analysis phase, raw information from the previous phase is used to determine whether or not the primary user is active within the channel. More formally during the analysis phase spectrum opportunities are evaluated. A spectral opportunity is conventionally defined as “a band of frequencies that are not being used by the primary user of that band at a

particular time in a particular geographic area" [37]. At the conclusion of the analysis phase, there are three possible outputs that are directly inputted into the decision phase. The first is a result of the primary user actively using the channel, in which case the analysis phase would conclude that this channel should not be used. The next is when a primary user is idle on the channel, in which case the analysis phase would conclude that the channel could be used. Then, the last phase is when the primary user is using the band but there is a possible opportunity for secondary users to use the band with minimal interference caused to the primary user. Information from the analysis phase is then pushed through to the decision phase. During the analysis phase, the cognitive radio also collects information about each channel. Channel parameters such as the signal to noise ratio and number of users within the channel are critical to making an informed choice in the decision phase.

At the conclusion of the detailed analysis phase during which spectrum opportunities are evaluated and one of three possible outputs was decided upon. We enter the decision phase of the cognition cycle. During the decision phase we are presented with one of three results coming in from the previous two phases and we must make the best possible decision using this information. The best channel to use is usually the one that has no primary user active on the channel. However, other consideration to take into account include: the number of secondary users that are already using the channel, the signal to noise ratio and even how likely the primary user is to become active in the future (usually done using some machine learning techniques that predict primary user activity using historical data). In addition to the hard decision that has to be made in the decision phase, the decision phase is also used to specify transmitting parameters such as the transmission power, the transmission start time, modulation rate and the number of antennas to be used [36] [37] [38]. These are often specified to achieve the best possible results.

The last step of the cognition cycle is the adaptation phase. The previous three steps

are used to gather information which is used in this phase to perform the best action possible. More formally, the adaption phase is a direct extension of the decision phase and is where all the parameters from the previous stage are implemented. This implementation is done utilising software defined radios (SDRs). It is essential to understand that efficient information gathering and decision making are key to the efficient operation and implementation of cognitive radio. After the action has been taken, the cycle begins again. If a suitable channel is identified and the secondary user decides to utilise it, the user go back to start of the cycle and perform sensing again. Only this time the sensing is on a the channel correctly being utilised. If no suitable channels are identified, the process restarts just as before with the secondary user scanning a number of frequency channels looking for a suitable candidate.

2.2 Spectrum Sensing

The most important aspect of cognitive radio operation is efficient and accurate spectrum sensing, defined as the task of obtaining awareness about the spectrum usage and the existence of primary users on a specific frequency band [39]. Spectrum sensing allows a secondary user to identify frequency bands that are not being utilised by PUs. The sensed spectrum bands can be classified into three categories: black spaces, white spaces and grey spaces [40]. White spaces correspond to spectrum bands that are completely vacant. Grey spaces are partially used spectrum bands that can be considered by secondary users; they are bands that are occupied by low-power PUs or distant PUs. The black spaces are spectrum bands that are occupied by primary users and should not be considered for utilisation by SUs. There are a number of different spectrum-sensing techniques available for cognitive radio. The goal of spectrum sensing is to decide between two hypotheses [40].

$$x(t) = \begin{cases} n(t), & H_0 \\ hs(t) + n(t), & H_1, \end{cases}$$

where, the H_0 hypothesis specifies that no primary user is using on the channel, and the H_1 hypothesis indicates that a primary user is currently occupying the channel. s(t) denotes the received signal from the primary user, $n(t)$ is the channel noise which is additive white gaussian noise(AWGN) and h is the shadowing constant. The first and simplest technique for spectrum sensing is called energy detection. This basic technique measures the received energy of the incoming signal. In energy detection the signal is measured over a period of time and the average energy is acquired. This average energy is then compared to a pre-set threshold which determines if the transmitted signal is a primary user or just noise. A key feature of energy detection is that it does not require any knowledge about the characteristics of a primary user signal. This enables energy detection to determine very quickly if the channel is being used very quickly. Figure 2.3 provides a summary of the different sensing methods with their corresponding sensing accuracies and complexity.

2.2.1 Energy Detection

Energy detection is the primary means of spectrum sensing when the secondary user has no prior knowledge about the signal characteristics of the primary user. Energy detection is very simple to implement and does not require complicated hardware for implementation. Energy detection has a number of drawbacks. It is not able to distinguish between channel noise and the signal from a transmitter. This means that noise has great effect on its performance. It has been shown, that energy detection performs badly in low signal to noise environments [41] [42] [43]. Another problem with energy detection is the threshold selection. It is very difficult to set a threshold that will optimize performance

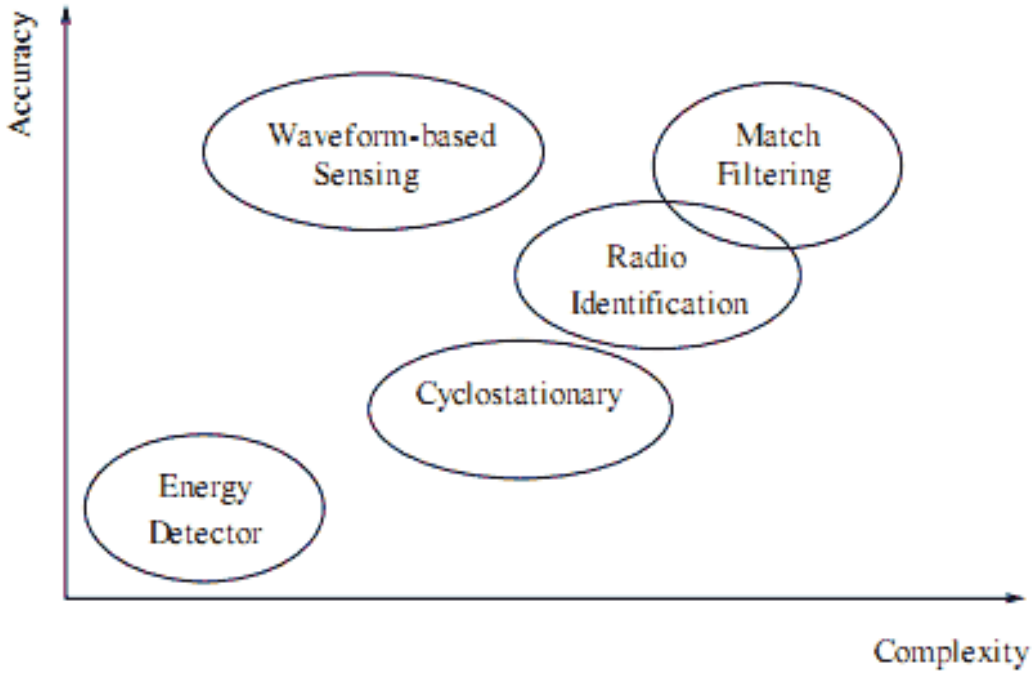

Figure 2.2: Spectrum sensing techniques.

because a low threshold allows for a higher degree of error, where high noise might be miss-identified as a primary user. Whereas, a high threshold means that distant primary users might not be identified.

2.2.2 Matched-Filter Detection

Matched-filter detection is a more sophisticated form of detection then energy detection; the incoming signal from the primary user is put through a filter matched to the PU signal waveform, which is correlated to a signal sample [33]. The result of the correlation is compared to a predefined threshold and a decision is made on whether the signal came from a primary user or not [44]. Matched-filter detection performs much better than energy detection. It is able detect a primary user more accurately than energy detection and is much less susceptible to noise than energy detection. Matched-filter detection has

also been shown to be very quick and efficient [33]. Its main disadvantage is that, in order to work, it must have prior knowledge of the PUs signal wavefrom. If it does not have this, its performance is very poor. Therefore, even with its improved performance over energy detection it is often overlooked for spectrum sensing because of its dependence on prior knowledge [45].

2.2.3 Cyclostationary Detection

The idea of the cyclostationary feature detection is to utilise the built-in periodicity of a modulated signal [46] [40]. Cyclostationary feature detection works by auto-correlating the incoming signal, which separates the signal from the noise. The fact that noise on the channel is not periodic in any way allows cyclostationary detection to efficiently separate the noise from the signal. This means that, unlike energy detection, cyclostationary has better detection performance than energy detection because it takes advantage of particular features of the PU waveform. Cyclostationary is also able to distinguish between a secondary user signal and primary user signals. The reason for this is that different wireless systems usually employ different signal structures and parameters [33]. Cyclostationary detection requires that the incoming signal has cyclostationary properties. These signal properties may be represetnted as a function of frequency and cyclic frequency [40]. A major disadvantage of cyclostationary detection is that it needs complicated equipment for its implementation and needs multiple fast fourier transform(FFT) calculations, which make it slow and computationally expensive to implement [46] [40]. Cyclostationary detection has been shown to have much better detection performance than energy detection. This is because of pattern recognition of signal features, it provides much better performance results in noisy environments. However, compared to energy detection, it has much higher computational complexity and is more expensive to implement.

2.2.4 Waveform-based sensing and radio-identification based sensing

In addition to the classic spectrum-sensing techniques for cognitive radios, we present two additional techniques: waveform-based sensing and radio identification sensing. Waveform based sensing takes advantage of patterns in the preamble and pilots of a transmitted signal to identify a primary user. A preamble is a sequence of bits transmitted before each signal burst. If a secondary user on the network has knowledge of what patterns are used by a primary user, the SU can analyse the preamble and decide whether the signal is coming from a primary user or not [47]. Radio identification based sensing uses prior knowledge about the transmission techniques used by the primary user. This allows a cognitive radio to identify key features about the primary user which help it detect the presence of a PU on the spectrum band [47].

2.2.5 Combined Detection

Benko [48] presents the idea of using a combination of these techniques to achieve better results than each individual technique could achieve by itself. In [48] Benko proposes an algorithm based on a combination of energy detection and feature detection. The method proposes to use energy detection to find candidates and feature detection to identify the type of signal on the band. In the first part of the technique, large parts of the spectrum are sensed using energy detection, and, at this stage, the sensing sensitivity is not important. After the energy detection scheme identifies possible bands for use, feature detection is used with higher accuracy to determine if a primary user signal is present or not [48] [46]. The use of a combination of sensing techniques helps improve the detection performance and decrease the time required to make a sensing decision. Energy detection is used to scan a large number of frequency bands very quickly. Then the most

promising bands are selected and are further scanned using feature detection to increase the detection performance of the result.

2.2.6 Challenges

The primary requirement of spectrum sensing is that the detection is fast and accurate. A successful spectrum sensing algorithm must achieve an optimum balance between speed and accuracy. It is important that sensing is done as fast as possible so that the secondary user can take maximum advantage of spectral opportunities without causing excessive primary user interference. However, if sensing is done fast but at a low accuracy, the overall performance of the network will decrease. Multipath fading and dispersion can cause serious degradation to signals in wireless networks. These are major challenges that secondary user networks need to overcome in order to be able to accurately and reliably sense the presence of a primary user on the network. The location of the cognitive user network can have a large effect on the amount of noise and interference that a signal is subjected to. This means that spectrum sensing techniques must be flexible and must be able to deal with noisy environments. Another major challenge of spectrum sensing is the implementation of the right detection method for the right application. In areas where there are large amounts of noise, energy detection is not very effective as a solution. If secondary users have prior knowledge of the primary user signal, matched-filter detection is an effective solution. Spectrum sensing is still an open research field and optimum methods for particular, sets of requirements and constraints are still being investigated.

2.3 Machine Learning (ML) and Artificial Intelligence (AI) in Cognitive Radios

AI technology has been rapidly developing over the past few decades. AI agents are now able to analyse complicated situations, make calculations and decide on the best course of action to best suit their stakeholder. Cognitive radio can be identified as an AI based technology [1]. Cognitive Radios are able to analyse their environment to learn which parameters need to be modified to achieve their objective. For example, if a low amount of noise is present on the channel, then the transmit power output of the SU could be reduced without losing efficiency, while at the same time saving energy and decreasing interference.

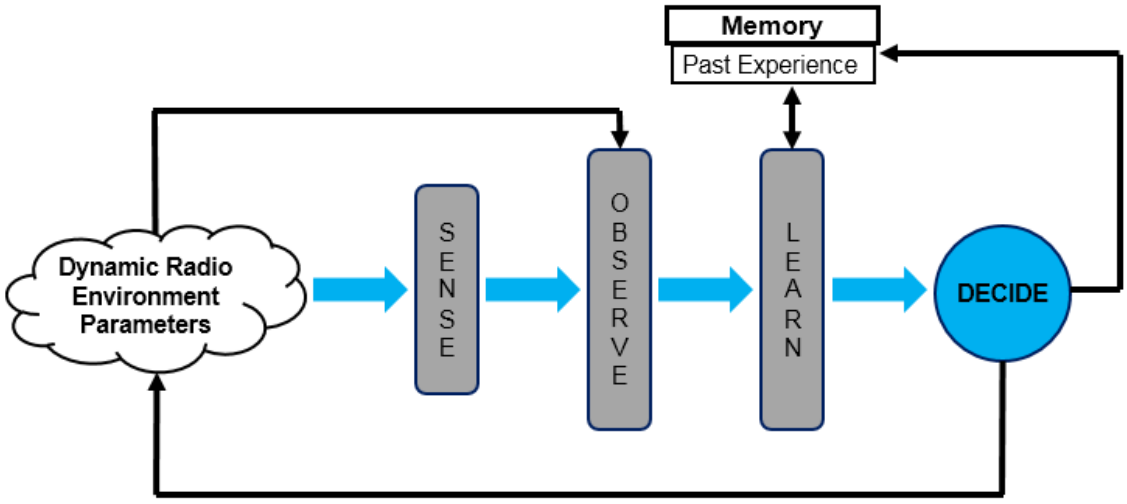

Figure 2.3: Cognitive Radio operation [1].

We see that after the sensing phase, where cognitive radios typically perform spectrum sensing, the CR must decide on transmission parameters. This functionality, in conjunction with the application of game theory, enables secondary users to predict which channels will be vacant at which time. For example during off peak hours, when businesses and

people are sleeping, certain spectrum bands would consistently be idle. Using techniques such as Q-Learning we are able to predict with a fairly high accuracy which bands will be idle and when these bands will be idle. Q-learning is known as a reinforcement learning technique. Q-learning is a simple learning algorithm, it is a state based algorithm. In every state an action is executed, and each action corresponds to a reward. The goal of Q-learning is to maximise its long term reward. To do this, Q-learning checks each action at each state to ensure that all possible actions are considered [49] . The best action is taken and the current Q value is updated using the following:

$$Q(s_t, a_t) \leftarrow Q(s_t, at) + \alpha[\, r_{t+1} + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, at)] \tag{2.1}$$

where, $Q(s_t, a_t)$ represents the old Q value and α represents the learning rate. The higher the value of α, the more the Q-value will change at each new state. An α value of 0 represents no change and a value of 1 would drastically change the Q-value with every state. γ is the discount rate. r_{t+1} represents the feedback value, which can be understood as an estimate about the effectiveness of the previous action [49]. If the feedback is negative, that means the action was not optimal. The greater, value of the feedback value the better the action is. $\max_a Q(s_{t+1}, a)$ represents the maximum future Q-value. The Q-value is updated once every state with the best possible state. After convergence, Q-learning is able to determine the optimum strategy, with respect to band selection and parameter selection for the SU.

2.4 Software-Defined Radio (SDR)

Software defined radios (SDRs) are an essential part of CR implementation. Cognitive radio devices are designed to be highly adaptable radios that are able to change their functionality and parameters to suit changes in the environment. It is therefore essen-

tial that cognitive radios have an extremely adaptive and flexible software and hardware platform. In [50] Software defined radios are defined as "a collection of hardware and software technologies where some or all of the radio's operating functions (also referred to as physical layer processing) are implemented through modifiable software or firmware operating on programmable processing technologies. These devices include field programmable gate arrays (FPGA), digital signal processors (DSP), general purpose processors (GPP), programmable Systems on Chip (SoC) and other application specific programmable processors".

There are a large number of models that describe both cognitive radio and software defined radios. Figure 2.4 illustrates a model that relates cognitive radios to software defined radios. This model enforces the important relationship that must exist between cognitive radios and SDRs. A cognitive radio aims to satisfy the radio link requirements of users [35]. It does this by continually monitoring the environment using a number of sensors, and its goal is to be agile and be aware of changes in the environment as quickly as possible. After measurements are taken, they are analysed and evaluated by the cognitive radio device. If sufficient change has occurred in the environment, the cognitive radio engine will implement changes to ensure that the required level of performance is maintained. It is able to implement the changes by modifying the SDR configuration. This ensures that the upper layer functionality requirements are met.

There are a number of advantages of implementing cognitive radio devices using software defined radios. Low cost manufacturing, implementation and maintenance of a product are key considerations during the development of any product. The use of software defined radios will enable development companies to implement low cost, high quality,

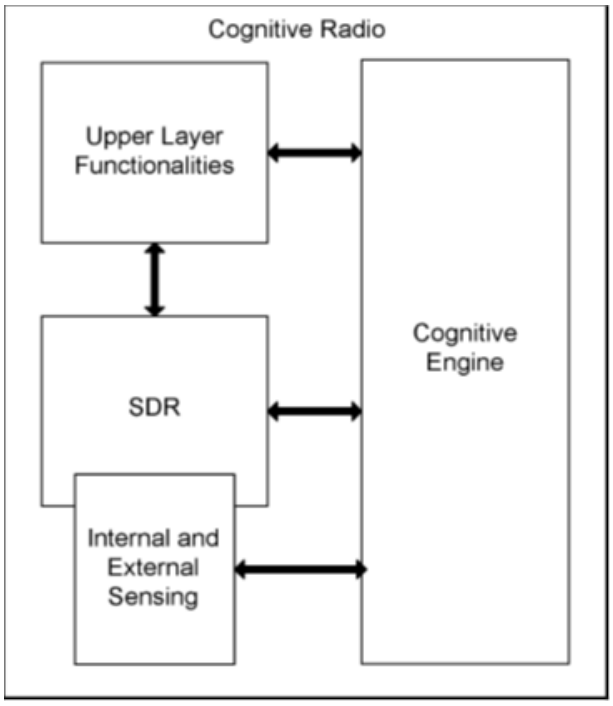

Figure 2.4: Relationship between SDR and CR.

cognitive radio devices. SDRs not only offer low cost manufacturing, but also enable it to be upgraded at a lower cost. Software defined radios allow for remote troubleshooting and reprogramming, which decreases the cost of maintenance and fault correction within a CR device.

A key feature of SDRs is their ability to offer great power efficiency for cognitive radio nodes. Power efficiency is an essential feature in cognitive radio design since most cognitive radios are going to be implemented in mobile devices such as mobile phones. These mobile devices have certain design restrictions as consequences of their size. To ensure that this restriction is kept, manufacturers must use appropriate components. This has a great impact on the battery life of the device and means that devices have to be built to be as power efficient as possible.

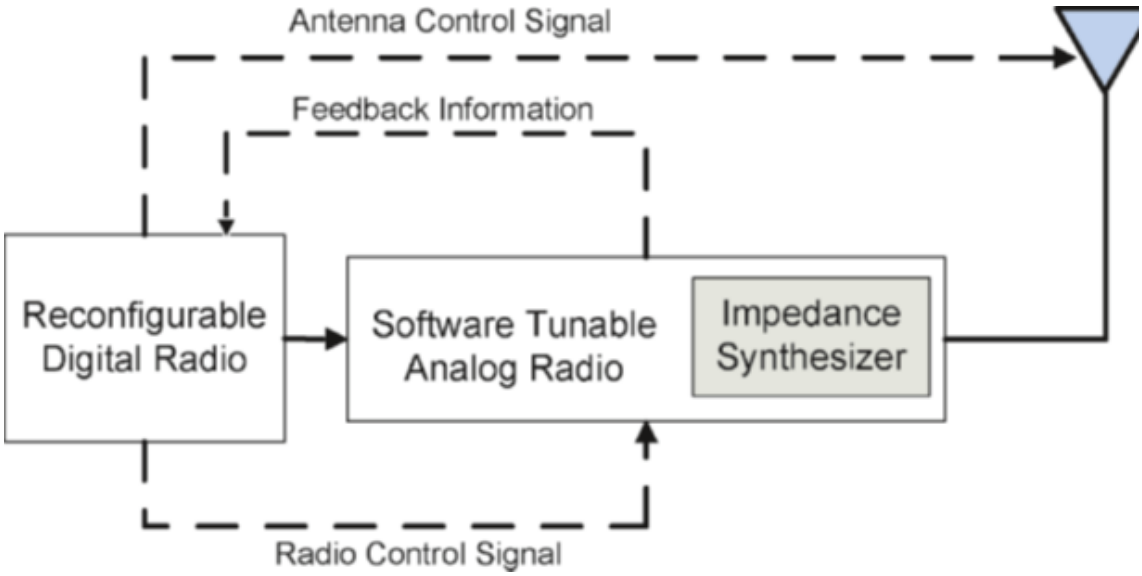

Figure 2.5: Ideal SDR architecture.

A simple architectural model of a SDR is shown in Fig. 2.5 [35]. This model is made up of three different parts: the configurable digital antenna, the software tuneable analogue radio and an Impedance Synthesiser. All three components of a software defined radio are fully reconfigurable, which allows the device that is using the SDR to be flexible. The reconfigurable digital radio performs digital radio functionality, the software tuneable analogue radio performs functions that are associated with analogue radio functionality, and the impedance synthesiser is used to optimise the performance of software tuneable antenna systems [35].

2.5 Network Architecture

Cooperative communication allows users in a wireless network to share resources and create collaboration through distributed transmission and processing [33]. Cooperation is an essential part of cognitive radio development. It is important that secondary users in

the network are able to share information about network conditions, spectrum availability and the presence of malicious users. Cooperation promises significant capacity and multiplexing gains in CR users. It also realises a new form of space diversity to combat the detrimental effects of severe fading [33] upon observed radio environment conditions. However, cooperative communications use radio spectrum resources which is an overhead for the cognitive radio networks.

2.5.1 Distributed vs Centralised Architecture

Within wireless networks there are two distinct network architectures, known as distributed architecture and centralised architecture. The choice of which approach to use depends heavily on the operational environment of the wireless network, and neither architecture is applicable to all instances. The centralised approach uses a central node to regulate, collect and process all network traffic. The central node is sometimes called the master node, the server or the base station. Within this thesis we will refer to the central node as a base station or a central entity. In the centralised approach, each node within the network gathers information about its environment. Nodes within the network do minimal computation and processing of gathered information. Instead, gathered information is passed on to the central entity, which is responsible for information processing. The central entity uses this information to make decisions about spectrum status, bandwidth allocation, synchronisation and many other aspects. The central entity must ensure that the information coming from nodes is legitimate. User authentication is a key aspect to successfully implementing a centralised architecture in a wireless network. In Cognitive Radio Networks, a centralised architecture is common for resource management. When an idle spectrum band is discovered, secondary users commonly use a centralised base

station that assigns spectrum in a fair manner. Base stations are also commonly used to aggregate spectrum sensing results in large networks when single secondary users do not have the computational power to perform aggregation (which involves the combination of separate results into a single result representing the overall status of the network) of results independently [33]. In essence, in a distributed architecture all nodes are responsible for their own operations. Resource management and message exchange are done using group protocols that ensure that each user receives equal resources. .

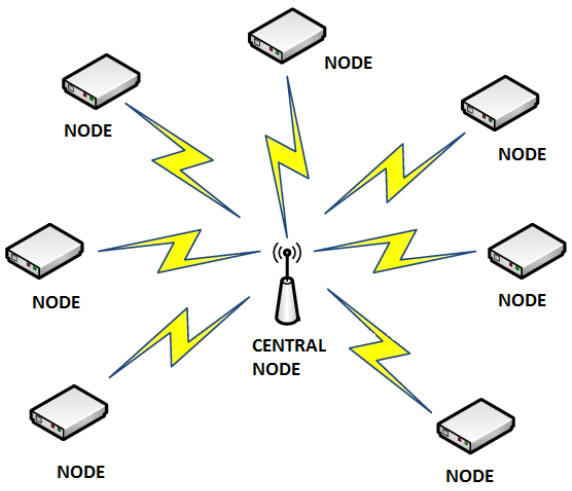

Figure 2.6: An example wireless network with a centralised architecture.

Cognitive Radio Networks use both a distributed and a centralised architecture. For the most part we assume that many of the devices that make up a network within the cognitive radio framework have fairly low computational power. A central entity must be employed to collect and process information, delegate resources and authenticate users. A great example of this is within a smart home. A user would utilise their smart phone as the central node, and the smart phone would receive and send information to each appliance, adjusting their operation to suit the preferences of the user. Fig. 2.6 shows

an example of a centralised wireless network where each user reports to a central base station. It would be responsible for resource allocation, authentication and if necessary synchronisation of the household appliances. At the same time, the appliances within the house would be communicating with each other to cooperatively achieve their goal. This type of network is often denoted as distributed. In a distributed network each user is responsible for their own data collection, processing and decision making.

Fig. 2.7 shows an example of a distributed wireless network, where each user is self-dependent and there is no central entity to congregate information. Therefore, distributed networks rely on users sharing information amongst each other. An example of this within the home network would be the light and the smart TV communicating to ensure that the best conditions for viewing are achieved.

One of the key advantages of Cognitive Radio networks has been their capacity to thrive in a distributed environment. Each secondary user in the network is able to collect information, learn from it and adjust their operation to suit their environment. In order for cognitive radios to be as effective as possible, each secondary user must communicate their spectrum sensing information to all their neighbours. In that way, each secondary user gets a number of spatial perspectives on whether the spectrum band is idle or not. User cooperation in Cognitive Networks as well as in all other wireless networks is the key to ensuring maximum accuracy of results. In the case of Cognitive Radio environmental degradation factors such as noise and interference fading and shadowing could affect spectrum sensing, resulting in a secondary user detecting to a wrong result about the activity of a primary user on a radio frequency band [51].

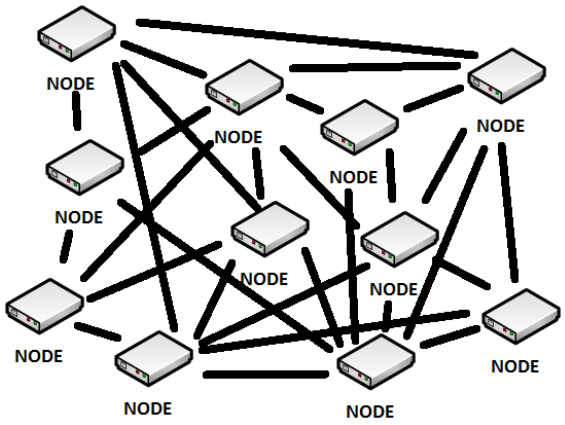

Figure 2.7: An example wireless network with a distributed architecture.

When deciding on which architecture to use within a wireless network, we must consider the advantages and disadvantages of each approach. The primary advantage of the centralised approach is that it takes the computational burden off users within the network. This enables users to conserve energy and resources and focus on operational goals and gathering information. As users do not have to do any complex computations, they are able to be smaller and cheaper. For example in large sensor networks, each sensor would have a small battery and high lifetime. This would allow network administrators to deploy complicated networks with higher cost efficiency. However, the centralised approach has a few disadvantages. Since all the processing is done at a central entity, if the central node were to fail the entire network would fail. This presents a great target for malicious nodes. Instead of trying to disable an entire network an attack could focus solely on the central node. For example, man in the middle attacks (where a malicious user intercepts data between two legitimate users) and emulation attacks (where a malicious node impersonates a legitimate user) would be very effective within a centralised framework. A malicious node could intercept communication between the central node

and its users, which with time would allow it to emulate the central node and take control of the network.

Attacks such as the man-in-the-middle attack and emulation attack do not have as much effect on distributed networks [52]. Since no central entity exists, the malicious user would only effect a very small part of the network. To effect the entire network, the amount of power and the time needed multiply quickly and are usually not feasible. This is a key advantage of distributed networks. Attacks on one or a small group of users within the network do not have a great effect on the rest of the network. As the number of users within the network increases, attacks on the network become less effective. This inherent feature of the distributed approach helps with its attack resilience, but it means that each user must perform all their own data gathering and processing. This means that nodes must now have sufficient storage and processing power, which leads to a number of disadvantages for network administrators. Firstly, the cost of such devices increases exponentially as the number of users within the network increases. Nodes will also be much larger in comparison to nodes within the centralised approach. However, the size difference with today's technological advancements would not be significant enough to have any serious effects. Centralised approaches are usually better suited for larger cities that have the funding and the architecture available to implement them. In a rural setting it becomes difficult, as nodes are scattered through a much larger area. Therefore, in remote areas distributed approaches are usually better suited. The algorithms presented in this thesis use both centralised and distributed approaches depending on the application and the complexity of the algorithm.

2.6 Transmitter Localisation

The localisation of a transmitter is a key aspect of wireless network technology [53]. Accurate localisation of users within a network is used many applications in both traditional wired and wireless networks. Not only is localisation needed in wireless networks to understand sensor data in a spacial context, it is used in many other applications such as navigation [54], social media platforms, location based billing and many others [55]. A number of localisation techniques has been proposed in the literature, most at their core are based on either Receive Signal Strength (RSS), Time Difference of Arrival (TDOA) or Angle of Arrival (AOA). These three form a basis for almost all localisation techniques in use in todays systems.

2.6.1 Received Signal Strength (RSS)

Receive Signal Strength (RSS) is seen as the simplest localisation method. In wireless communication, a signal that is sent between a transmitter and a receiver slowly gets weaker as it travels through air. The further away the signal travels the weaker it becomes. It is said that received signal power is proportional to $d^{-\alpha}$ [56], where d is the distance between a transmitter and the receiver and α is a propagation constant that represents how fast the signal attenuates as it travels through the environment, where $\alpha < 0$ and usually $2 < \alpha < 5$. A Large amount of research has gone into the development of accurate models to predict the impact that degradation effects have on RSS localisation. Over many decades, very accurate models have been developed. However, degradation effects such as noise and multipath fading are notoriously difficult to predict. This is primarily due to the fact that they vary significantly in different environments. For example, multipath fading on a channel can vary significantly with minimal changes in geometry, such as a car passing through the region between the transmitter and the receiver.

When a user receives a signal from a transmitter, the user can localise the transmit location using the receive signal strength. The received signal strength can be modeled as follows:

$$P_r = P_t d_t^{-\alpha} h_t + \eta, \tag{2.2}$$

where, P_r represents the Received Signal Strength (RSS) which corresponds to the received power from a transmitter, P_t is the transmit power of the transmitter, d_t represents the distance between the transmitter and the receiver, h_t is a shadowing variable, α is the path-loss constant and η represents noise power. When a secondary user receives a signal, the SU is able to estimate the distance to the transmitter. However, they do not know the direction of the signal. Fig. 2.9 the information that a user would have about the transmitter after it has received its signal. A user is able to calculate a circle with a radius corresponding to the distance between itself and the transmitter. This however does not give a single location for the transmitter, so a single user cannot accurately localise a transmitter alone.

A single user working alone is able to calculate the distance to the transmitter but cannot localise the exact location of the transmitter. To calculate the exact location of a transmitter three or more users must collaborate using a method called trilateration. Trilateration of a transmitter is shown in Fig. 2.10. We see that using three users we are able to calculate three circles which intersect at a single point. This point is where the transmitter is located.

RSS based methods are popular in low end systems. However, they have a number of disadvantages, that often make it unusable in certain environments. RSS measurements are significantly impacted by degradation factors such as noise, multipath fading and shadowing which often means that the radius of their circles can vary greatly when degradation factors are prevalent. This results in either no single intersection point for the

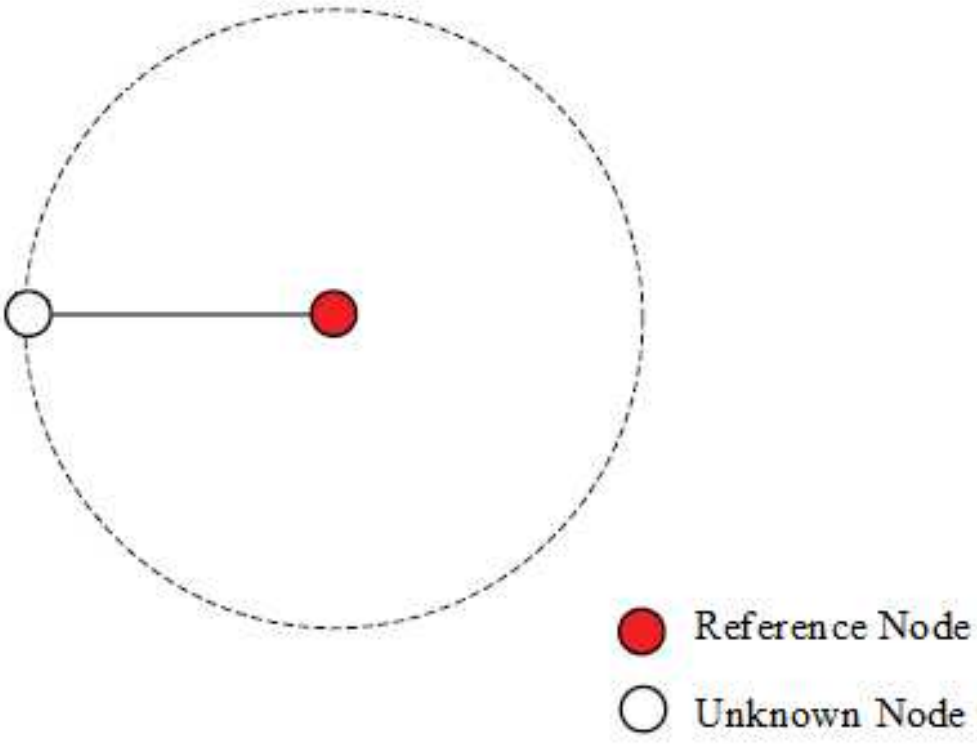

Figure 2.8: Localisation using RSS.

circles or the circles intersecting in the wrong spot. The major advantages of RSS are its low complexity, RSS does not need complicated equipment and RSS can be implemented in almost all systems. RSS often works well for smaller networks where the distances are not great, as the distances between users increases it become more unreliable.

2.6.2 Time Difference of Arrival (TDOA) and Time of Arrival (TOA)

Time Difference of Arrival calculates the location of a transmitter using the time of arrival of a signal two or more receivers. TDOA should not be confused with Time of

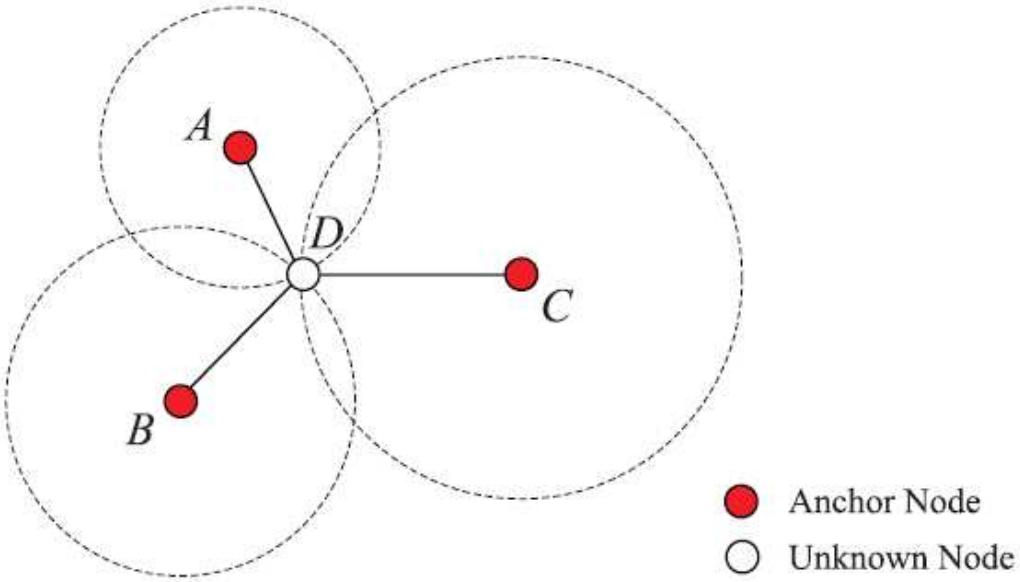

Figure 2.9: RSS localisation using trilateration.

Arrival(TOA). In TOA both the transmit time and the receive time must be known by the receiver in order for accurate localisation. Whereas, TDOA does not need the transmit time TDOA can calculate the location of the transmitter using the difference in arrival times between two receivers. Much like RSS, it is difficult for a receiver to accurately calculate the location of a transmitting node alone. As we see in Fig. 2.10 a number of users is needed for accurate localisation.

Both TDOA and TOA work well in large networks where users are located far away from each other. Unlike, RSS that suffers from degradation factors such as noise and multipath fading, TDOA and TOA are some what immune to multipath fading, which enables them to be more efficient in many applications. The implementation is more complex than RSS. It requires specialised equipment. The use of time and time difference also means that time synchronisation must be very accurate in both the transmitters and receivers. This requires extremely precise equipment that is often expensive and has a

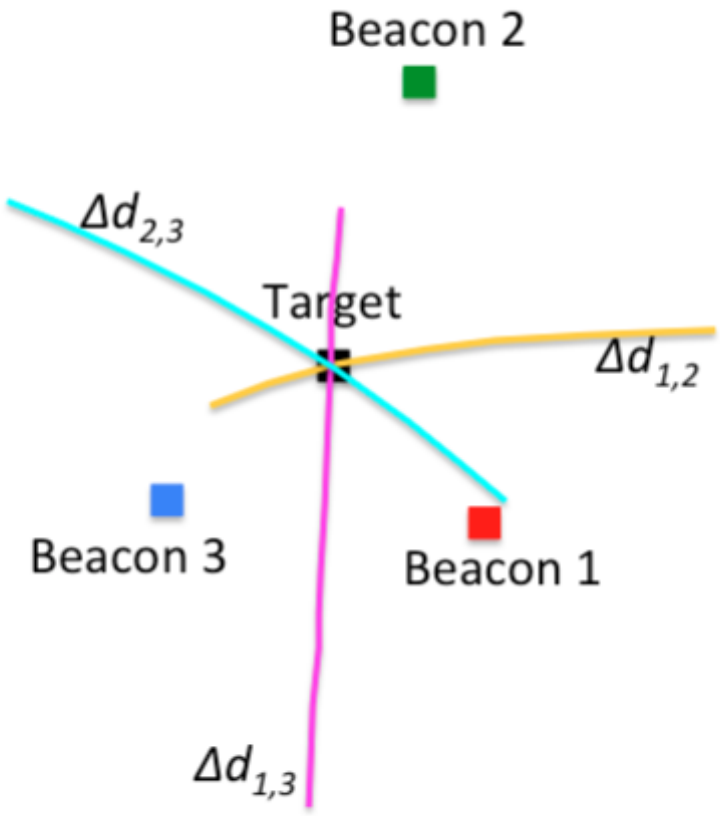

Figure 2.10: Localisation using TDOA [2].

high computational complexity.

2.6.3 Angle of Arrival AOA

Angle or Arrival is another technique that is used to localise a transmitter. AOA uses the direction of the incoming signal to localise the location of the transmitter. AOA uses a number of antenna elements often placed at certain positions in an array to compute the angle of the incoming signal. The structure of the elements can be modified to suit the application and they are often set up in a single line or in equal spaced positions around the circle. A typical AOA setup is shown in Fig. 2.11.

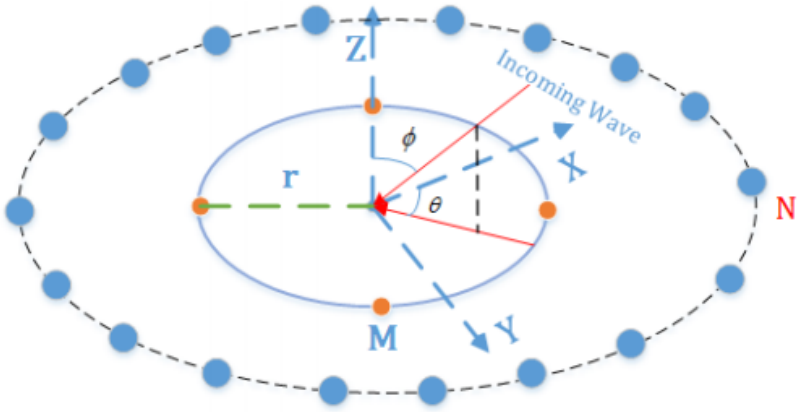

Figure 2.11: Typical antenna structure for AOA. [3].

AOA has a number of advantages over the other conventional techniques. It does not work with time like TDOA and TOA. Therefore, time synchronisation is not an issue. Unlike RSS it does not suffer from multipath fading effects, so it can be used over large distances with small fading degradation. AOA usually needs a number of antenna elements to produce accurate results. This is often difficult to implement in portable devices such as mobile phones because of the physical dimensions of the antenna array. In addition, the added hardware in the antenna array results in added cost for the user.

Chapter 3

Security Threats for a New Generation of Networks

Security is an essential component of any system. Increased reliance on computer based technologies has led to the simplification of many tasks. Tasks such as money transfers and withdrawals can now be made using a mobile phone with no need to carry cash or physically go to the bank. This has allowed many industries to become increasingly efficient and expand significantly. It has also created a dependance on such systems. As a result, much of our personal information is now stored on servers of companies that handle our finances or provide online services. Companies such as Uber are completely cashless, which means that they not only posses personal details they also have access to the financial information of many of their clients. Since Uber is a respected company, we assume that our personal information is not going to be used in a malicious manner. However, much like any other online business they are prone to attacks that could potentially cost its customers millions of dollars. A good example of such an attack can be seen in the attack perpetrated on eBay in 2013. The attack on eBay resulted on 145 million users being effected [57]. The official statement from eBay was as follows "hackers got

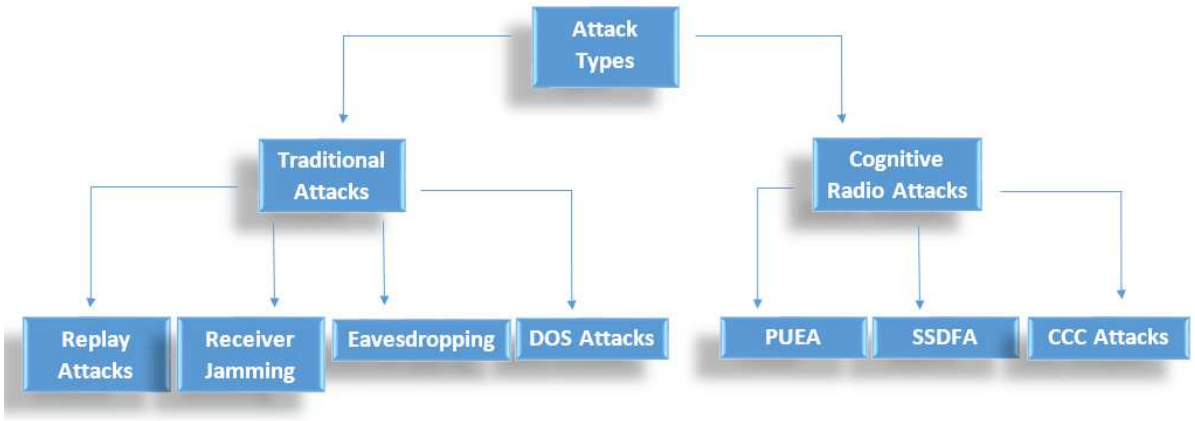

Figure 3.1: A summary of attack types in wireless networks.

into the company network using the credentials of three corporate employees" [57]. Unfortunately, eBay was not the only large cooperation to be attacked in such a way. Other notable attacks in the last couple of year include attacks on the Playstation network, Uber, JP Morgan and many more. In this section an introduction into of a number of security concerns for traditional networks, Cognitive Radio Networks and IoT networks. We see how these attacks can be used in subtle ways to gain access to some of the most secure networks on the planet. Fig. 3.1 provides an overview of the main types of attacks both on traditional networks and on CR networks.

3.1 Traditional Security Threats

Since the implementation of the internet, there have been individuals and groups that have attacked certain parts of the networks for a variety of reasons. Over the last few decades hackers have devised a number of attacks that exploit weaknesses in network architecture. These attacks are often performed remotely, with the victim rarely aware of the attack until it is too late. With the anonymity of the internet, it has become

very difficult to identify these hackers and seek retribution. It was decided that a more proactive approach was needed, and as a result we have seen a number of highly effective security frameworks being developed. With technological advances, we have a cat and mouse game being played out by the attackers and the security developers. We have seen attackers develop new and more effective techniques that have often resulted in security experts developing improved algorithms as countermeasures to the security attacks.

This section will detail a number of prominent attacks on traditional wired and wireless networks. We will present the advantages of group attacks, the effects of various attack types on networks. We will also present some popular methods to combat these attacks.

3.1.1 Group Attacks

Traditionally we have seen attackers classed as highly intelligent individuals who usually work alone. In reality, attackers often work in large groups located around the world. There are countless advantages of working in a group as opposed to working as an individual. A group have a great appeal to many individuals. It enables them to achieve much more and have access to resources that they would never have as an individual. In cognitive radio, group attacks consist of a number of individuals attacking various channels at the same to make it difficult for secondary users to gain access to spectrum. Even a small number of attackers working in conjunction with each other can have a serious impact on the secondary user throughput of the network. Therefore, it is important to consider not only the effects of single attackers but also the effects of a group of attackers working together when designing a mitigation algorithm. As attackers often attack in groups, it is logical that to prevent such attacks, users within the network work together in groups. Therefore, many of the mitigation schemes are formed with cooperation between secondary users as a basis for accurate detection and mitigation of network attacks.

3.1.2 Identity Theft

Identity attacks involve the impersonation of an individual to gain access to restricted/classified information or infiltrate private networks. Identity theft attacks represent one of the oldest types of attacks, not only in wireless networks, but in society. We have seen examples of identify theft throughout history, as a result we have seen the introduction of various identification methods, such as the drivers licence. Even with these measures we have seen the introduction of fake licences, so in many instances we use our own intuition, experience and common sense to identify identity theft. However, these methods of identification are usually not available in wireless networks. Therefore, a number of method to alleviate identity theft have been developed over the years. These include the introduction of the private/public key encryption [58], hash functions [59], reputation based functions, the use of certificates and many more. These methods look to establish trust between a sender and a receiver and they often do that using some sort of encryption method. Encryption methods usually work using a special key that both the parties are given at the commencement of their communication session. In general trust is the most effective way to mitigate identity theft attacks.

3.1.3 Man in the Middle Attacks

Man in the middle or eavesdropping attacks involve an individual intercepting information between two legitimate users. Intercepted information can be used for a number of purposes. For example, replay attacks are a type of man in the middle attack. During a replay attack, the attacker uses previously intercepted information to authenticate themselves. For example, if two users want to communicate with each other such that user 1 wants to communicate with user 2, user 2 would request a password from user 1 to make sure that it is legitimate. If the attacker were listening and intercepted the information,

the attacker could keep a copy of it. As a result, at a later date the attacker would be able to falsely authenticate themselves as user 1. This type of attack is extremely dangerous and it is very difficult to mitigate. It is used extensively not only in wireless networks but also the internet with the use of Malware. Attackers can gather information on a host PC using a pre-installed program that can be hidden in web sites and applications. Much like identity theft, man-in-the-middle attacks are often mitigated using trust establishment techniques. Examples of such techniques include hash functions [59] and reputation based functions [23]. These aim to continually authenticate users making it difficult for attackers to penetrate the network.

3.1.4 Denial of Service Attacks

A Denial-of-service (DOS) attack [60] aims to disrupt the network by limiting access to resources for legitimate users. This is usually accomplished by flooding the network server. Flooding the network involves sending out large amounts of information to create a bottle-neck, which causes the server to become congested and not able to handle traffic and requests from legitimate users on the network. This attack is very common as it does not require any specialised equipment or a great deal of expertise to accomplish. In fact, a large amount of software has been developed to perpetrate DOS attacks with the push of a button and they are often freely available on the internet. DOS have been implemented successfully a number of times, most notably in 2016 when the largest attack in history was conducted on a company called GITHUB [61]. It was estimated that 1.35GB were flooded through their networks each second, rendering their servers unusable an extended period of time. One method of mitigating DOS attacks is to implement access control lists on routers. These allow routers to only accept packets from recognise IP addresses. All other packets from other IP addresses are discarded as soon as they arrive. If implemented correctly, this is an effective method to mitigate this type of attack. However, it has some

limitations. For example, the access control lists grow very quickly as the number of legitimate users becomes large.

3.2 Cognitive Radio Based Attacks

In addition to the traditional attacks, Cognitive Radios are prone to a number of new more sinister attacks. The cognition ability that is proposed as a central feature of cognitive radio is one of its main advantages. This ability helps it mitigate a number of traditional attacks. However, additional features and capabilities introduced for legitimate users are also available to adversaries. Such abilities are often used to conduct specialised attacks. Security vulnerabilities are often seen as a primary deterrent to full implementation of cognitive radio technology in today's communication systems. It is therefore essential to develop highly effective mitigation methods to ensure a high level of security for users in cognitive radio networks. This section introduces the most serious types of attacks on cognitive radio networks.

3.2.1 Primary User Emulation attacks (PUEA)

Primary user emulation attacks are seen as the most serious type of attack on the physical layer. In order for secondary users to access network resources, they must scan the radio frequency bands looking for idle channels that they can utilise. When a secondary user finds idle channels, the SU is free to share it with other secondary users as long as the primary user does not become active. If the primary user does become active, all secondary users on the channel must vacate it immediately to ensure that there is no interference between them and the primary user. This inherent feature of cognitive radio is one of its key features. It enables secondary users to utilise the available spectrum which is under utilised by primary users. With a great emphasis on spectrum sensing and continually

monitoring of the channel, an attacker might identify spectrum sensing as a possible area to exploit. If, for example, an attacker were to mimic a primary user and trick legitimate secondary users into thinking that the primary user has become active, the attacker would have an entire channel vacant for their own personal use. The emulation of a primary user in this way is called a primary user emulation attack(PUEA) [**?**].

Research into primary user emulation attacks has been growing steadily over the last few years and we have seen a number of effective mitigation techniques proposed to identify and mitigate against primary user emulation attacks. In this thesis, we propose a localisation based method to identify the location of a transmitter(either an attacker or a primary user) and compare this location to the location of the primary user. If two locations correspond we say that the transmitter is in fact the primary user. If not, the transmitter must be an attacker. Methods have been proposed using RSS, TDOA, TOA and AOA, with each having various advantages and disadvantages [62]. The significant advantage of these methods is that the primary user does not need to be modified at all for the methods to be effective. Other methods utilise the signal characteristics of primary users [63]. These often identify the transmitter by comparing the incoming signal with a sample of a primary users signal. If they match, the transmitter is deemed a primary user. These methods are very effective. However they need fairly complicated equipment to analyse incoming signals, which is not always practical for implementation in cognitive radio devices.

3.2.2 Spectrum Sensing Data Falsification Attacks (SSDFAs)

Spectrum Sensing Data Falsification Attacks involve a malicious node spreading falsified spectrum sensing results throughout the network to try and influence secondary users into a wrong conclusion about channel availability. This type of attack is especially potent in cognitive radio networks because of their distributed nature, which means that secondary

users often rely on each other's observations to get accurate results. Therefore, this attack is extremely effective and often has a domino style effect that is propagated throughout the network. It is therefore essential that effective methods are developed to mitigate SSDFAs. Unlike PUEA, SSDF attackers can have more than one motive to attack. Therefore, we classify the following three types of spectrum sensing data falsification attackers:

- Selfish Attackers - attackers attempt to convince legitimate secondary user that the channel is occupied by a primary user to attempt for them to gain access to the channel uncontested.

- Malicious Attackers - attackers cause interference between secondary users and primary users. They try to convince secondary users to transmit on a channel that is being used by the primary user, which creates interference to the primary user.

- Accidental Attackers - these often include secondary users that are effected by some degradation factors that result in inaccurate spectrum sensing results. Other possible reasons include a malfunctioning node that sends out falsified spectrum sensing results without realising it. This form of attack is somewhat rarer than the previous two but must also be mitigated effectively.

A number of methods have been proposed to mitigate against SSDFAs [64]. Most attempt to establish a trust between secondary users within the network. The trust is usually a dynamic function that rewards secondary users who send out legitimate results and punish secondary users who send out falsified results. In this thesis, we propose a reputation based scheme that works exactly in this way. However, we develop an algorithm that takes into account a number of additional scenarios and attack types for which no mitigation techniques have been suggest in the previous literature.

3.2.3 Common Control Channel Attacks

Establishment of spectrum sharing and common procedures to establish communication between two secondary users is conducted on a dedicated channel called a common control channel. This is usually done so the rest of the spectrum is left vacant for data transmission. In the context of cognitive radio networks the common control channel is used for transmitter-receiver handshake, neighbour discovery, forwarding topology and route change updates [65]. The importance of a safe and secure common control channel is essential in establishing a reliable environment for secondary user opertaion. However, because of its importance, the common control channel is often seen as a target for attacks. Attacking the common control channel is a convenient way for attackers to efficiently disrupt communications within a cognitive radio network. If the control channel is disabled, secondary users have no way of communicating with each other. This causes massive problems, particularly in spectrum sensing phases, where secondary users rely on each other to obtain accurate results. Attackers are able to inflict massive damage on the network with relatively little effort. Instead of attacking an entire network, a smart attacker would focus its resources on disabling the control channel, which would effect the entire network.

In fact, common control channel attacks can be done so efficiently that it is often enough for a single attacker to conduct a full attack without the need of additional support. This makes them extremely dangerous and has prompted a number of mitigation methods to be established by the research community. Traditionally, networks have dedicated a single common control channel that is known by the entire network and never changed. It was quickly recognised that this method of establishing the common control channel was not secure. The static nature of such an allocation means that it is constantly under threat from attackers. If an attacker were successful in their attack, there exists no other method for secondary users to communicate. The attacker can simply continue

the attack indefinitely. Static allocation of the control channel was quickly replaced by sequential and pseudo-random methods. A central base station is a common facilitator of such schemes. In a sequential scheme, users are given a number of frequencies that can be used as the common control channel. Initially, the first frequency is used. Then if there is an attack on that frequency, users simply move to the next frequency and continue communication. This method of mitigation is fairly effective unless the attacker is able to obtain the sequence, in which case it becomes ineffective. Random schemes usually involve the central base station choosing a random frequency channel and changing it randomly with time or when it senses that it has been compromised. This method is more effective than the sequential method but it has a larger amount of overhead. The nodes are synchronised using randomised sequences. Synchronisation can be achieved by using GPS (Global Positioning System) clock, by a central base station or through direct communication between two secondary users. GPS synchronisation is achieved by a secondary user with the help of orbiting satellites. Their position and the time it takes the signal to reach the receiver gives both the location and the time delay which allows users to synchronise their clocks [66]. Centralised synchronisation is achieved by synchronising users to a master clock that is kept at a centralised location. Each secondary users synchronises to the master clock and therefore each other. Distributed synchronisation between two users is done by using one receiver as a references and synchronising the other to match. This method is less effective because the synchronisation only applies to a pair of secondary users [67].

The distributed nature of cognitive radio networks means that there is often no central base station to establish and change the common control channel. Allocation of a common control channel then often falls on groups of secondary users. In general, when a channel is identified as useable, a group secondary users can share that channel, but they must be able to communicate with each other to establish communication parameters. A

number of methods exist to effectively establish a safe and reliable common control channel. Much like traditional systems, frequency hopping rendezvous based methods (where secondary users hop through channels until they meet) are the most popular and most effective methods. Often pre-set sequences are exchanged, which enables secondary users to quickly switch between channels should they become compromised. Common control channel attacks are an efficient way for attackers to disrupt the network. Unlike conventional attacks, in which entire bands must be jammed, in CCC attacks a much smaller partition of the band is attacked. This intelligent type of attacking network resources means that a single attacker is now able to jam multiple band simultaneously, without the need of any specialised equipment and with minimum power output.

3.3 New Class of Attacks

Attackers are constantly attempting to find different methods to attack networks. In SSDFAs, attackers sent out falsified information to legitimate secondary users in order to trick them into concluding false spectrum sensing results. The cooperative nature of cognitive radio means that these results are often propagated throughout the network and have long lasting effects on network performance. This type of attack is highly effective and needs a fraction of the resources required for other attacks. This means that it can be conducted frequently and in a number of channels, making it essential that effective mitigation methods are developed. SSDFAs are often mitigated using reputation based schemes where users are assigned a reputation that is increased/decreased according to the legitimacy of spectrum sensing results. These methods are often very effective, which has prompted attackers to find ways to exploit such mitigation schemes. Two types of attacks that look to exploit reputation based schemes are the Reputation Mining Attack and the Reset Attack, which are described in the next two sections.

3.3.1 Reputation Mining Attack

Reputation mining attacks are based on increasing one's reputation by reporting legitimate spectrum sensing information for a period. Then, when one has increased their reputation and is trusted by everyone on the network, the attack can begin. With most reputation based schemes, users with a high reputation have a greater say in the overall consensus of the network as they are seen to be trusted users. This means that when an attacker has a high reputation they are able to cause maximum damage to the network.

This form of attack is often not considered in the tradition mitigation methods. We develop a method in this thesis that mitigates this type of attack. We develop a method that uses a combination of an outlier detection method with a "thee-strike" rule (where a user is kicked out if they do the wrong thing three times). When a spectrum sensing report comes, a determine is performed to check whether the spectrum sensing report represents and outlier or if it is within the range of other spectrum sensing results. If it is not, it is discarded and the sender is cautioned. If this happens repeatedly, the secondary user is dropped from the network. This form of attack could have serious implications if it is not mitigated effectively.

3.3.2 Reset Attack

Reset attacks also take advantage of reputation based mitigation schemes in cognitive radio networks. In a reset attack, the attacker continually sends out falsified information until their reputation is low, at which time they reset their device (turns it off and after a period turns it back on, appearing to be a new user), which resets their reputation to the default value. This allows them to continue to send out falsified results. To mitigate against this type of attack a probation function is introduced in which every new secondary user that comes on the network must wait for a probation period before they are able to

contribute to the consensus of the network. During the probations period the new user must still send out spectrum sensing reports which means that their reputation value is going to be effected by falsified results. This ensures that after they are identified before they can have an effect on secondary users results.

Chapter 4

Mitigation of Primary User Emulation Attacks

In this chapter we present a belief propagation based method to identify and mitigate against primary user attacks [68]. The contributions of this chapter can be summarised as follows:

- Significant reduction of in computational complexity of the algorithm compared to existing algorithms. Convergence time is reduced significantly in both small and large networks. This improvement is especially evident in large networks with thousands of users. In which case, the convergence time is decreased from a few hours to a few seconds.

- An increase in performance accuracy through the introduction of a compatibility function that increases cooperation between secondary users compared to already existing algorithms. Increased cooperation means that secondary users have more information available to them, which enables them to make more accurate decisions.

- With these improvements the belief propagation algorithm is low in computational

complexity and able to effectively and quickly determine whether the transmitter is a primary user or a primary user emulator. It's incredibly fast convergence time and lightweight nature make it perfect for implementation in highly distributed networks.

The first part of the chapter outlines the framework used throughout this thesis. The basic belief propagation framework is introduced. We then present a newly developed belief propagation algorithm that is both computationally faster and more efficient than the existing belief propagation based methods. The new algorithm has a number of key improvements. The first, is a simplified local function that significantly reduces the computational complexity of the algorithm while increasing the efficiency. This key improvement allows us to reduce the time of convergence of the original algorithm [**?**] from a couple of hours (in cases where there are several thousand users) to a couple of seconds. At the same time, the efficiency and accuracy of the algorithm are slightly increased. The introduction of the new local function significantly decreases computational complexity and improves primary user detection performance. In addition to the introduction of the new local function, a new and improved compatibility function is introduced. The new compatibility function has a dual impact. Much like the local function it decreases the computational complexity of the algorithm. In addition, the new compatibility function increases the level of cooperation between secondary users in the determination of whether the channel is occupied by a primary user or a primary user emulator. With an increased cooperation between users, the primary user detection accuracy of the algorithm increases. This is due to the increase in the amount of information each secondary user has about the status of the spectrum. With more information, a secondary user is able to make a more informed decision about whether channels are occupied by primary users or vacant.

4.1 Belief Propagation

Belief propagation is known as a message passing algorithm. For communication networks it is primarily used in distributed networks where secondary users are able to communicate with each other. It allows for a high level or cooperation between secondary users which results in high accuracy spectral sensing. We use belief propagation to incorporate a number of secondary user observations into a single probability at a user that corresponds to whether or not a primary user is active on a radio frequency band.

4.1.1 Original Belief Propagation Method

Belief propagation provides high accuracy detection of primary user emulation attacks. In belief propagation, each secondary user performs local observations and calculates the probability that the channel output is an incoming signal belonging to a primary user. To accurately detect the presence of a malicious user, neighboring nodes must communicate with each other and exchange local observations. If a user does not have access to other users; local observations the local user will not have accurate results (due to noise and shadowing effects). Local observations are exchanged in the form of messages. Each secondary user computes a belief about whether the suspect is a primary user or an attacker according to its own local observations and the sum of all incoming messages from all its neighbours. A final belief is calculated using the sum of all beliefs from all SU. This final belief is compared to a preset threshold. If the belief final is above the threshold, the suspect is deemed to be a primary user. If it is below the threshold, the suspect is considered to be a malicious user. The belief propagation framework is based on pairwise Markov Random fields(MRF) [69].

Relative power observations of secondary users represent a pattern of receive powers which characterise by the location of the transmit station. The exchange of information

between secondary users enables recognition of patterns for the purposes of determining whether or not the transmission originates at a known primary user location. In MRF, we define Y_i as the local observations at secondary user i, and X_i as the state of the suspect observed at user i. If X_i=1, the suspect is a primary user and if X_i=0, the suspect is a malicious user. The local function at user i is defined as $\phi_i(X_i, Y_i)$. The local function represents the observations made by a secondary user i about whether the suspect is a primary user or not. The compatibility function $\psi_{ij}(X_i, Y_j)$ is used to model the relationship between secondary users. The larger the compatibility function between two users is, the more relevant the local observations of the two users become to each other. For example, if SU_1 is 1m away from SU_2 and SU_1 is 30m away from SU_2, then local observations that come from SU_2 to SU_1 will be more relevant to the final belief of SU_1 then local observations that come from SU_3. This is because close-by terminals have similar shadowing while distant terminals have essentially independent shadowing. The conditional probability distribution of the set of random variables ($\{X_i\}$ has a joint probability function given by:

$$P(\{X_i\}|\{Y_i\}) = \prod_{i=1}^{M} \phi_i(X_i, Y_i) \prod_{\substack{j=1 \\ j\neq i}}^{M} \psi_{ij}(X_i, Y_j), \tag{4.1}$$

where, M is the number of secondary users in the network. We aim to compute the conditional probability at secondary user i, which we denote as the belief. The belief at a secondary user i is given in equation Eq. (4.2). It is the product of the local function at user i and all messages coming into user i from all the neighbours of i:

$$b_i(X_i) = k\phi_i(X_i, Y_i) \prod_{\substack{j=1 \\ j\neq i}}^{M} m_{ij}(X_i), \tag{4.2}$$

where, X_i is the state indicating whether the channel is in use by a primary user or an emulator, Y_i is the local observation at secondary user i, $b_i(X_i)$ is the belief of state X_i at

secondary user i, $\phi_i(X_i, Y_i)$ is the local function at secondary user i, $m_{i,j}$ is the message sent from secondary user j to secondary user i indicating the belief of secondary user j of the state of X_i, and, k is a normalisation constant to insure that the beliefs sum to 1. Therefore,

$$1 = b_i(0) + b_i(1) = k\phi_i(0, Y_i) \prod_{\substack{j=1 \\ j \neq i}}^{M} m_{ij}(0) + k\phi_i(1, Y_i) \prod_{\substack{j=1 \\ j \neq i}}^{M} m_{ij}(1) \tag{4.3}$$

As a result, we are able to derive k as follows:

$$k = \frac{1}{k\phi_i(0, Y_i) \prod_{\substack{j=1 \\ j \neq i}}^{M} m_{ij}(0) + k\phi_i(1, Y_i) \prod_{\substack{j=1 \\ j \neq i}}^{M} m_{ij}(1)} \tag{4.4}$$

In order to compute the belief at each user, a message exchange equation is introduced, that can used to iteratively update the belief at each secondary user. For the lth iteration (defined as one cycle of message exchange which ends when all secondary users exchange messages, a secondary user j sends a message $m_{i,j}^l$ to secondary user i which is specified by,

$$m_{ij}^l(X_i) = C_i \sum_{\substack{j=1 \\ j \neq i}}^{M} \psi_{ij}(X_i, Y_j)\phi_j(X_i, Y_j) \prod_{\substack{k=1 \\ k \neq j}}^{M} m_{j,k}^{l-1}(X_i) \tag{4.5}$$

where, $\psi_{ij}(X_i, Y_j)$ is the compatibility function which indicates the relative conditional of observation Y_i upon observation Y_j at secondary user j, $\phi_j(X_i, Y_j)$ is the local function at secondary user j, and C is a normalisation constant such that $m_{ij}^l(1) + m_{ij}^l(0) = 1$. Therefore,

$$C_i = \frac{1}{\sum_{j=1}^{M} \psi_{ij}(0, Y_j)\phi_j(0, Y_j) \prod_{\substack{k=1 \\ k \neq j}}^{M} m_{j,k}^{l-1}(0) + \sum_{j=1}^{M} \psi_{ij}(1, Y_j)\phi_j(1, Y_j) \prod_{\substack{k=1 \\ k \neq j}}^{M} m_{j,k}^{l-1}(0)} \tag{4.6}$$

The iterative computation is continued until there is a convergence to the limit,

$$m_{i,j}(0) = \lim_{l\to\infty} m^l_{i,j}(0), for j = 1, 2, ..., M \quad for \quad j \neq i$$

$$m_{i,j}(1) = \lim_{l\to\infty} m^l_{i,j}(1), for j = 1, 2, ..., M \quad for \quad j \neq i$$

The steady state messages $m_{i,j}(1)$ are then used to compute,

$$b_i(1) = k\phi_i(1, Y_i) \prod_{\substack{j=1 \\ j\neq i}}^{M} m_{ij}(1), \tag{4.7}$$

The message exchange in establishing the belief is equivalent to how members of a committee formulate their beliefs based, in part, on the beliefs of the other committee members.

Finally, when all secondary users finish computing their beliefs they are added up and averaged to derive a final belief. The final belief is then compared to a predefined threshold. If the final belief is higher than the threshold, the suspect is believed to be a primary user. If the final belief is lower than the threshold the suspect is believed to be a malicious user:

$$Decide : H_0 : X_i = 1, i = 1, 2, ..., M \quad \frac{1}{M} if \sum_{i=1}^{M} b_1 \geq \tau_b$$

$$Decide : H_1 : X_i = 0, i = 1, 2, ..., M \quad \frac{1}{M} if \sum_{i=1}^{M} b_1 < \tau_b,$$

where, M is the total number of secondary users in the network, $\sum_{i=1}^{M} b_i$ denotes the sum of all the beliefs of all the secondary users on the network and b_τ denotes the pre set threshold. It is possible that some users would relay inaccurate information to other users in the network. However, inaccurate information by a small number of nodes would not influence the final belief value significantly.

Local Function

The local function represents the local observations at a single secondary user. Each secondary user calculates its own local function which corresponds to a probability of a suspect being a primary user. To calculate the local function we must compute two probability density functions (PDFs). The first PDF is computed using the RSS measurements that are computed from the primary user location and is denoted by PDF_{pu}. The second is a PDF that is computed using RSS measurements acquired from the attacker received signal and is denoted by $PDF_{attacker}$. The local function corresponds to the similarity between the two PDFs. If the PDFs are the same the local function returns a probability equal to 1, which indicates that the suspect is transmitting from a primary user location. The more dissimilar the distributions are, the lower the local function and the higher the probability that the suspect is an attacker. We define, location 1 as the location of SU_1 and location 2 as the location of a close by SU_2. The theoretical ratio received signal power from the primary user at secondary user locations 1 and 2 which is based on the distances between the primary user k and secondary users 1 and 2 respectively, can be obtained using the following equation:

$$\frac{P_{r1(PU_k)}}{P_{r2(PU_k)}} = \left(\frac{d_{1(PU_k)}}{d_{2(PU_k)}}\right)^{-\alpha} \left(\frac{h_{1(PU_k)}}{h_{2(PU_k)}}\right), \tag{4.8}$$

where, $P_{r1(PU_k)}$ and $P_{r2(PU_k)}$ are the RSS power values from a primary user(PU_k) to SU_1 and SU_2, $d_{1(PU_k)}$ and $d_{2(PU_k)}$ are the distances between PU_k and SU_1 and SU_2, respectively. $h_{1(PU_k)}$ and $h_{2(PU_k)}$ represent the shadow fading between PU_k and secondary users SU_1 and SU_2. It is assumed that the shadow fading, $h_{i(PU_k)}$ is a circular Gaussian variable $\mathcal{CN}(0,1)$. If we define q as:

$$q = \frac{h_{1(PU_k)}}{h_{2(PU_k)}} \tag{4.9}$$

We can then define B as:

$$B_{i,j} = \left(\frac{d_{i(PU_k)}}{d_{j(PU_k)}}\right)^{-\alpha} \tag{4.10}$$

$B_{i,j}$ will be expressed as B for notational convenience. Therefore, the primary user's PDF can be written as follows:

$$PDF_{PU_k} = \frac{1}{\mid B \mid} \frac{2\frac{q}{B}}{((\frac{q}{B})^2 + 1)^2} \tag{4.11}$$

The PDF for the attacker, which is based upon received power measurements at two secondary user, is defined in a very similar way to the PDF of a primary user. SUs collect RSS measurements which they then exchanged with their neighbours. We define $P_{r1(attacker)}$ and $P_{r2(attacker)}$ as the received signal strength from the attacker to SU_1 and SU_2 respectively, and the distances between SU_1 an SU_2 and the attacker as $d_{1(attacker)}$) and $d_{2(attacker)}$) respectively. We can then define the value of $A_{i,j}$ as follows:

$$A_{i,j} = \left(\frac{d_{1(attacker)}}{d_{2(attacker)}}\right)^{-\alpha} = \frac{P_{r1(attacker)}/P_{r2(attacker)}}{\pi} \tag{4.12}$$

Therefore, the attackers PDF can be written as follows:

$$PDF_{PU_{attcker}} = \frac{1}{\mid A \mid} \frac{2\frac{q}{A}}{((\frac{q}{A})^2 + 1)^2} \tag{4.13}$$

To compare the two PDFs we use the Kullback Leibler distance. The Kullback Leibler distance is defined as:

$$KL_{(PDF_{PU_k}, PDF_{attacker})} = \int_0^\infty PDF_{PU_k} log \frac{PDF_{PU_k}}{PDF_{attacker}} dq \tag{4.14}$$

The KL distance calculates the difference between the two PDFs, one based on the receiver powers and the other being the theoretical and based on distances between the receiver and transmitter. If the difference between the PDFs is large the KL formula will return a large number and if the distance is small the KL formula will return a small number. To obtain the local function from the KL distance we use the following formula:

$$\phi_i = \exp(-minKL_{(PDF_{PU_k}, PDF_{attacker})}) \tag{4.15}$$

The local function returns a variable that is proportional to the probability that a suspect is a primary user. The higher the value of ϕ_i, the more likely the suspect is a primary user. The lower the value of ϕ_i, the less likely it is that the suspect is a primary user.

Compatibility Function

The compatibility function is essential for cooperation between secondary users. In the belief propagation framework, the compatibility function is a scalar. The higher the compatibility function between two SUs the more relevant the information from one SU is to the the second SU. A compatibility function, reflecting this relationship is defined by the following expression:

$$\psi_{i,j}(X_i, Xj) = \exp(-Cd^{\beta}_{SU_i,SU_j}) \tag{4.16}$$

Where C and β are constants, d_{SU_i,SU_j} represents the distance between secondary users i and j. The compatibility function is heavily dependent on the distance between the two secondary users because the similarity of shadowing depends upon distance. Secondary users which are close in distance will have similar shadowing. If the distance between the secondary users is large then the compatibility function tends to zero. If the distance between secondary users is small the compatibility function tents to 1.

The compatibility function is used to insure that users that are far away do not have a large contribution to each others beliefs. The reason for this is that secondary users at different locations suffer from different shadow fading and the further away users are the less likely that their belief will correspond with each other. It also insures that users that are closer to each other have a greater impact on each other's belief.

Complete Algorithm

The belief propagation algorithm used in this paper is summarised in Algorithm 1. Each secondary user performs measurements and calculates their PDF_{PU_k} and their $PDF_{attacker}$ using Eq. (4.9) and Eq. (4.11). Using these measurements each secondary user iteratively computes their local and compatibility functions using Eq. (4.13) and Eq. (4.14). Each secondary user then computes and exchanges messages with all its neighbouring nodes.

The last step of the algorithm is where each secondary user calculates their belief using their own local observations and the product of all the messages from all their neighbours.

After a number of iterations the mean of all the beliefs is calculated and compared to a predefined threshold. If the final belief is lower than the threshold, the suspect is detected as an attacker. If the final belief is greater than the threshold, the suspect detected a primary user. In both cases the final decision is relayed to all secondary users who will either ignore the transmitter (if he is an attacker) or conclude that a primary user is active and look for another band to transmit on. The algorithm converges when there is no significant change in the final belief from the previous iteration to the current iteration. A reasonable termination rule for the algorithm is:

$$| b_i^{l-1} - b_i^l | < 0.001, \tag{4.17}$$

where, b_i^l is the final belief at iteration l, for all $1 \geq 1 \leq m$. Since at every iteration the final belief is going to change (the higher the iteration the smaller the change), we set a threshold for change at 0.1%. If the change from the previous iteration to this one is less than the algorithm is said to have converged to its final value. In [10] the authors claim that the algorithm is able to converge to a satisfactory result within 8 iterations. The results of the belief propagation based strategy depend on the ability of secondary users to communicate with each other. With more cooperation between secondary users exists greater accuracy is achieved.

Algorithm 1 Complete defence strategy against the PUEA using belief propagation

1: Each secondary user performs measurements using Eq. (4.8) and Eq. (4.10)
2: While $\mid b_i^{l-1} - b_i^l \mid < 0.001$, for all $1 \geq 1 \leq m$
3: **for** Each iteration **do**
4: Compute the local function using Eq. (4.15) and the compatibility function using Eq. (4.16)
5: Compute messages using Eq. (4.5)
6: Exchange messages with neighbours
7: Compute beliefs using Eq, (4.2)
8: **end for**
9: Break
10: The PUE attacker is detected according to the mean of all final beliefs based on comparison against threshold.
11: Each SU will be notified about the characteristics of the attacker's signal and ignore them in the future.

4.2 Iterative Belief Propagation

This section provides an outline of the changes that were made to the algorithm presented in [10]. These modifications are a significant research outcome and provide a significant improvement to the algorithm. We used MATLAB simulations to demonstrate the significant improvement of the algorithm. The two most significant improvements made to the old algorithm are (1) the new simplified local function which greatly decreases the computation complexity of the algorithm, from a few hours in some cases to a couple of seconds, and (2) a new compatibility function which allows for a higher degree of cooper-

ation between secondary users resulting in an increase in the accuracy of the algorithm. The more cooperation exisits between secondary users the more information is available. This results in secondary users making highly accurate decisions.

Local Function

The local function that was used in the original technique [**?**] suffered from being overly complicated and introducing a high level of complexity into the algorithm making it slow to converge. Our key contribution was the development of a simpler more efficient local function. The new local function is just as accurate as the previous function. However, instead of doing a large number of integrals for each secondary user in the network the new function calculates a simple arithmetic equation that allows the system to grow linearly instead of exponentially. The new local function that exhibits these desirable characteristics is:

$$\phi_{i,j} = \frac{\mid A_{i,j} - B_{i,j} \mid}{A_{i,j} + B_{i,j}} \tag{4.18}$$

We define $A_{i,j}$ as a theoretical measurement (Eq. (4.10)). It is essential the baseline measurement (the actual RSS value corresponding to the PU localtion), which we compare with the incoming measurement, denoted as $B_{i,j}$ (Eq. (4.8)). The local function is a measure of the similarity between the RSS measurements from a PU and the RSS measurements from a suspect. The closer the correlation between the two RSS values the more likely it is that the suspect is a primary user. The method used to obtain the local function in the old algorithm was over complicated and significantly increased the computational time and complexity. This was primarily due to the fact that the Kullback Leiber(KL) distance was used to calculate the difference between the two probability density functions. The problem with the KL distance is that it uses an integral to determine the difference between two variables. This introduces an unwanted amount of

complexity into the algorithm and makes it slow to converge. In Eq. (4.16) we present a new local function that calculates the difference between the RSS measurements using a simple difference equation that is orders of magnitude faster than the KL distance. By replacing the integral and using a simple arithmetic operation, we were able to obtain a high level of accuracy while keeping the computation complexity very low. As the number of secondary users on the network increases, we see a significant difference between the two methods. This is primary due to the fact that the local function has to be evaluated for each pair of secondary users in the network. As as we add more SUs to the network, the number of calculations of the local function increase exponentially. In the sections that follow, we present results that verify that our new local function achieves results that are more accurate and more efficient than those obtained by the previous local function.

Compatibility Function

The compatibility function that was presented in the original paper [**?**] discouraged co-operation between secondary users in the CR network and as a result decreased the accuracy of the final belief. This was primarily due to the fact that the compatibility function returned values that were very close to zero unless secondary users located in close proximity. For example, if the distance between the secondary users is 2 meters the compatibility function returns a value that causes messages that are exchanged between the two users to be meaningless. After a large number of tests and simulations a modified version of the compatibility function was derived as:

$$\psi_{i,j}(X_i, Yj) = \exp\left(\frac{-d_{SU_i,SU_j}}{100}\right) \tag{4.19}$$

This compatibility function insures that secondary users that are close to each other are able to cooperate and share their result effectively to increase the accuracy of the results. The goal of the modified function is to insure that the messages between secondary

users on the network are more relevant. We show in the next section that the modified compatibility function is able to improve the performance of the algorithm by allowing a greater degree of cooperation.

4.3 Simulation Results and Analysis

In this section we present the results of the original [**?**] BP algorithm against the improved BP algorithm. We compare the results of the two algorithms to determine which is more effective in combating primary user emulation attacks against cognitive radio networks. The first part of this section focuses on the results that were obtained in [10]. The second part presents the results that were obtained by us using the modified local and compatibility functions. In the last part of this section we compare the two algorithms according to their efficiency and accuracy. All simluation was done using an Intel(R) Core(TM) i7-3930k CPU, using MATLAB as a simulation tool.

We chose to use similar simulation parameters as those presented by the authors in [10]. We set the path loss constant α as 2.5, the transmit power of the secondary user is 0.1W (since the malicious user is also using a cognitive radio this is also the transmit power of the malicious user, we assume this corresponds to a transmission range of about 20 meters). There are 30 secondary users, one primary user and one malicious user deployed in a 100m by 100m grid. Fig. 4.1 provides an illustration of the CR network model that was used throughout paper.

4.3.1 Original BP Results and Analysis

This section outlines the results that were obtained in [10]. The authors went through a number of scenarios where they moved the locations of the primary and malicious users

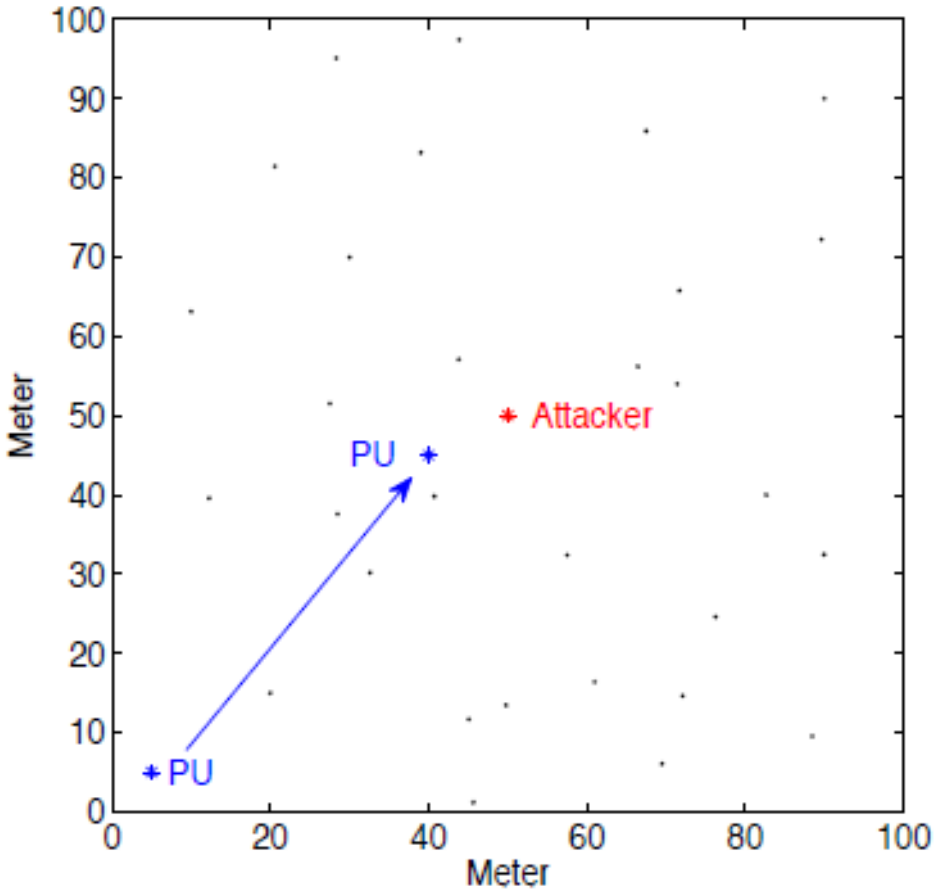

Figure 4.1: CR network model.

around the grid. They noted that as the distance between the primary user and malicious user increased the final belief decreases meaning that it is easy to distinguish between a primary user and a malicious user if they are far apart. However, as the distance between the primary user and the malicious user decreases, the final belief increases which means that it becomes more difficult to distinguish between a primary user and a malicious user. We demonstrate the effectiveness of the old algorithm in Fig. 4.2.

The results presented in [10] clearly show that as the malicious user moves closer to the primary user it becomes more and more difficult to distinguish between the two. We

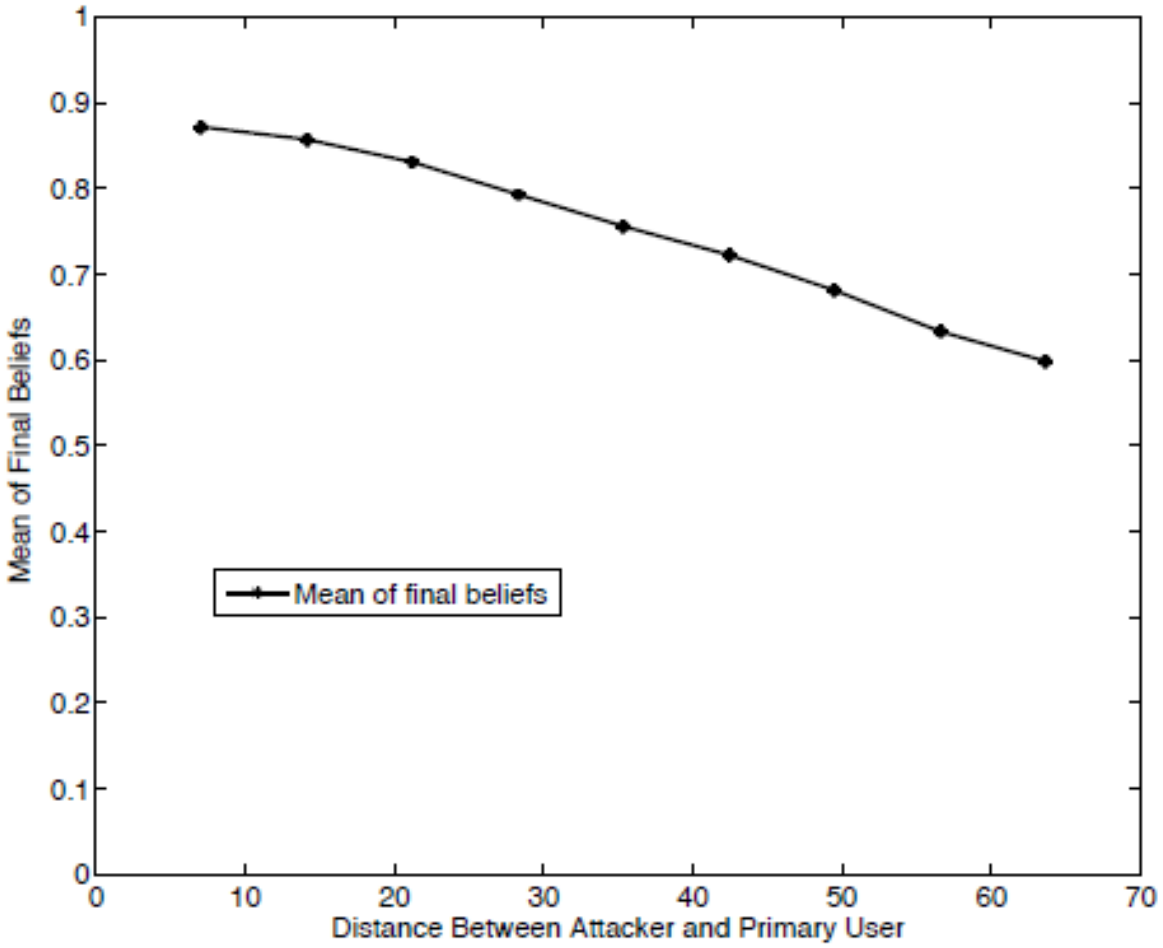

Figure 4.2: Final belief Vs Distance (original technique).

see from the results presented in [10] that the original algorithm [**?**] is able to distinguish between a legitimate primary user and a malicious user with fairly high accuracy. However the algorithm that is proposed in the original paper [**?**] has several deficiencies. The key among these is its high computational complexity. During our simulations we observed an exponential growth in the computational complexity as the number of secondary users in the network is increased. Fig. 4.3 shows the effects that increasing the number of secondary users has on the computational complexity of the algorithm.

From these results we concluded that although the original algorithm [**?**] is fairly effec-

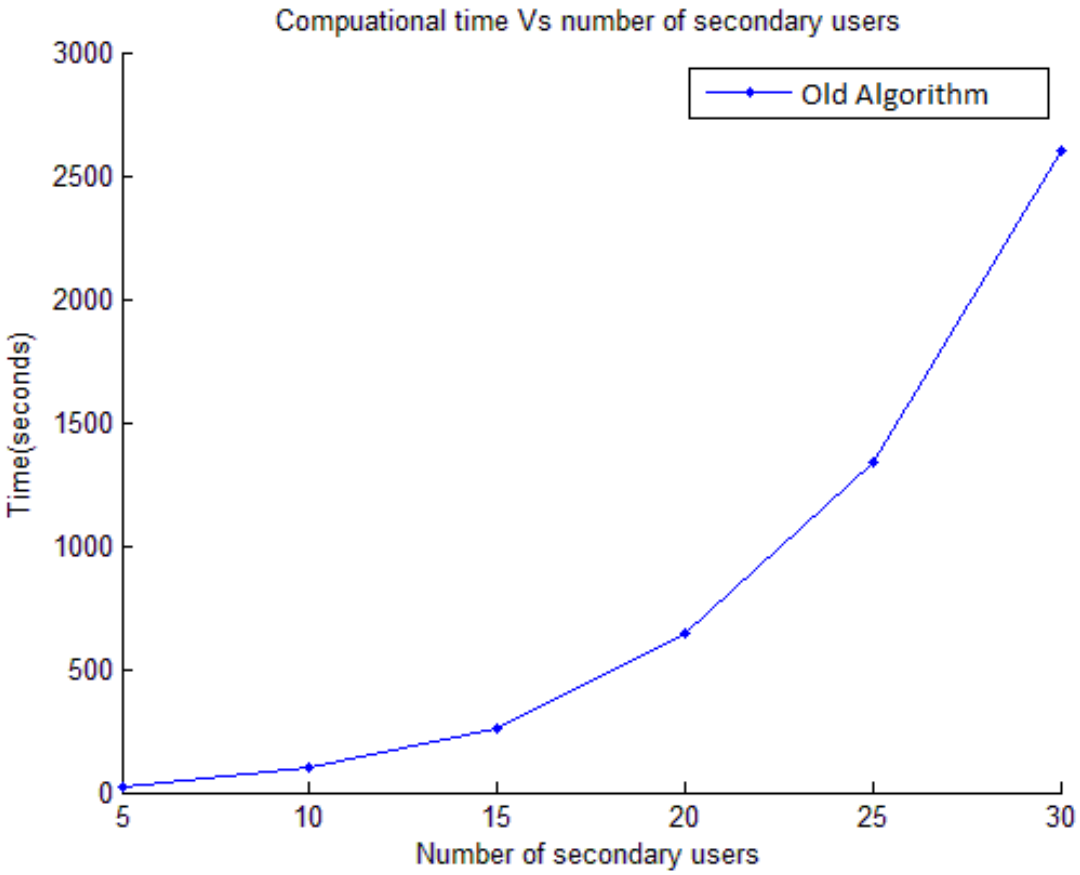

Figure 4.3: Computational time of the old technique.

tive in identifying a malicious user from a primary user, its high computational complexity means that it is not a feasible option for implementation using low power consumption cognitive radio terminal devices. We identified that the primary reason for the high computational complexity of the original BP algorithm is the local function. The Kullback Leibler distance that is used to evaluate the difference between the primary user probability density function and the attackers' probability density function was recognized as the main problem. The reason for this is that the KL function evaluates the dissimilarity between two function using an integral expression. If there are n secondary users in the network, the KL distance has to be evaluated once for each pair of secondary users, which means that it is calculated $n * (n - 1)$ times. This is a serious deficiency which makes this

algorithm computationally infeasible for practical networks where the number of users is large.

4.3.2 New BP Results and Analysis

To combat the deficiencies of the original algorithm [**?**] we present a new and improved algorithm that makes two important improvements that increase the accuracy and decease the computational complexity of the original algorithm [**?**]. To decrease the computational complexity of the original algorithm we propose a new simplified local function which provides the same level of accuracy with a reduced level of complexity. In addition, we modify the old compatibility function to help increase the level of cooperation between secondary users in the network.

Computational complexity / Run time

The most significant improvement obtained by the new technique is the reduced computational complexity and run time of the algorithm. The new algorithm is able to reduce the run time of the original algorithm [**?**] by a introducing a simplified local function. The new local function insures that the computational complexity grows linearly instead of exponentially, which insures that the algorithm is flexible, scalable and still just as effective. Table 1 shows a comparison between the run times of the old BP algorithm and the new BP algorithm. Table 1 presents results that were obtained using an Intel(R) Core(TM) i7-3930k CPU and all simulations were performed and timed using MATLAB.

Number of users	Comp time Old	Comp Time New
5	22 seconds	0.0491 seconds
10	101 seconds	0.0496 seconds
15	262 seconds	0.0564 seconds
20	648 seconds	0.0682 seconds
25	1337 seconds	0.071 seconds
30	2605 seconds	0.10 seconds

Table 1: Comparison of run times between the old and new algorithms.

From Table 1 it is clear that the new algorithm has much less computational complexity than the original algorithm [**?**] by a large factor. We note that the run times of the new algorithm increase only linearly as the number of secondary users in the network is increased. This presents a significant step forward for the algorithm and allows it to be used in large networks. Fig. 4.4 provides a visual comparison of the results that were presented in Table 1.

Additionally, we tested the computational complexity of the new algorithm when much larger numbers of secondary users are added to the network. The results of the simulations are presented in Table 2. Table 2 shows that the run time of the original technique [**?**] with 5 secondary users takes nearly as long as the run time of the new technique with 1000 secondary users. Table 2 presents results that were obtained using an Intel(R) Core(TM) i7-3930k CPU and all simulations were performed and timed using MATLAB.

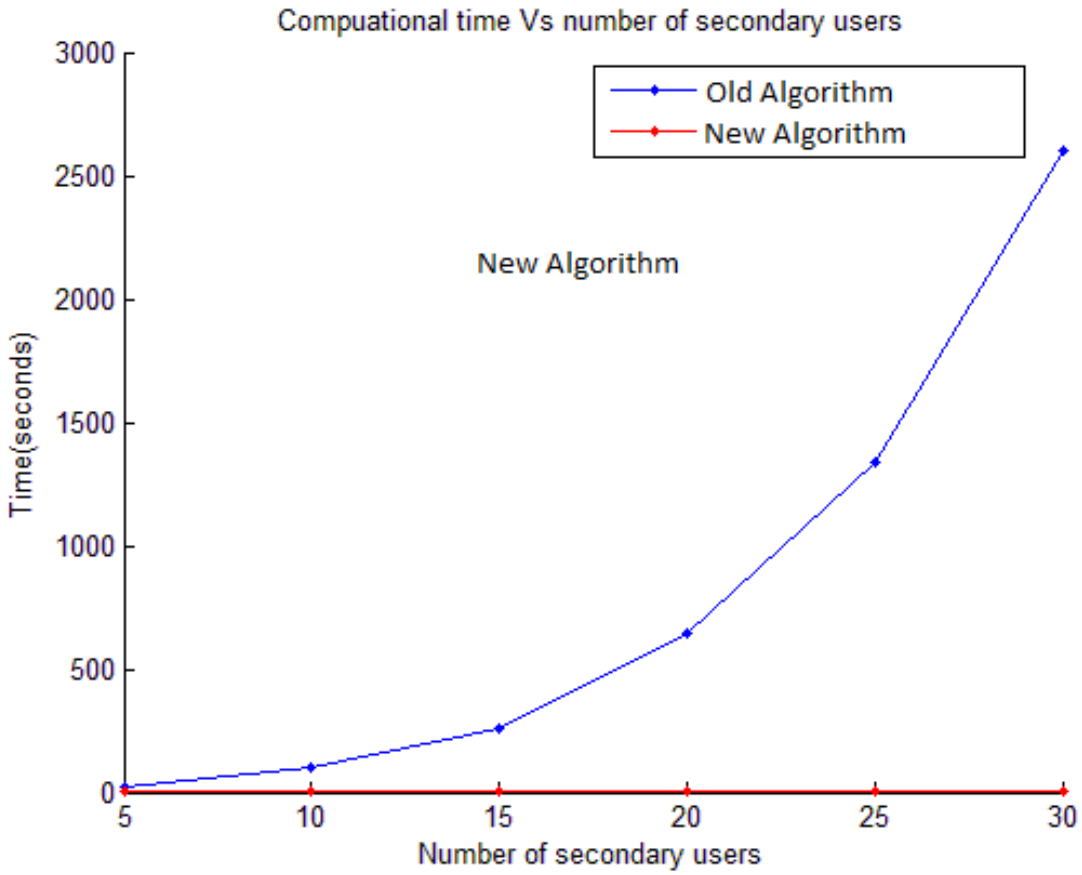

Figure 4.4: Computational time comparison between the old and the new techniques.

Number of users	Computation time
100	1.4 seconds
300	4.2 seconds
500	11 seconds
1000	30 seconds

Table 2: Run times of new algorithm with high number of SUs.

Performance and Accuracy

In addition to the reduced computational complexity of the new algorithm we show that it also exhibits superior performance to the algorithm presented in [10].. This is primary

due to the introduction of a modified compatibility function that allows for a larger degree of cooperation between secondary users. The greater the degree of cooperation between secondary users in the network the lower the chance of false or missed detection of a malicious user. Fig. 5 shows a comparison between the performance of the new algorithm and the performance of the original algorithm [?].

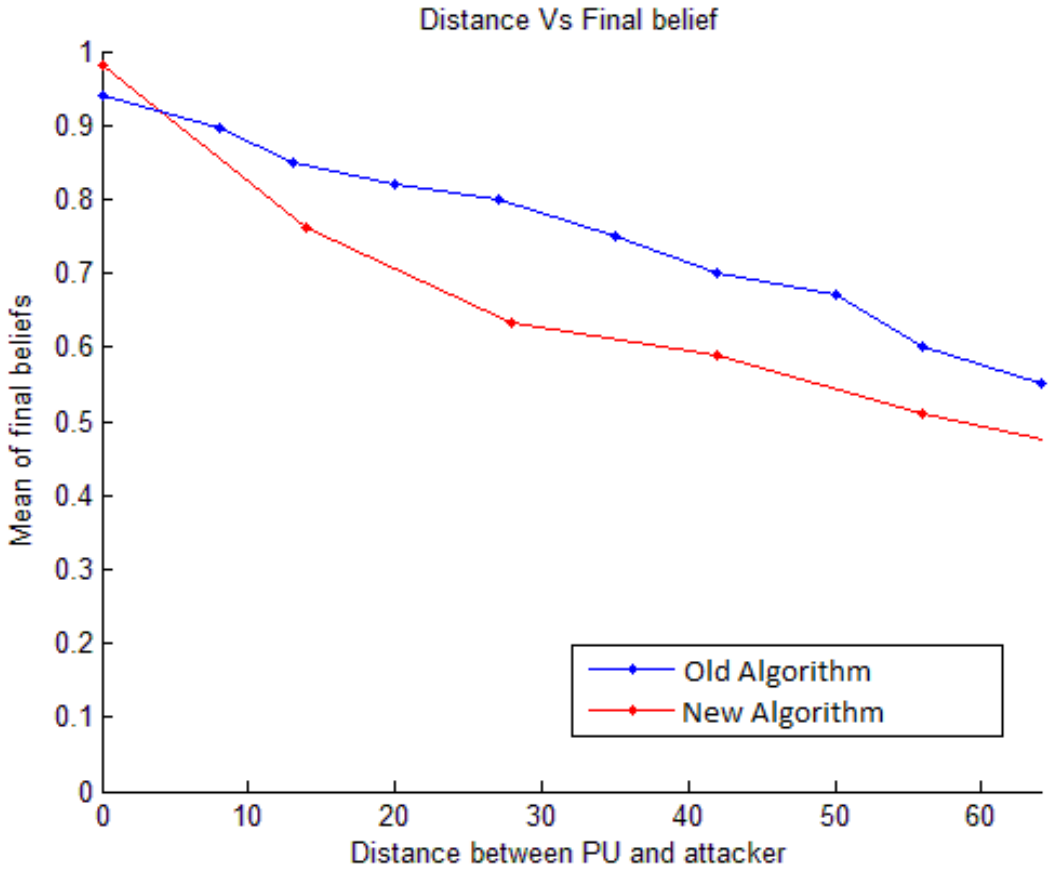

Figure 4.5: Comparison of performance between the old and the new techniques.

The perfect BP algorithm would result in a final belief value of 1 when the malicious user and the primary user are at the same location and would result in 0 in all other cases. The simplest way to evaluate how well an algorithm performs is to analyse the slope of its curve. The more negative a curve is the more effective the algorithm is (visually the steeper the curve is the better the algorithm). Since, in the perfect case the slope of

the curve would be infinitely negative. Simple comparisons between the two algorithms shows that the slope of the new algorithm is more negative than the slope of the original algorithm [**?**](new algorithm has a steeper slope). This simple and effective comparison shows that the new algorithm is not just less complicated but also detects PUEA with a higher degree of accuracy. We used a Gaussian distribution for h_2 and h_1 to attain the results presented in Fig. 4.5.

ROC curves

The received operating characteristics (ROC) curve is used for diagnostic test evaluation. It plots the probability of detection conditioned upon a primary user being on the channel (sensitivity) as a function of detecting a primary user conditioned upon an emulator being on the channel (specificity) [56][57]. We use the ROC curve to evaluate the performance of the new algorithm under varied conditions. Fig. 4.6 compares the performance of the new technique with different numbers of secondary users on the network. The larger the area under the curve the better the technique is performing. We see that as we add more secondary users on the network we improve the performance of the algorithm. The improvement in performance comes from greater degree of accuracy due to the increased number of secondary users cooperating with each other. The more secondary users on the network the less likely the chance false detection. We note that we acquire good results even when there are a low number of secondary users present on the network.

Fig. 4.7 compares the performance of the algorithm when the distance between the primary user and the malicious user is increased. We expect that as the malicious user moves closer to the primary user we would see a decrease in performance because secondary users will have a greater degree of trouble distinguishing between the PU and the malicious user. As the distance between the two increases secondary users are able to distinguish between them which results in an increase in accuracy of the algorithm. We

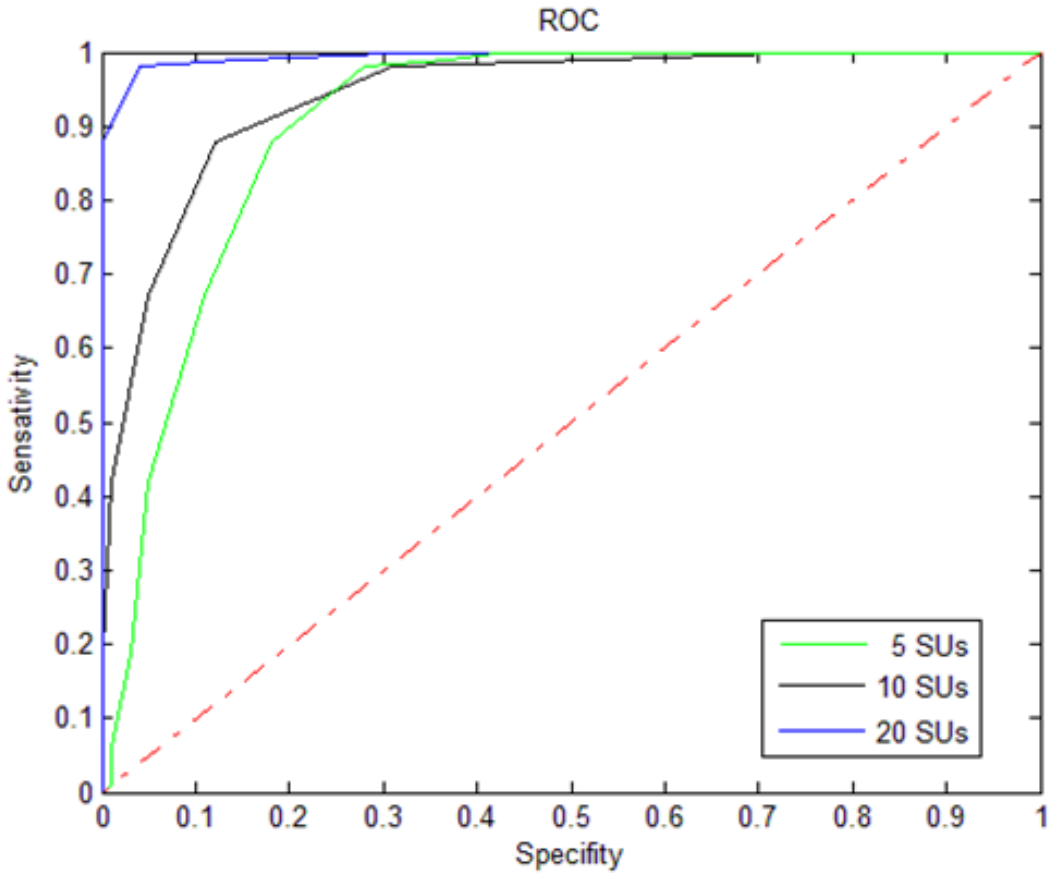

Figure 4.6: ROC curve showing what happens when the number of secondary users in increased.

demonstrate this in Fig. 4.7 where we see that as the distance increases the performance increases. From Fig. 4.7 we see that we are able to get very high accuracy results even when the distance between the malicious user and the PU is very low. For instance we are able to achieve good results even when the distance is as small as 2 meters.

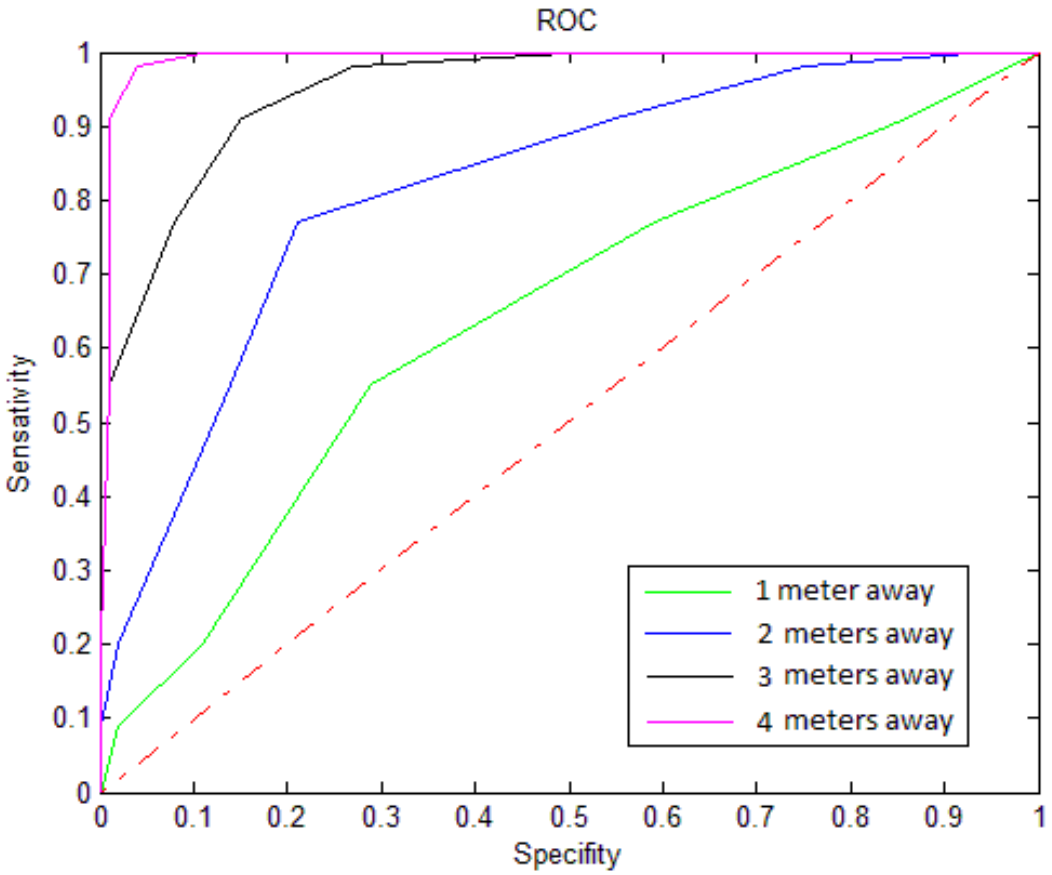

Figure 4.7: ROC curve showing the effects of altering the distance between the PU and the attacker.

A key consideration of an algorithm is its performance when subjected to different levels of noise. In Fig. 4.8 we demonstrate the effects that different variance levels of shadowing have on the performance of the algorithm. We see that as we increase shadowing variance we decrease the performance of the algorithm. We assume that shadowing get worse as the distance between secondary users increases. In other words, we assume that shadowing is a function of distance. When we have no shadowing in the algorithm we see that the algorithm performs perfectly (red line), the more shadowing is introduced, the worse the algorithm performs. With increased $\sigma = 5$, the performance decreases significantly.

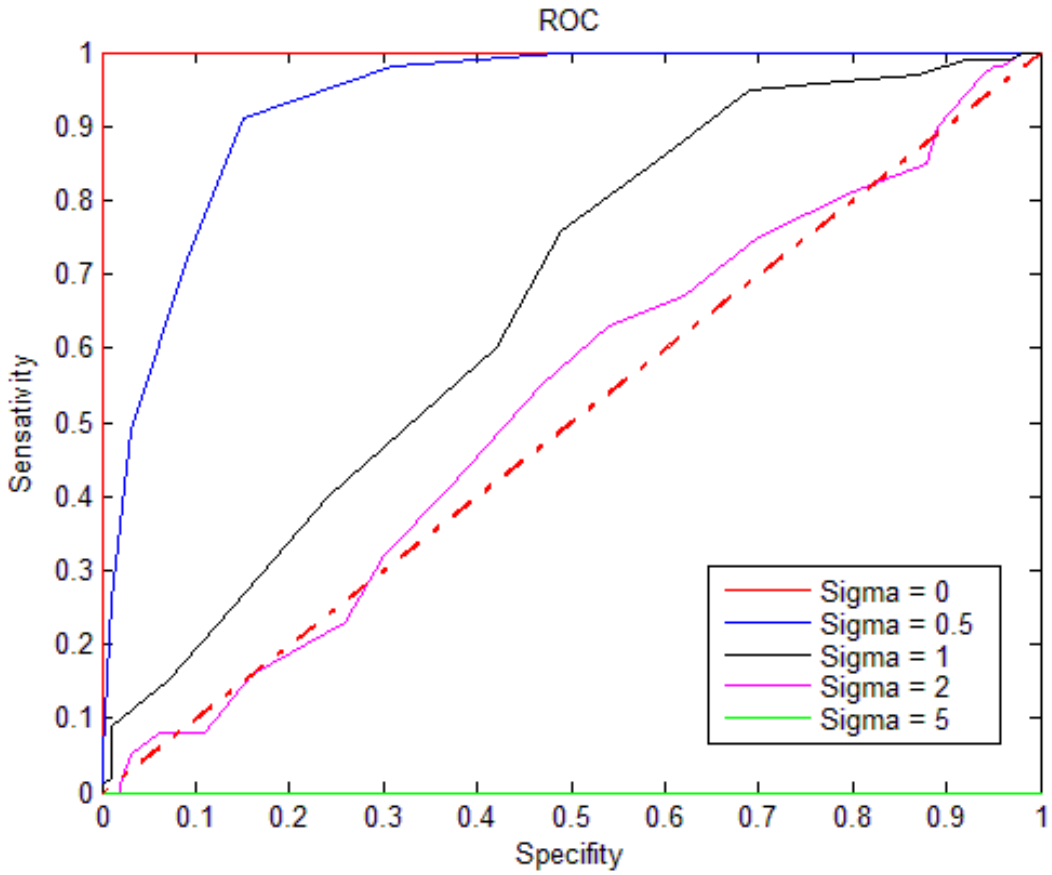

Figure 4.8: ROC curve showing the effects of shadowing on the performance of the new technique.

Using ROC curves we show that our algorithm is effective in a number of different scenarios. This provides evidence of the flexibility and effectiveness of the algorithm. It shows that the new algorithm is able to handle non-ideal and unpredictable situations with a high degree of accuracy. These results provide proof that this algorithm would be well suited for practical implementation.

Chapter 5

Single Iteration Belief Propagation

This section presents an improved belief propagation based algorithm. Previous work with belief propagation has resulted in algorithms that take a number of iterations of message processing to converge to a final consensus. Within this chapter we present a single iteration belief propagation algorithm that reduces the computational complexity by converging to a final belief within a single iteration. The main contributions in this chapter can be summarised as follows:

- A significant reduction in the computational complexity and run time of the algorithm. Achieved through the reduction in the number of iterations that the algorithm needs to converge. In previous work we needed 4-7 iterations to converge to a final belief. In our new algorithm that is decreased to a single iteration.

- Improvements in the way messages are treated at secondary users allows for more consistent and accurate results. Messages are aggregated as averages which leads to a better representation of the belief of neighboring secondary users.

- Significant improvements in accuracy through the introduction of a shadowing correlation function for secondary users who are in close proximity to each other. In-

stead of assuming that shadowing is random for each secondary user, it is correlated with respect to distance. As a result, beliefs become less erratic and independent of random variables. Which means, that final belief is determined with a higher reliability.

- Its decrease in computational complexity mean that it is perfectly suited for users that are limited in power and computational complexity.

Belief propagation is a powerful algorithm that we use to compare the location of an unknown transmitter to the location of a known primary user. This can be achieved by only considering the local observations at a secondary user. However, to accomplish a higher level of accuracy and reliability we use a belief propagation framework that is based on pairwise Markov Random Fields (MRF) [69]. This means that we consider pairs of secondary users. The main contribution of this chapter is a redefined messaging protocol and a new method for computing the belief at each secondary user. With the above modifications, we are able to use a single iteration and achieve results which are just as accurate as the previous method that used 7 iterations. We achieve this with a significantly lower computational complexity and a great reduction in control channel data transmission requirements.

Relative power observations at secondary users are used to determine the location of a transmitter. Due to the use of the ratio of received powers at two secondary users, belief propagation works independently of transit power observations, as long as the power is high enough relative to in band noise [68]. In Markov Random Fields, we define Y_i as the local observations at secondary user i and X_i as the state of the transmitter at secondary user i. Much like in the previous section, when $X_i = 0$ the transmitter is deemed a malicious user and when $X_i = 1$ the transmitter is deemed a primary user. A local function at secondary user i is expressed as $\phi_i(X_i, Y_i)$, it denotes independent local

observations at a SU. To represent the correlation of results between two secondary user we use a compatibility function, denoted by $\psi_{ij}(X_i, Y_j)$. From [39] the joint probability distribution of an unknown variable X_i is defined previously in Eq. (5.1). From the joint probability equation, we can compute the marginal probability at a secondary user i, which we denote as a belief. The belief is the product of secondary user i's local observations in the form of a local function, and all received messages and was defined previously in Eq. (5.2). We believe that converging to a final belief using Eq. (5.2) was an ineffective method to calculate the overall belief. Therefore, we derived a new belief equation which is presented in Eq. (5). In the previous algorithm, the product of all messages was initially computed. This led to the derivation of a normalisation constant and was an ineffective way to represent the significance of the incoming messages. We derive the final belief using the local function and all incoming messages at each secondary user. The previous function did not allow for appropriate weighting of the received messages. The proposed belief equation is as follows:

$$b_i(X_i) = \frac{1}{2}\phi_i(X_i, Y_i) + \frac{1}{M-1}\sum_{\substack{j=1 \\ j\neq i}}^{M} m_{i,j}(X_i) \tag{5.1}$$

where $m_{i,j}$ represents all the messages that have been sent to secondary user i from secondary user j, M is the number of neighboring secondary users. The new belief equation does not use a normalisation constant. Instead of using the product of all incoming messages into secondary user i, we calculate the mean of all incoming messages. Using the mean instead of the product makes the algorithm more robust when there are secondary users that are relaying false or inaccurate information. The reason is that with the mean of all messages, a single outlier is going to have a smaller effect on the belief, especially when there is a large number of secondary users exchanging information. Therefore, the new belief equation is more reliable, robust and accurate than the previous one. The exchange

of messages between secondary users is a critical part of the belief propagation algorithm. In the algorithm presented in [68], we used an iterative approach. In our approach we needed between 3 and 7 iterations for convergence. The message exchange equation is presented in the previous section in Eq. (5.4). A message denoted as $m_{ij}^{l}(X_i)$ can be understood to be a message from secondary user j to secondary user i, in the l_{th} iteration. The messaging protocol proposed in Eq. (5.4) was dependent on a number of iterations to achieve an accurate result: at each iteration the local and compatibility functions had to be recalculated. This added an unnecessary level of complexity to the system. Through the introduction of the new messaging protocol we were able to significantly reduce the computational complexity of the algorithm. We base the new messaging equation on a similar principle to the belief function. We use the mean of the compatibility function and the local function. Through the introduction of the new messaging equation we are better able to represent the local observations at each secondary user, as well as highlight the compatibility between secondary users. This is due to the compatibility function having the same weighting as the local function. The new equation is as follows:

$$m_{ij}(X_i) = \frac{1}{2}\psi_{ij}(X_i, Y_j) + \phi_i(X_i, Y_i) \tag{5.2}$$

A major deficiency of the algorithms presented in [10] and [68] is scalability. These algorithms work well in small networks. However, as the number of secondary users increases, the accuracy of the results begins to degrade, in some cases when there is a large number of secondary users the results become unpredictable. The scalability of these algorithms makes them impractical. The new messaging protocol is simpler and allows the algorithm to converge in a single iteration. The new messaging equation ensures that the results of our method are consistent and accurate, even when the number of secondary users is large. This is illustrated further in the simulation and results section.

After each secondary user has exchanged messages with all its neighbors, they must

then compute a belief about whether or not the transmitter is a primary user or a malicious user. Each user computes their own belief. Subsequently, a final belief is determined as the average of all the beliefs of each secondary user. The final belief is compared to a pre-set threshold. H_0 represents the hypothesis that the transmitter is a primary user. H_1 represents the hypothesis that the transmitter is a malicious user.

To effectively combat primary user emulation attacks we utilize an RSS based localization method. To compare the incoming measured RSS of a transmitter and the theoretical RSS measurements corresponding to a primary user, we employ a belief propagation algorithm. The culmination of local measurements at a SU is represented as a local function. In order to increase the detection accuracy, each secondary user exchanges messages with its neighbors. Each neighbor in range of a reference node is assigned a scalar value, which indicates how relevant that neighbors local observations are to the reference node. We denote this scalar value as the compatibility function. The compatibility function is a measure of how relevant two secondary user observation are to each other. This primary correlation factor for high compatibility is distance . The closer two secondary users are to each other, the more relevant they will become to each other's final belief. This is because two secondary users located in close proximity have similar channel fading.

Local Function

The local function corresponds to the probability of a transmitter being a primary user. Each secondary user calculates the local function through comparison of the RSS from a transmitter with the theoretical measurements corresponding to the fixed location of a primary user. The closer to the similarity is between the two measurements, the closer the local function is to 1. The closer the local function is to 1, the more likely that the transmitter is a primary user. The power measurements corresponding to the primary user form a basis for the comparison. The ratio of signal strength measurements from a

primary user can be defined as follows. Much like in the previous algorithm we use the incoming RSS measurements to localise a transmitter and using that information we are able to classify the transmitter as a primary user or an emulator. The first step in this process is to define a baseline value which can be used a comparison. We define $B_{i,j}$ to corresponds to theoretical ratio in RSS from a primary user at SU_i and SU_j, and define it in a similar fashion to Eq. (4.2) for the kth primary user:

$$B_{i,j} = \left(\frac{d_{i(PU_k)}}{d_{j(PU_k)}}\right)^{-\alpha} \tag{5.3}$$

We assume that each secondary users knows the location of all neighboring secondary users. Therefore, the values of $d_{i(PU_k)}$ and $d_{j(PU_k)}$ are known to all secondary users on the network. With this information each secondary user is able to calculate the value of $B_{i,j}$, which we can think of as a theoretical value corresponding to where the transmitter should be (primary user location). To identify a transmitter each secondary user samples the RSS values of the incoming signal. If we define $P_{r1(attacker)}$ and $P_{r2(attacker)}$ as the received signal strengths from the attacker to SU_1 and SU_2 respectively, and the distances between SU_1 an SU_2 and the attacker as $d_{1(attacker)}$) and $d_{2(attacker)}$) respectively. $A_{i,j}$ corresponds to difference in RSS measurements from a suspect at SU_i and SU_j, it is defined as follows for the kth primary user:

$$A_{i,j} = \left(\frac{d_{j(attacker)}}{d_{i(attacker)}}\right)^{-\alpha} \left(\frac{h_{i(PU_k)}}{h_{j(PU_k)}}\right) \tag{5.4}$$

Where $h_{i(PU_k)}$ and $h_{j(PU_k)}$ represent two log-normal, random shadow variables. $h_{i(PU_k)}$ and $h_{j(PU_k)}$ are correlated with respect to the distance between secondary users. The closer a pair of secondary users is to each other the better the correlation between their shadowing variables. If two secondary users are at the same location they would have the same shadow fading. We use the Gudmundson model [70] to describe the correlation between shadowing constants from a transmitter to two secondary user locations [71].The Gudmudson model is as follows:

$$R_{i,j} = \exp\left(\frac{-d_{SU_i,SU_j}}{D}\right) \tag{5.5}$$

where, $R_{i,j}$ is the correlation function between two secondary users from a transmitter, d_{X_i,X_j} is the distance between secondary user i and secondary user j in meters, D is the decorrelation distance which is empirically determined as 8.3058 meters in [71]. $B_{i,j}$ is acquired using the theoretical RSS from a known primary user location and $A_{i,j}$ is acquired from the RSS measurements of an unknown transmitter. In order to compare the two values this thesis introduces a local function. The local function derived in [68] is as follows:

$$\phi_{i,j} = exp\left[-\left(\frac{\mid A_{i,j} - B_{i,j} \mid}{A_{i,j} + B_{i,j}}\right)\right] \tag{5.6}$$

The local function derived in [68] provides us with a simple and effective way to compare the incoming RSS measurements with the fixed primary user location. The closer the correlation between the two measurements, the more likely that the transmitter is a primary user. This local function provides a much better comparison than the one presented in [10]. It proves a more accurate and less computationally complex solution.

5.1 Results and Analysis

This section is focused on the simulation and analysis of the new BP algorithm. This section is broken up in two sub-sections. The first presents the computational complexity analysis. In the first sub-section we show that, in comparison to the algorithm presented in [10], the new BP algorithm is able to operate with a much lower complexity while also performing at high accuracy. The second sub-section compares the accuracy of the new BP algorithm with the accuracy of the algorithm presented in [10]. It is important to ensure that we are able to keep a high detection accuracy from our method even as we decrease the computational complexity of the underlying BP algorithm. The improvements presented

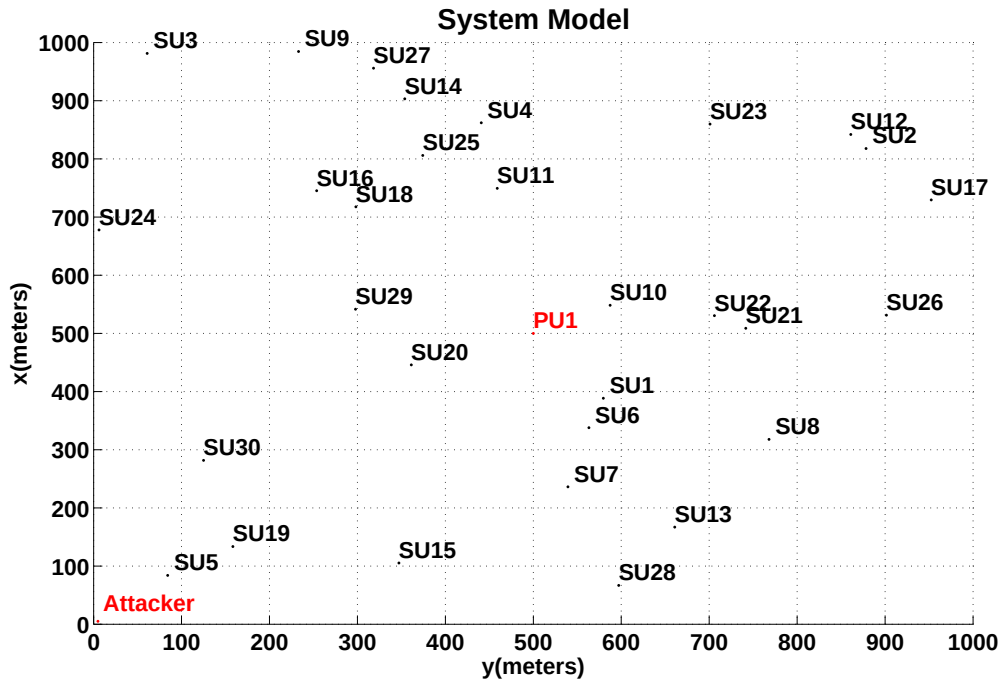

Figure 5.1: A typical secondary user network

throughout this thesis are a result of a newly developed message exchange protocol and a new belief function. Together, they allow the new algorithm to operate with a single iteration. This ensures that the convergence time of the new algorithm is far below that of the algorithm presented in [10], which increases the scalability of the algorithm. These improvements contribute to ensuring that our method is more suited for practical implementation. The results presented here were obtained using 30 randomly generated, uniformly distributed secondary users scattered around a network with an area of 100 m x 100 m. The distance between the primary user and the attacker were modified from 0 to 40 m. A typical network configuration can be seen in Fig. 5.1.

5.1.1 Computational Complexity

The reduction of the number of iterations is the primary contributing factor in the dramatic decrease in the computational complexity of the entire method. The algorithm presented in [68] and [10] relies on an iterative approach. The BP algorithms need between 3 and 7 iterations to converge to a final value. When the number of secondary users in the network is small the computational time of these methods is fairly small. However, as the number of secondary users grows, the methods presented in [10] and [68] become impractical. In [10], the BP algorithm is extremely slow and takes up to an hour to converge even when there are only a few dozen secondary users. This was partially solved in [68] with the introduction of a new local function. However, in this thesis we provide an even better solution that significantly minimises the computational complexity of the previous method.

In Fig. 5.2, we demonstrate the results that were obtained through simulations. Fig. 5.2 demonstrates the difference in the computational time between the new algorithm and the one presented in [10]. The results demonstrated were obtained by simulating 100 random secondary user configurations. From the diagram, it is evident that for a smaller amount of secondary users on the network the algorithms have a similar run time. However, as we increase the number of secondary users, the complexity of having multiple iterations increases the computational time of the algorithm presented in [10]. At approximately 300 secondary users, the old algorithm begins take noticeably longer than the new algorithm. The computational complexity and run time of the algorithm are two very important factors in determining its efficiency and effectiveness. In order to mitigate primary user emulation attacks, the method used must be responsive and accurate. It must be accurate enough to identify whether a transmitter is a primary user or an attacker and must be able to do this as efficiently as possible. For an algorithm to be applicable, it must have the right balance between accuracy and speed. The method

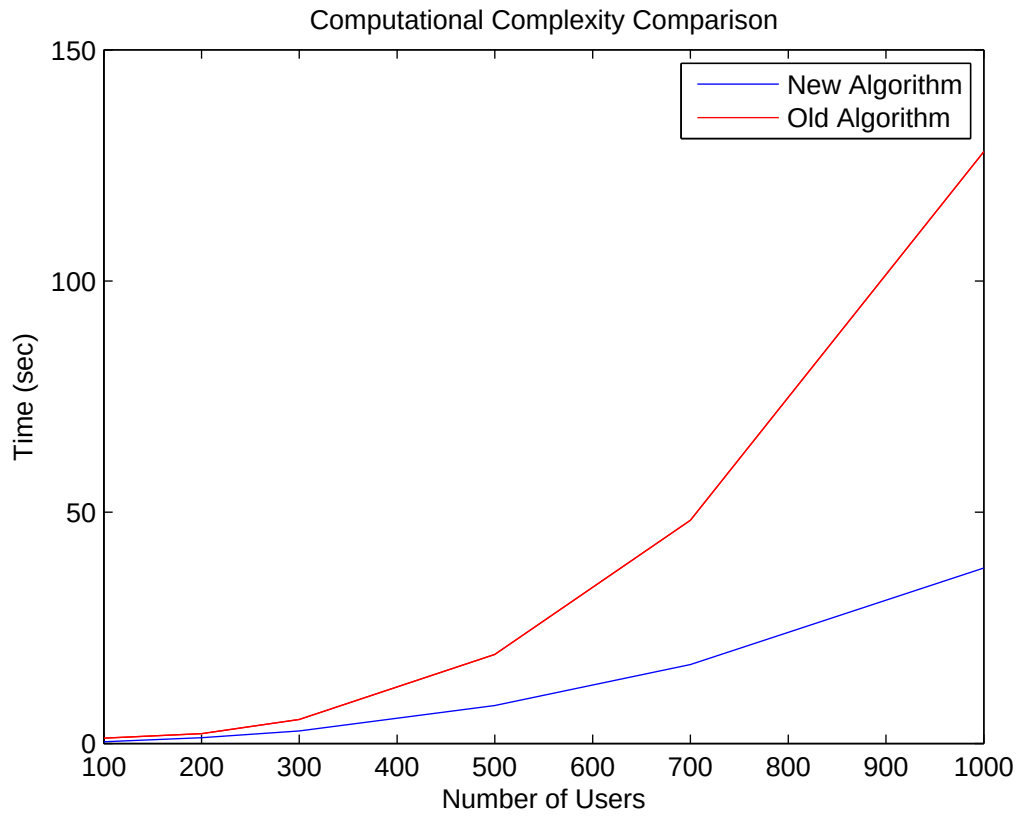

Figure 5.2: Shows the difference in computational time between the two methods.

presented in this thesis operates with a good balance between the two.

5.1.2 Performance and Accuracy

The algorithm proposed in this thesis has been shown to be more efficient than the algorithms presented in [68] and [10]. However, to mitigate against a primary user emulations attack it must be able to distinguish between primary users and attacks with a high accuracy.

Fig. 5.3 presents a comparison of the accuracy between our algorithm and the one presented in [10]. We used a log normal distribution to model the shadow fading on the channel. The results demonstrated were obtained by simulating 100 random secondary

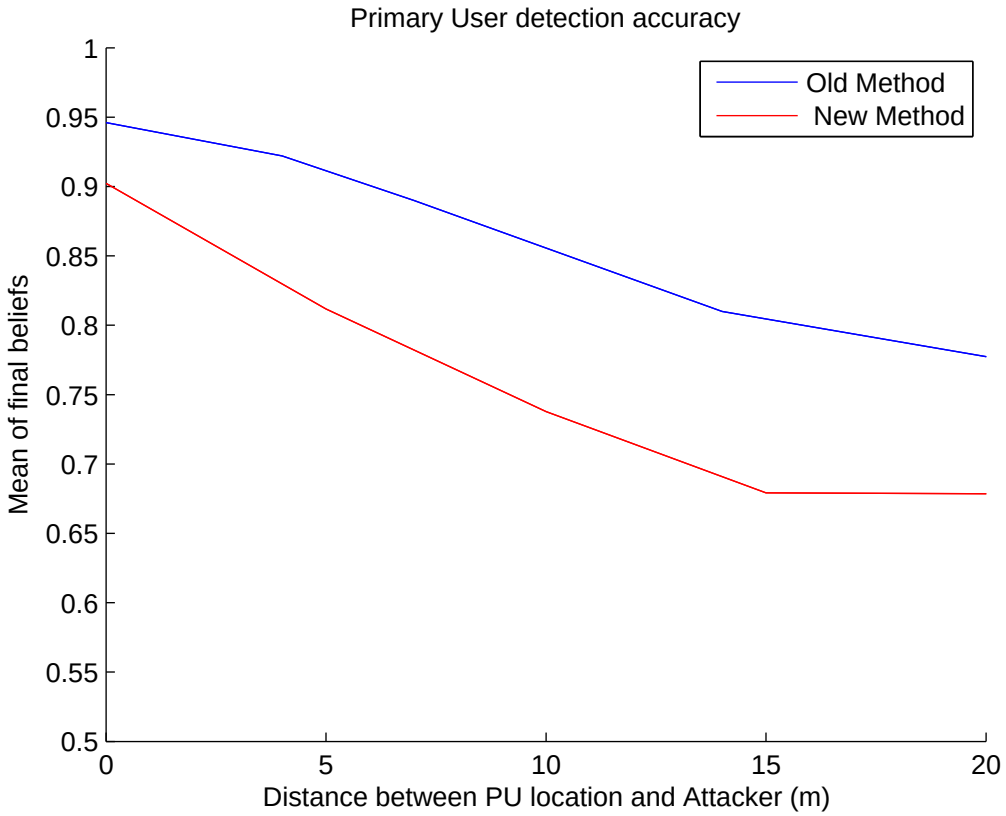

Figure 5.3: Shows difference in performance accuracy between the two methods

user configurations. The pass loss constant (α) is set to 2.5. If we were to plot the perfect algorithm, it would have a value of 1 for the final belief when the transmitter is a primary user and a value of 0 in all other cases. A simple way to evaluate the performance of the algorithms is to examine the slope of each curve. The more negative the curve is, the more effective the algorithm is (visually the steeper the curve the better the algorithm). Since, in the perfect case the slope would be negative infinity. From visual inspection we see that there is very little difference between the accuracy of the two algorithms in terms of performance. However, the new algorithm performs better in terms of accuracy. We assume that the attack is able to perform any of the functions that secondary users are able to perform and that it is stationary. From the simulation results we see that the new

algorithm is clearly superior to the one proposed in [10]. It is more accurate, with a much lower computational complexity.

Chapter 6

Compressive Sensing Belief Propagation Hybrid

In our previous work, we assumed that the location of the primary user is known for all secondary users. This is true in some networks, while in others the primary user might be mobile and consistently changing location. Since our previous methods rely on the primary user being stationary, a hybrid method is introduced to allow us to gather a more accurate location for the primary user. To do this, we used belief propagation in conjunction with Compressive Sensing. The main contributions of this work are as follows:

- An increase in the reliability and accuracy of results using compressive sensing. Compressive Sensing allow us to continuously monitor the location of the primary user. If they move we are able to adjust accordingly.
- The ability to track primary user movement, increasing the effectiveness of the algorithm. In practical situations, we must assume that primary users might be mobile. In addition, there might be more than one primary user that is utilising the frequency band. It is therefore key that secondary users have an accurate

representation of all primary users and where they are located at all times. Previous literature is static and ignores primary user movement.

- Compressive sensing allows secondary users to obtain a more accurate local observation. Since precise localisation of the primary user is now known, secondary users have a well defined baseline RSS which enables them to rely less on the observations of its neighbours.

- Hybrid algorithm that is well suited for both distributed and centralised schemes. Belief propagation is lightweight and can be used by secondary users with limited resources.

Compressive sensing is used to localise the primary user. Using compressive sensing we are able to periodically calculate the location of the primary user. Within our framework this would correspond to the theoretical value defined previously in Eq. (6.3). However, due to the high computational complexity of Compressive Sensing, we propose a hybrid centralised/distributed architecture for this algorithm.

We propose to use compressive sensing periodically at the fusion center to confirm the theoretical results are correct. This would allow us to establish an accurate baseline for the primary user location. If the location of the primary user has changed since the previous period, the fusion center would send out a broadcast message to all secondary users within range to inform them that the location of the primary user has changed. Performing compressive sensing at the fusion center takes the burden off secondary users who we assume have limited power and computational complexity. It allows secondary users to use the belief propagation algorithm with the highest possible accuracy.

Due to the constantly changing radio environment, influenced by multi-path, interference and shadowing, a finger-printing based approach to localise a PU has been adopted. The grid layout has been constructed using N unique grid points, with grid resolution w in

both x-axis and y-axis. The N grid points are located at $\{V_n, 1 \leq n \leq N\}$, where V_n is a two dimensional position vector. The M SUs are positioned at $\{U_m, 1 \leq m \leq M\}$, where U_m is also a two dimensional position vector. Earlier in Section II, we mentioned that a PU is randomly placed among one of the N possible grid points. The model assumes that the FC has prior knowledge of the two dimensional location information V_n and U_m. The Euclidean distance between the N grid points M SUs are fed into the pathloss model described in (1) to populate a radio environment database matrix. In matrix form the database can be expressed as:

$$\Psi = \begin{pmatrix} \psi_{1,1} & \psi_{1,2} & \cdots & \psi_{1,N} \\ \psi_{2,1} & \psi_{2,2} & \cdots & \psi_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ \psi_{M,1} & \psi_{M,2} & \cdots & \psi_{M,N} \end{pmatrix} \tag{6.1}$$

where,

$$\psi_{mn} = 10^{-Pathloss_{dB}(d_{mn})/10}, \tag{6.2}$$

and,

$$d_{mn} = \parallel U_m - V_n \parallel_2 . \tag{6.3}$$

d_{mn} is the Euclidean distance between the m^{th} SU and the n^{th} grid point, and Ψ_{mn} is the pathloss power ratio between m^{th} SU and n^{th} grid point. The raw observations from M SUs are stored in a column matrix Y, where y_m is the raw power received at the m^{th} SU. Equation (2) and column vector Y can be combined to formulate a problem of an under-determined set of equations:

$$Y = \Psi X + \eta. \tag{6.4}$$

where, $X_{N\times 1}$ is an $N \times 1$ column vector, that represents the N possible grid points on which the PU can be positioned. In a realistic scenario, the raw power measurements are

corrupted with a noise power vector $\eta_{M\times 1}$ where the m^{th} entry is a statistically independent variable with variance σ_n^2, and is chi-square distributed with 1 degree of freedom. In some cases, due to small distance between the grid points, the database matrix Ψ may suffer from having a high coherence among columns, which degrades the uniqueness of each column and restricts Ψ from efficiently utilizing the vector spaces. A data-processing technique based on matrix transformation has been adopted from [72] to increase the incoherence between the columns of Ψ. Let T be a processing operator,

$$T = S\Psi^{+} \tag{6.5}$$

where, $S = \text{orth}(\Psi^T)^T$ which corresponds to the orthonormal basis of $(\Psi^T)^T$. The built in function of MATLAB, orth(Ψ), returns an orthonormal basis of the range of Ψ, and Ψ^Treturns the transpose. $\Psi^+$is the Moore-Penrose pseudoinverse [73] of Ψ. Applying the operator T on both sides of (6) yields,

$$S\Psi^{+}(Y) = S\Psi^{+}\Psi X + S\Psi^{+}\eta$$

$$\hat{\mathbf{Y}} = \mathbf{AX}+\mathbf{W}. \tag{6.6}$$

The processed measurement matrix, $\hat{\mathbf{Y}} = S\Psi^{+}(Y)$, the processed measurement matrix is $\mathbf{A} = S\Psi^{+}\Psi$ and the processed measurement noise, $\mathbf{W} = S\Psi^{+}\eta$. The problem formulated in (7) can be considered as a second order cone program and can be solved using several Compressive Sensing (CS) algorithms to retrieve the solution vector X [72]. To obtain an optimum solution vector, CS algorithms require the solution vector to be sparse. Sparsity in general terms indicates the number of non-zero elements in a vector. Since the model assumes having just 1 PU among N possible grid points, it can be claimed that the requirement for obtaining an accurate solution using CS has been satisfied. From the solution vector X, the non-zero amplitude will represent the power measurement of the PU, while the index indicates the grid point on which a transmitting PU is located.

Hence using the grid based technique, the power and location information can be jointly estimated.

6.1 Simulation Results

In this section, we present the simulation results of the proposed method. We test a number of scenarios to validate the accuracy and scalability of our method. In order to diagnose and combat a malicious node, we must ensure that we are able to accurately identify a primary user. As discussed in the previous section, our method relies on a hybrid compressive sensing, belief propagation algorithm. Belief propagation works by analysing the incoming RSS values and coming up with a belief about whether a transmitter is a primary user or not. In a perfect scenario belief propagation would decide H_0 if the transmitter is a primary user and H_1 in all other cases. However, in practice this is never the case; a transmitting node will have a belief of higher than zero and as a transmitter gets closer to the primary user the belief will increase. The key to a highly accurate method is to maximise the probability that the belief is smaller than the pre-set threshold for all cases other than when a legitimate primary user is transmitting.

Fig. 6.1 details the effectiveness of the CS based localisation method to accurately locate the PU in the network. A 13×13 grid was selected with a grid spacing of 80 m. A PU is randomly (normal distribution) positioned among the 169 unique grid points, whereas 25 SUs are deployed randomly. A total of 1000 Monte Carlo simulation runs are carried out and the average of the results are depicted in Fig. 6.1. Details of the CS based localization algorithm is available in [72]. The plot in Fig. 6.1 reflects that a higher SNR enhances the average detection (number of times the SUs detect a primary user from a set of observations) of the PU in the network while significantly reducing the mean square error (MSE) in power estimation (which measures the average of the mean square errors).

In Fig. 6.2, we demonstrate the effect that increasing the distance between a transmitter and primary user has on the overall belief of a network. We note that our algorithm is able to mitigate multiple attacks with multiple primary users. Each secondary user performed local observations and distributed their beliefs around the network. Fig. 6.2 shows the mean of all beliefs of all secondary users. We see that when the transmitter is located at the same location as the primary user (i.e. the transmitter is a primary user) we get a belief that is very close to 1. As the transmitter is moved away from the primary user location the belief begins to decline. The simplest way to analyse the performance of our method is to observe the slope of the curve: the steeper the slope the better the method. Fig. 6.2 shows the effects of varying the SNR. We note that even at low dB we have good results.

The received operating characteristic (ROC) curve is used for diagnostic test evaluation [74]. It plots the true positive rate (Sensitivity) against the false positive detection rate for different threshold values [75]. We define the sensitivity and specificity as:

$$Sensitivity = P_r\{H_1 \mid H_1\} = P_r\{detection \mid H_1\} \tag{6.7}$$

$$Specificity = P_r\{H_1 \mid H_0\} = P_r\{false\ alarm \mid H_0\} \tag{6.8}$$

The sensitivity (true positive rate) and specificity (the false positive) are used to develop a ROC curve which is a tool for test evaluation at different threshold values. We use the ROC curve to evaluate the performance of the new algorithm under a number of conditions. The simplest way to evaluate the performance of the algorithm using the ROC curve is to observe the area under the curve. The larger the area under the curve the more

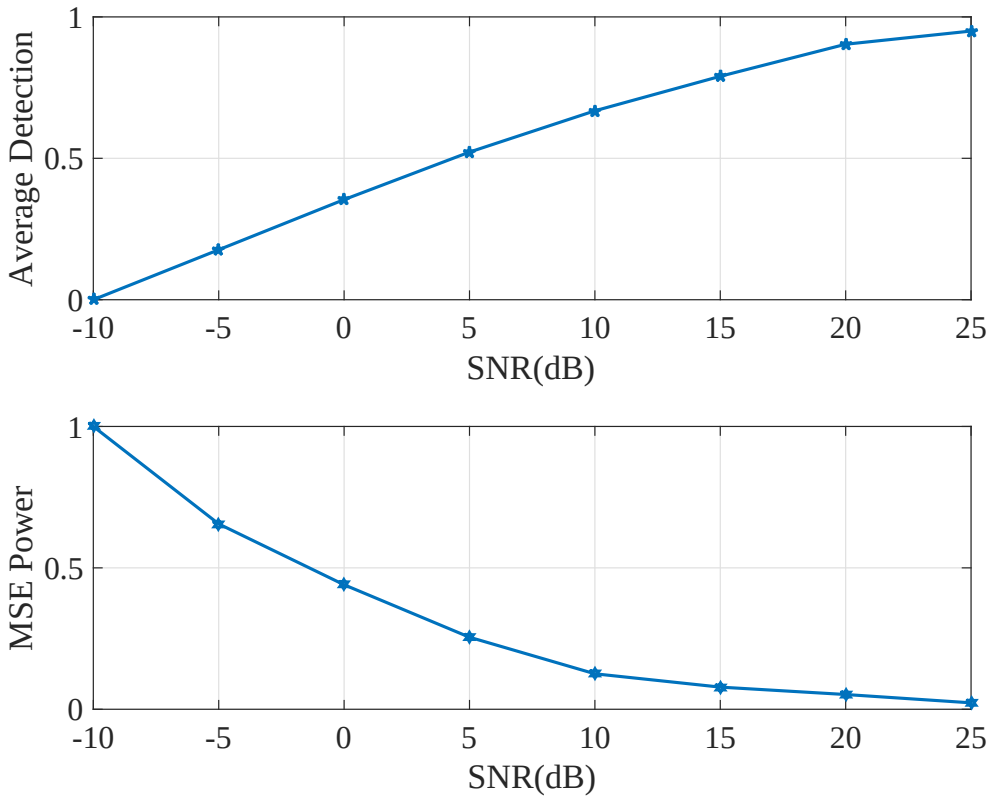

Figure 6.1: Performance analysis of the CS based localization algorithm.

efficient the algorithm. In Fig. 6.3 we analyse the performance of the BP algorithm as the distance between the primary user and the attacker is varied. We expect that, as the distance between the attacker and the primary user is decreased, the false positive rate will increase. The primary reason for this is that as the distance decreases it is harder for secondary users to distinguish between a primary user and an attacker. As the distance between the attacker and the primary user increases, it should be easier to distinguish between the two. From Fig. 6.3, we see that at about 6 metres our algorithm has a high detection accuracy making it effective at distinguishing between a PU and an attacker, the SNR used to plot this figure is 10dB and 100 secondary users.

Fig. 6.4 compares the performance of our technique as the number of secondary

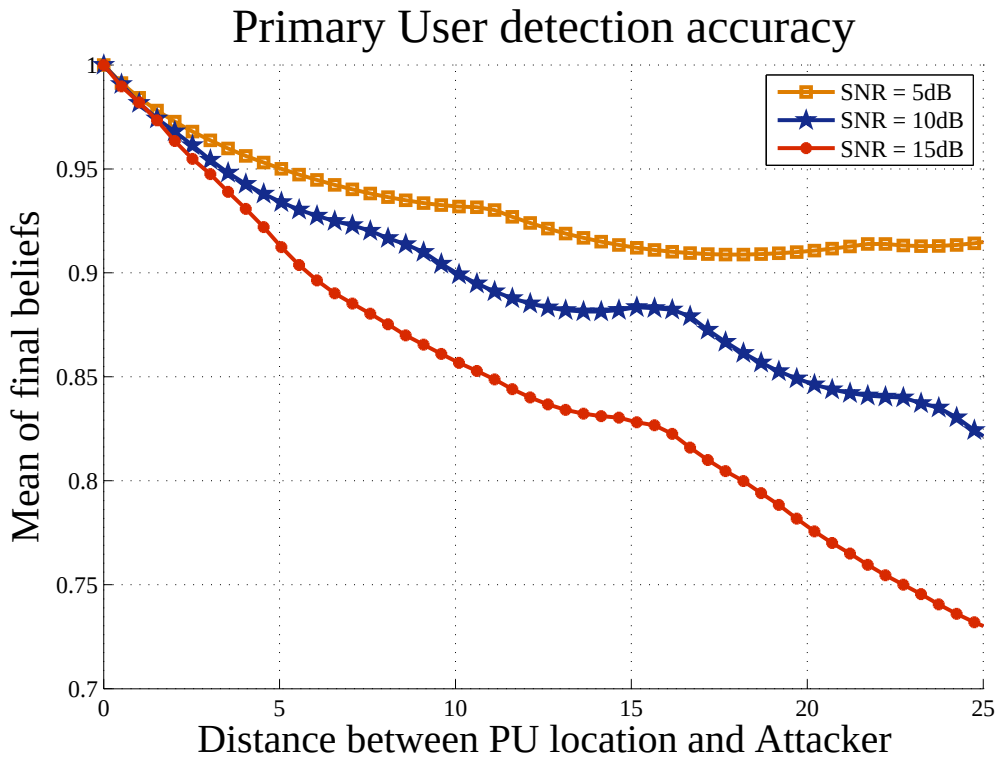

Figure 6.2: Belief Propagation analysis.

users is increased. Intuitively, as the number of secondary users in the network increases, the performance of the algorithm will improve. This is due to the fact that, as more secondary users are added, more information is available, enabling higher accuracy results. In order to increase the effectiveness of the algorithm, we use statistical averaging, where secondary user observations are relayed throughout the network and congregated to a final belief. The increase in cooperation between secondary users leads to highly accurate beliefs. As a result, the likelihood of false detection is decreased. Degradation factors such as noise and fading have a lesser impact as the number of secondary users increases, the SNR used to plot this figure is 10dB.

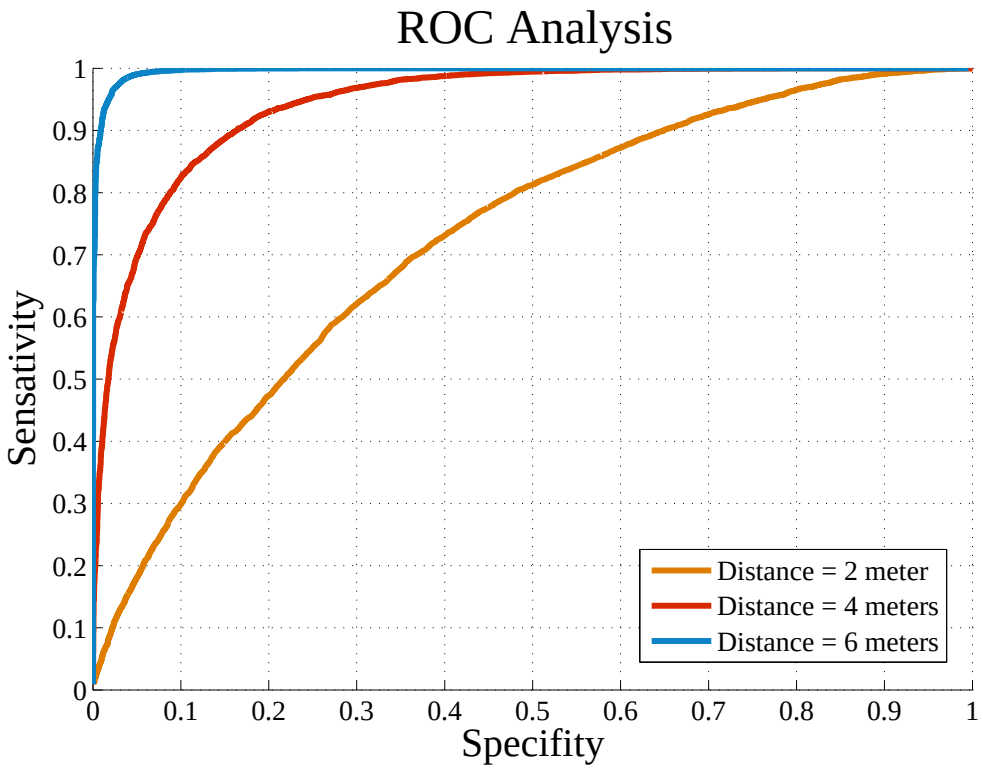

Figure 6.3: ROC analyses with varied distance.

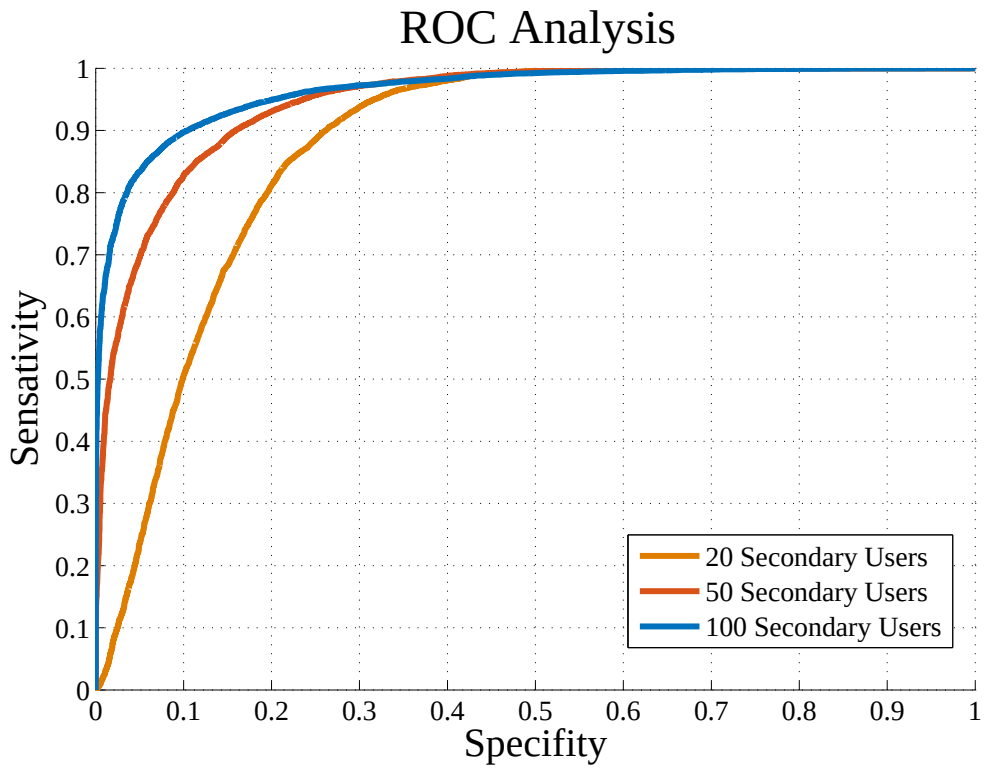

Figure 6.4: ROC analysis with a varied number of secondary users.

Chapter 7

Mitigation of Spectrum Sensing Data Falsification Attacks

Spectrum Sensing Data Falsification Attacks can be extremely effective in deceiving secondary users into falsified spectrum sensing results. To do a single, or a group of malicious users sends falsified spectrum sensing results. This results in legitimate secondary users believing that a frequency band is idle when it is not or that the frequency band is busy when it is idle. Spectrum sensing data falsification attacks are particulary potent because legitimate secondary users often pass on falsified spectrum sensing information without knowing so. This means that malicious users can cause wide spread damage with very little effort. With well positioned malicious users working in conjunction with each other, an entire network can be effected with minimum effort and time. Through this chapter, we present a reputation scheme that is able to identify and neutralise untrustworthy users by ensuring that their reputation is kept low. Then using belief propagation, we are able to identify with a high level of accuracy whether or not a radio frequency band is occupied. The main contributions for the chapter are as follows:

- A powerful algorithm that uses reputation to identify SSDFAs within the network.

- A dynamic punishment/reward function that can be altered depending on network conditions. Previous literature presented static schemes which can be exploited by smart malicious users. In our scheme we are able to punish users more for falsified results and reward them less, therefore deterring falsification. This is opposite to schemes that add 1 for every legitimate report and that often do not punish users who are sending out falsified information.

- Use of statistical outlier methods to determine with great accuracy the legitimacy of spectrum sensing results. The use of Z-scores which allow us to quickly and efficiently identify spectrum sensing results outside the expected.

7.1 Reputation/Belief Propagation System Model

In order to defend against spectrum sensing data falsification attacks, we must establish a method to determine which users are trustworthy. To achieve this we develop a reputation based scheme. Each secondary user within the network is assigned a default reputation. If they send out legitimate reports about the status of a radio frequency band, their reputation will increase. If they do not, their reputation will naturally decrease. Secondary users with low reputation are not able to contribute to the consensus of the network. Secondary users with a high reputation are able to contribute. To effectively defeat spectrum sensing data falsification attacks we use reputation in conjunction with belief propagation.

7.1.1 Local Function

Our method uses an underlying framework based on belief propagation (BP) as presented in [68], [10]. In order to analyse spectrum sensing results, we employ a belief propagation algorithm. Belief propagation is a distributed, probability based, cooperative protocol. Initially, spectrum sensing analysis is undertaken by each secondary user to calculate a

probability of whether a primary user is active on the channel. We denote this as a local belief. Local beliefs are then encapsulated into messages and distributed throughout the network [69]. Each message has a weight associated with it, which is a function of the reputation of the sending secondary user. After a secondary user receives all messages from all its neighbors, a final belief is calculated. The final belief at a secondary user is calculated using that users local beliefs and the average of all incoming messages. The proposed belief propagation method is a variant of the original BP algorithm presented in [69]. Conventional belief propagation algorithms converge after a certain number of iterations, during which each secondary users broadcasts its local belief to its neighbors.

The spectrum sensing phase is a highly vulnerable time for cognitive radios. It provides a great opportunity for malicious users to attack the network. During the spectrum sensing phase, malicious users relay falsified information about channel occupancy to legitimate secondary users in order to decrease network efficiency or gain an unfair advantage. The relay of falsified spectrum sensing information to legitimate secondary users is known as a spectrum sensing data falsification attack (SSDFA). To combat SSDF attacks, this thesis introduces a reputation based scheme that rewards secondary users transmitting legitimate spectrum sensing reports and punishes secondary users transmitting falsified reports. Secondary users with a high reputation have a high contribution to the belief of other secondary users, as their messages have a higher weight assigned to them. Messages from secondary users with a low reputation are weighted less and have a small contribution to the belief of other secondary users. The reputation score can be thought of as a measure of how correlated a pair of observations at a pair of secondary users are to each other. The higher the reputation, the higher the correlation between the a pair observations (at a pair of secondary users), the more they contribute to each other's final beliefs.

We define α_j as the decision variable of the spectrum sensing device and ϕ_j as the

quantized output of the spectrum sensing devices. The local observations for the jth secondary user, α_j is obtained using the algorithm presented in [68]. The difference between the receive signal strength (RSS) measurements is used to determine the occupancy of a channel. Each secondary user calculates the local function through comparison of the RSS from a transmitter with the theoretical measurements corresponding to the fixed location of a primary user. The higher the correlation between the RSS measurements the more likely the channel is used by a primary user. The local function corresponds to a value between 1 and 0. The closer the correlation is between the RSS values, the higher the local function value becomes. We characterise spectrum sensing reports from a secondary user j into five categories: when a primary user is active, when it is highly likely a primary user is active, when it is unknown whether a primary user is active or idle, when it is highly likely that a primary user is idle and when the primary user is idle. To represent these categories as well as the quantization values associated with each decision, we present the local function as:

$$\phi_j = \begin{cases} 0, & \text{if a PU is idle (} \alpha_j < 0.15) \\ 0.25, & \text{if PU is likely idle } (0.15 < \alpha_j < 0.35) \\ 0.5, & \text{Undecided } (0.35 \text{ ¡ } \alpha_j < 0.65) \\ 0.75, & \text{if PU is likely active } (0.65 < \alpha_j < 0.85) \\ 1, & \text{if a PU is active } (0.85 < \alpha_j \text{ }) \end{cases}$$

The local function is derived from channel output observations at SU_j, where SU_j is defined as a secondary user j. It corresponds to a belief about whether there is a primary user active on a channel or not. It is a major contributor to both the messages and the calculation of the final belief. It is therefore essential that the local function accurately represents activity of a primary user.

7.1.2 Compatibility Function

In order to characterise the correlation between secondary user observations, this thesis introduces a compatibility function. In our method, we use two scalars: the first is dependent on the distance between secondary users, the second is dependent on the reputation of each secondary user. Here a distance based compatibility function is introduced. The distance compatibility function models the correlation of the shadowing between the transmitter and two secondary users which are d_{X_i,X_j} meters apart. A pair of observations is considered highly correlated if that pair of secondary users is in close proximity to each other. Secondary users that are in close proximity usually suffer from similar channel degradation factors, such as shadowing and fading. Therefore, they are more likely to have similar observations. The further apart a pair of secondary users is, the lower the correlation of their observations. The further apart secondary users are, the less likely their observations will correlate well with each other due to the different levels of shadowing and fading. Observations from secondary users in close proximity are seen as more reliable and have a higher contribution to each other's beliefs. [68] and [10] introduce a simple exponential function to represent the correlation between shadowing and fading, between two secondary users with respect to distance. We use the Gudmundson model to describe the correlation with respect to distance between two secondary users [71]. The Gudmudson model [70] is as follows:

$$\psi_{ij} = \exp\left(\frac{-d_{SU_i,SU_j}}{D}\right) \tag{7.1}$$

where ψ_{ij} is a distance dependent correlation function between SU_i and SU_j, d_{X_i,X_j} is the distance between SU_i and SU_j in meters, D is the decorrelation distance which is empirically determined to be 8.3058 meters in [71]. This compatibility function returns a value between 0 and 1, where 1 corresponds to perfect correlation of spectrum sensing observations between secondary users, and 0 corresponds to no correlation between a pair

of secondary users. The primary motive behind the compatibility function is to ensure that secondary users get the most reliable information possible. Secondary users in close proximity are likely to have similar shadowing and fading. Therefore, observations of a pair of secondary users in close geographical proximity will likely be similar.

7.1.3 Reputation Function

A critical element of our method is the establishment of an efficient and effective reputation function. Like the distance compatibility function, the reputation function is a scalar. The higher the reputation of a secondary user, the more relevant the observations of that user become. To calculate the reputation of a secondary user, we compare the spectrum sensing reports of a reference node to the overall consensus of the network. To compare the results we use a modified Z-score formula [30], Z-scores are used to identify outliers within a set of values. The higher the Z-score the further away a result is from the mean of the set of values. The Z-score can be defined as follows:

$$Z_{i,j} = 0.6745\frac{(S_i - M)}{MAD} \tag{7.2}$$

where $Z_{i,j}$ corresponds to the Z-score of a message from SU_i at SU_j, S_i corresponds to a message coming into SU_j from SU_i, M corresponds to the median of all messages coming into SU_i and MAD is the median absolute value of all messages arriving to SU_j, it is defined as follows:

$$MAD = \frac{\sum(|m - \bar{m}|)}{M} \tag{7.3}$$

where, M is the number of secondary users, m corresponds to the messages between users and $\bar{m}$ is the average of the messages. The Z-score is used to detect outlier results within a set of messages. If the Z-score [76] of the incoming message is above a set threshold, the message is identified as an outlier. The Z-score of an incoming message

indicates how far away that message is from the median of all messages. If the Z-score ($Z_{i,j}$) of the incoming message from SU_j to SU_i is above a threshold, the outlier message is discarded and the reputation of the sender is decreased. In our context an outlier corresponds to a message that significantly differs from the average consensus of messages from other users [30], [77]. We use Z-scores to identify outliers within the network and reduce the impact they have on final observations. Outliers can have significant effects on the final belief, especially when there is a small number of secondary users present in the network. Outliers can occur in three ways:

- When a secondary user is malfunctioning and sending out erroneous observations.
- When poor channel conditions cause errors in message data during transmission over the control channel.
- When a malicious user is intentionally propagating falsified spectrum sensing results.

Unreliable spectrum sensing results are identified as outliers through z-score analysis. After $Z_{i,j}$ has been calculated for a message, it is compared to a threshold. To insure that outliers are diagnosed effectively, we set the threshold corresponding to a z-score ($Z_{i,j}$) value of 1.0. If $Z_{i,j}$ is above that threshold, the message is discarded. In addition, the secondary user that sent the message (SU_j) is punished with a decrease in reputation. In our method, falsified spectrum sensing results incur a large penalty, while accurate results incur a small reward. $\gamma_{i,j}$ can be understood as a variable corresponding to the reputation of SU_i at SU_j. Each secondary user is assigned a default reputation of 5 when they become part of the network. The maximum reputation that a secondary user can achieve is limited to 10 and the minimum reputation is limited to 0. The secondary user's reputation is updated as follows:

$$\gamma_{i,j}^{l+1} = \begin{cases} \frac{3}{4}\gamma_{i,j}^{l} + \frac{5}{2} : & \textit{for legitimate reports} \\ \frac{\gamma_{i,j}^{l}}{2} : & \textit{for falsified reports} \end{cases}$$

where $\gamma_{i,j}^{l}$ is the reputation of SU_j at SU_i for the lth secondary user observation. The rate of change of $\gamma_{i,j}^{l+1}$ is lower for legitimate messages and the rate of change of $\gamma_{i,j}^{l+1}$ is higher for SSDF attackers. The constants are empirically set to insure that legitimate reports are only rewarded with a smaller increment, whereas, users that report falsified spectrum sensing reports are punished harshly. We implement this to ensure that malicious nodes do not impersonate legitimate users for a set amount of time, and when their reputation is high, send out falsified results and cause maximum damage. Using this method, nodes looking to disrupt the network by sending out falsified results are quickly identified because their reputation is decreased quickly. The update scale can easily be modified by changing the update coefficient.

7.1.4 Messaging Protocol

An essential aspect of belief propagation is cooperation between secondary users. In belief propagation, secondary users communicate their beliefs in the form of messages. Messages, in relation to whether the channel is occupied or not, are compiled and sent to all neighbors within range. The following is the message function defined in [68]; it can be understood as a message from SU_j to SU_i, m_{ij} is given by:

$$m_{ij} = \frac{\psi_{ij} + \phi_i}{2} \tag{7.4}$$

In the messaging protocol presented in [68], the message corresponds to the average of the sum of the local function, ϕ_i, and the compatibility function ψ_{ij}. This thesis introduces a reputation function , $\gamma_{i,j}$, that is used as a weighting scalar for all incoming messages.

The higher the reputation function the more the message contributes to the total. To do this, we modify the messaging equation present in [68] to the following:

$$m_{ij} = \frac{(\psi_{ij} + \phi_i) * \gamma_{i,j}}{2} \tag{7.5}$$

where $\gamma_{i,j}$ is the reputation of SU_i at SU_j. In order to calculate the belief at each secondary user, we must find the mean value at SU_j of all the incoming messages. The mean value must take into account the weight of each message. To calculate the average of all incoming messages to secondary user j we use the following formula:

$$\mu_j = \frac{\sum_{\substack{k=1 \\ j \neq k}}^{M} m_{ij}}{\sum_{\substack{k=1 \\ j \neq k}}^{M} \gamma_{i,j}} \tag{7.6}$$

where μ_j is a representation of the true weighted average of all messages coming into SU_j, as it takes into account the weight of the reputation of each secondary user. M is the number of secondary users in the network. Secondary users with a high reputation contribute more than secondary users with a low reputation. For the algorithm to become effective it needs to run for a number of sets of secondary user observations. After each set of secondary user observations have been received a better indication about whether a transmitter is a malicious user or not is determined. We demonstrate, through simulations, that our algorithm takes about 10 sets of secondary user observations to converge to steady state.

7.1.5 Final Belief

Once the exchange of messages has concluded, each secondary user calculates the sum of their local beliefs and the average of all received messages. The final belief is calculated at the end of each set of secondary user observations by each secondary user. The final belief at SU_j corresponds to the average of the local observations at SU_j and the average

of all the messages received by SU_j. The final belief is calculated as follows:

$$b_j = \frac{\phi_j + \mu_j}{2} \tag{7.7}$$

where b_j corresponds to the belief at SU_j. Each SU calculates their own belief using Eq. (5.6). The final belief corresponds to the probability of a primary user being active on a channel. Once all secondary users have calculated their individual belief, a final belief can be calculated and compared to a threshold. The final belief corresponds to the belief of the entire network. If the final belief is above the threshold there is a primary user active on the channel, if it is below it the primary user is idle. H_0 represents the hypothesis that the transmitter is a primary user. H_1 represents the hypothesis that the transmitter is a malicious user. These are defined in previous chapters. Algorithm 1 specifies the technique which provides effective mitigation against SSDF attacks.

Algorithm 1 Complete algorithm to mitigate against SSDF attacks

Calculate local function decision variable ϕ_j using algorithm presented in [68]
Quantise ϕ_j to obtain α_j
for Each set of secondary user observations l **do**
    for j = 1 to number of secondary users **do**
        for i = 1 to number of secondary users **do**
            Compute Compatibility function between SU_j and SU_i, ψ_{ij} using Eq. (7.1)
            Compute messages using Eq. (7.3)
            Exchange messages with neighbours
            Use Eq. (7.2) to determine whether a incoming message is an outlier (Z-score)
            if $Z_{i,j} > 1$ **then**
                if $1 < \gamma_{i,j}^{l}$
                    Punish user $\gamma_{i,j}^{l+1} = \frac{\gamma_{i,j}^{l}}{2}$:
            else
                if $10 > \gamma_{i,j}^{l}$
                    Reward user $\gamma_{i,j}^{l+1} = \frac{3}{4}\gamma_{i,j}^{l} + \frac{5}{2}$
            Compute the message average at SU_j using Eq. (5)
            Compute belief at SU_j using Eq. (6)
        end if
    end for
end for
end for
if $\frac{1}{M}\sum_{j=1}^{M} b_j > b_t$
    Decide primary user
if $\frac{1}{M}\sum_{j=1}^{M} b_j < b_t$
    Decide malicious user

7.2 Results and Simulations

In this section we provide simulation results indicating that our method effectively mitigates against spectrum sensing data falsification attacks. We consider two scenarios, the first when a malicious user simply reports the opposite of what they sense. In this case, if a primary user is active, the malicious user reports that they are idle. If the primary user is idle, the malicious user reports that they are active. This strategy ensures maximum impact on the network, but it means that malicious users are easier to identify. In the second case, a malicious user sends out a random normally distributed sensing result. The sheer randomness of the data means that the malicious user is hard to identify. However, the impact on the network is decreased. Our algorithm is a simple and effective way to diagnose and mitigate the effects of spectrum sensing data falsification attacks. In most cases, it takes about 10 sets of secondary user observations for the algorithm to effectively diagnose and mitigate a threat, even with a high percentage of malicious users in the network.

As the number of number of secondary user observations increases, a secondary user is able to establish a comprehensive reputation database. As the reputation values converge, the beliefs at the secondary user become more reliable and accurate. The underlying belief propagation algorithm used throughout this paper is very effective at minimising the effects of spectrum sensing data falsification attacks, even without the reputation component. Belief propagation results are aggregated, and a small number of malicious users will not have a great effect on the final belief. However, with the introduction of a larger percentage of secondary users, our results begin to degrade.

To simulate our scenarios, a simple system model (shown in Fig. 7.1) is chosen. In our model, we have a 100 by 100 meter grid. Secondary users are randomly scattered (using a normal distribution) throughout the grid. There are 50 secondary users in the network and there is a single primary user, located in the center. Malicious nodes are hidden within

the 50 secondary users scattered across the network. They act and function as though they are legitimate secondary users. We plot the number of secondary user observations against the mean of beliefs which is $\frac{1}{M}\sum_{j=1}^{M} b_j$, In the following simulation results, the channel is assumed to be occupied by a primary user, the SNR used throughout this chapter is 10dB.

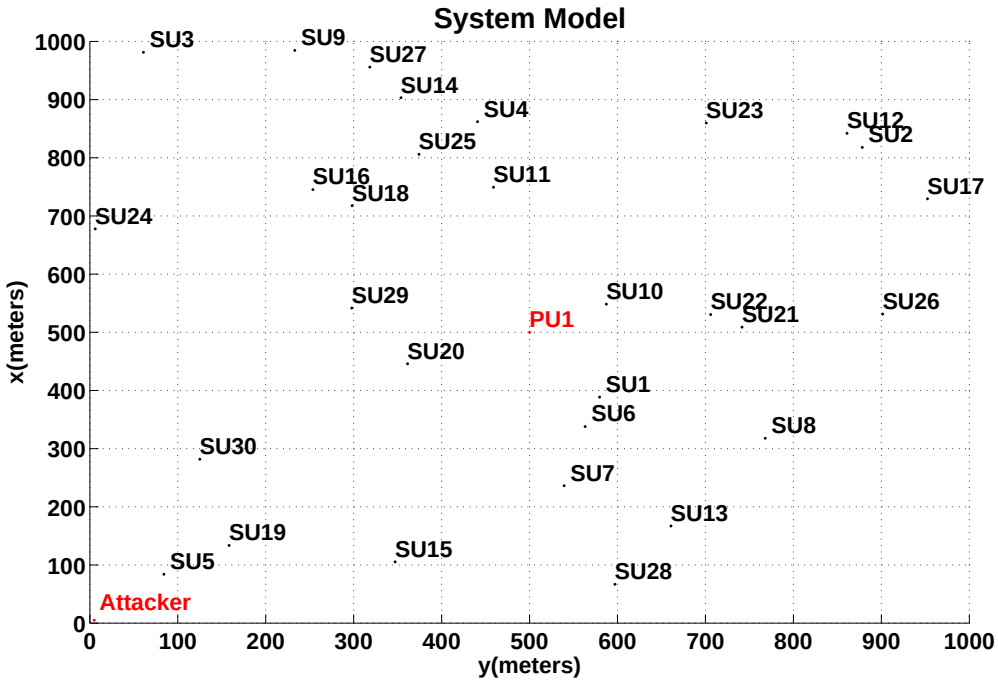

Figure 7.1: Network model.

In order to simulate the effects that malicious nodes have on the network, we randomly select 15 secondary users to become malicious nodes (corresponding to 30% of total users). We assume that a message from one node to another is delivered reliably and accurately. In the first scenario, 15 secondary users are selected at random to act as malicious users. These users will constantly send out falsified information to their neighbours. If a primary user is idle (corresponding to a 0), the malicious user reports that a primary user is active (corresponding to a 1), If a primary user is active, the malicious user reports that the primary user is idle. We denote this type of attacker as a naive attacker (with reference

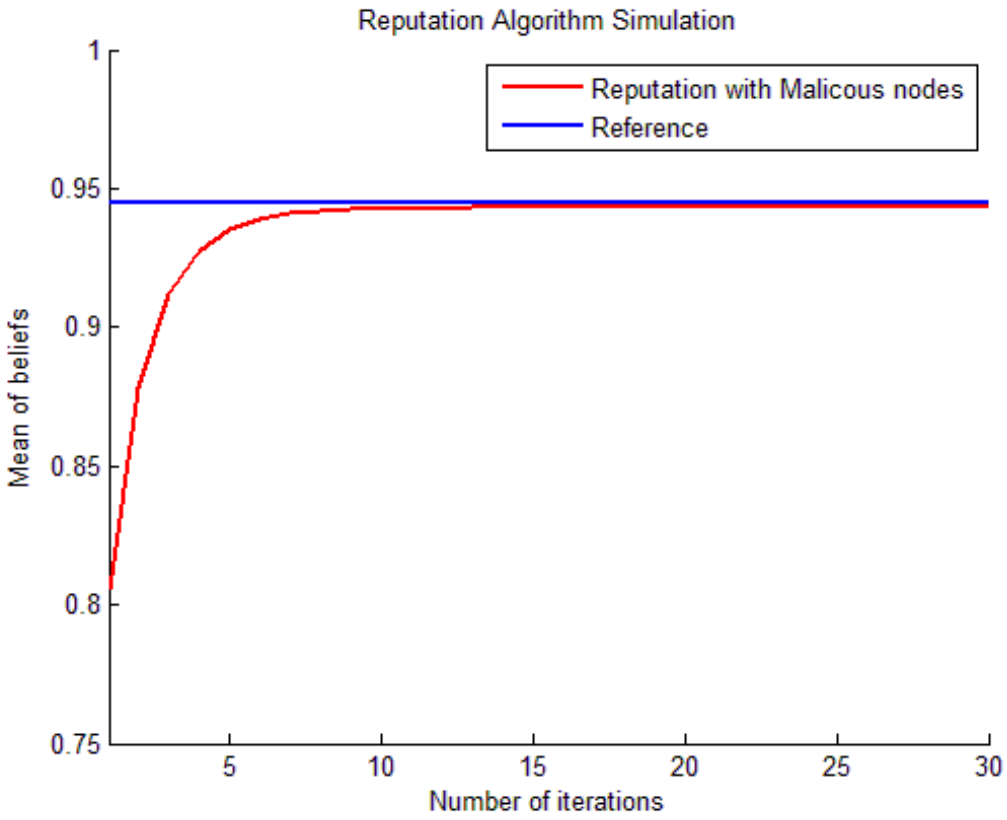

Figure 7.2: Results obtained with naive malicious nodes.

to the initial value of the reference plot). The naive attack causes maximum damage, but is relatively easy to mitigate. We investigate the effects of naive attackers on the network in Fig. 7.2. Initially the belief has decreased quite significantly. As we move through the a set of secondary user observations, the belief converges to the reference (the reference belief corresponds to the ideal case when no malicious nodes are present). It takes about 10 sets of secondary user observations for the malicious nodes to be identified and mitigated using our method. Fig. 7.2 demonstrates the effectiveness and efficiency our method in mitigating spectrum sensing data falsification attacks. In the second scenario, 15 users are selected once more. These users now send out random spectrum sensing information.

In order to investigate the effectiveness of our method further we consider a more

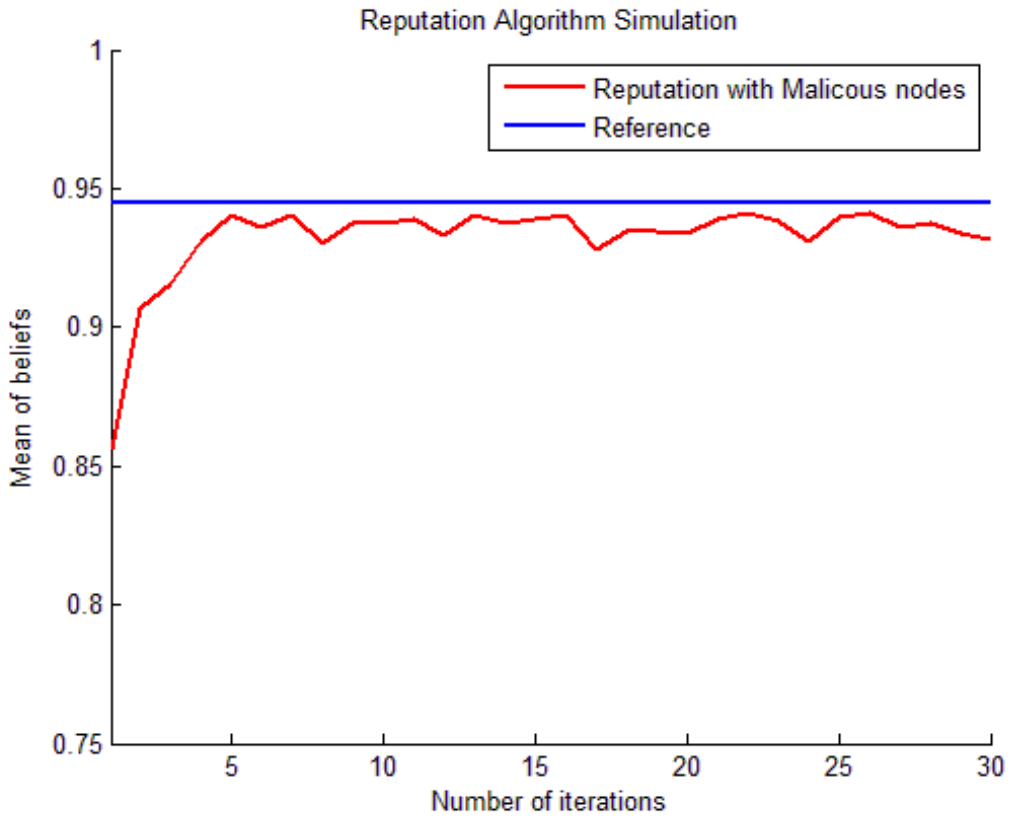

Figure 7.3: Results obtained with smarter malicious nodes.

sophisticated type of attack. When a malicious user sends out randomised results that are not all in close agreement with their own spectrum sensing results. This form of attack is much harder to identify, as some of the random results might correspond closely to actual spectrum sensing results. However, the randomness of the results means that they have a much smaller effect than that of the naive attack. Fig. 7.3 presents simulation results of our method. As is evident, within the first couple of sets of secondary user observations there is steep increase in the mean of beliefs. Followed by a more stable period near the ideal value (reference). The results near the ideal value do vary slightly due of the randomness of the observations of the malicious users. However, results are very close to ideal after only 5 sets of secondary user observations. Once again Fig. 7.3 demonstrates

the effectiveness of our algorithm. We see that secondary users that send out falsified results are excluded from contributing to the overall consensus fairly quickly.

Chapter 8

SSDFA, Reputation Mining and Reset attacks

In this section we present a Belief Propagation Based Statistical Reputation Function (BPBSRF) algorithm to combat Spectrum Sensing Data Falsification Attacks in Cognitive Radio networks. The contributions of this chapter are as follows:

- A complete algorithm that is able to mitigate not only SSDFA attacks, but also reputation mining and reset attacks. These have previously never been mitigated by a single algorithm. Which makes this solution the most complete solution.
- Identification of two novel attack types. The reputation mining attack and the reset attack which affect reputation based schemes. These are novel attack types often overlooked. However, if executed correctly they can have detrimental effects on network performance.
- Introduction of a random back-off period for users that report spectrum sensing information outside the statistical average. In addition a three strike rule to ensure that repeat offenders are identified and ejected from the network.

- A probation period that is activated when a new secondary users joins the network. This serves as a deterrent for secondary users who want to continuously report falsified information until their reputation decreases, then simply restart and reset their reputation to the default value.

To combat SSDFAs a dynamic function is introduced, which allows a user to change the penalty/reward for secondary users. We also introduce two new types of attacks that have previously not been identified. This thesis introduces a reset attack, which is where a malicious user continually sends out falsified information until their reputation is low and then resets their system by leaving the network and re-entering the network. This resets their reputation to the default and they are able to continue to attack. To combat this a probation period for new users is introduced. In essence the probation period corresponds to a set period of time that each secondary user must wait until their spectrum sensing results become relevant to the rest of the network. An important feature of the probation period is that new users must still send in their spectrum sensing results and their reputation values are still increased/decreased according to the validity of their results. This ensures that before a new user has the opportunity to contribute to the overall consensus they are evaluated as either trusted or malicious. Reputation mining attacks are another type of attack that has serious effects on the performance of the network. In a reputation mining attack, a malicious node will report legitimate spectrum sensing information until they accumulate a sufficient reputation and are deemed trustworthy. At this point they launch an attack and as a result of their high reputation, they are able to do significant damage. To mitigate against reputation mining attacks, a back-off period for secondary users is introduced, it sends out falsified reports. When falsified information is sent, the user is blacklisted and is subject to random back-off period, after which they can again contribute to the overall result. If after the back-off period the falsified reports continue, the secondary user is cautioned and then banded

permanently. The reason for this approach is that sometimes legitimate secondary users might malfunction, which could lead to them mistakenly being identified as malicious nodes. We present our algorithm in full below in the subsequent sections.

8.0.1 Energy Detection

During the spectrum sensing phase each secondary user must perform their own local spectrum sensing. For our method energy detection is the preferred spectrum sensing technique, chosen because of its simple implementation and design. A signal coming into a secondary user consists of two elements, the signal generated by a PU and the noise that accompanies that signal as it is propagated throughout the network. We define SU_i as secondary user i, where i corresponds to the index of SUs in the network. Then, the jth sample at SU_i is defined as follows:

$$X_i(j) = \begin{cases} n_i(j) & H_0 \\ h_i s(j) + n_i(j) & H_1 \end{cases} \tag{8.1}$$

where, we have n SUs such that $s_i(j)$ is the received signal at SU_i, $n_i(j)$ is the noise and h_i is the shadow fading variable defined as $h = e^{ab}$ where $a = \frac{ln10}{10}$, b is defined as a random Gaussian variable with a 0 mean and variance σ^2 [78]. If we take n samples at each SU in the network. The energy at a SU_i is defined as:

$$E_i = \sum_{j=1}^{n} |x_i(j)|^2 \tag{8.2}$$

We denote E_i as the measured energy at SU_i. We assume that SU know the location of the PU. Therefore, each SU is able to calculate a theoretical energy value (T_i), which can be used as a comparison. We use the local function to calculate the similarity between the measured and theoretical values.

8.1 Belief Propagation Based Statistical Reputation Function (BPBSRF)

In this section we propose the BPBSRF algorithm. We base our algorithm on a belief propagation (BP) framework with a reputation based component. We add two new features to the algorithm to mitigate against two new types of attack, the reputation mining attack and the reset attack.

8.1.1 Local Function

The local function corresponds to the local observations at a SU, regarding the presence or absence of a PU on the channel. The local function serves as a baseline observation for each SU on the network. The local function can be understood as a probability about whether or not a PU is actively transmitting. We define the local function at SU_i as follows:

$$\eta_i = exp\bigg(- \frac{|E_i - T_i|}{E_i + T_i} \bigg), \tag{8.3}$$

where, E_i is the measured energy from the transmitter and T_i is the theoretical energy measurement, both at SU_i. The local function corresponds to 1 when a SU is certain that a PU is actively using the channel and 0 if the secondary user is certain the channel is idle. The local function is a representation of a PUs activity, it can be thought of as single perspective of a much larger picture. In order to have an accurate representation of the whole picture, we must obtain observations from as many sources as possible. The larger the number of observations the higher the accuracy of our algorithm. Each SU is therefore obligated to share their local observations with every other user on the network.

8.1.2 Computability Function

The reputation function is essentially a measure of compatibility between two SUs. It can be seen as a trust metric used by SUs within the network to gauge how reliable incoming spectrum sensing results are coming from another SU. The higher the reputation function the more likely that spectrum sensing results are valid. Prior to defining the reputation function we must establish a method for identifying results that are outside the expected range. To identify falsified results we use the Modified Thompson-Tau Outlier Detection Method (MTTODM) [79], which takes a set of values and an incoming value and determines whether or not the new value is a statistical outlier.

We denote a reference SU as SU_i. The spectrum sensing results from all neighbouring SUs are denoted as $m_{i,j}$. $m_{i,j}$ is defined as a message containing spectrum sensing results from SU_j to SU_i, if there are n SUs we have $m_{i,1}$,$m_{i,2}$,...,$m_{i,n}$ messages received by SU_i. The MTTODM is a multi step process, and the algorithm is outlined as follows:

- Calculate mean ($\bar{x}$) and standard deviation (s), of all incoming messages.
- A deviation value is calculated at each point. The value with the biggest deviation is the most likely suspect $\delta_n = |x_n - \bar{x}|$.
- The Thompson-Tau outlier τ is calculated using:

$$\tau = \frac{t_c(n-1)}{\sqrt{n}\sqrt{n-2+t_c^2}} \tag{8.4}$$

where, t_c is a critical value that depends on the number of SUs. If an outlier is found it is omitted from the set. Using the MTTODM we are able to identify statistical outliers within the network. With this information we are able to formulate a reputation function that rewards SUs that report legitimate information and punishes SUs that report falsified information. The reputation value of SU_j at SU_i is defined as follows:

$$\omega_{i,j}^{l+1} = \begin{cases} \omega_{i,j}^{l} + \left(\frac{10-\omega_{i,j}^{l}}{a_l}\right) : & \textit{for legitimate reports} \\ \frac{\omega_{i,j}^{l}}{a_f} : & \textit{for falsified reports,} \end{cases}$$

where, $\omega_{i,j}^{l+1}$ represents the updated reputation of SU_j at SU_i, $\omega_{i,j}^{l}$ is the previous reputation value of SU_j at SU_i, a_f and a_l are dynamic variables that can be changed to incur a larger or smaller penalty/reward for SUs reporting falsified reports/legitimate results. If for example, a_1 is set to 2 than the secondary users increase their reputation by 50% for every legitimate report. If the value is changed to 4, than the reputation would increase by 25%. In this way a_1 and a_2 control how much reward/punishment is inflicted onto secondary users. It is important to note that $0 < \omega_{i,j}^{l+1} < 1$. In this paper we use $a_f = 2$ and $a_l = 4$, primarily because we want our reputation to decrease quicker when SUs are reporting falsified information and increase slower when SUs are reporting legitimate reputation. This feature foils another type of attack that looks to take advantage of the reputation based function. Smart secondary users can report legitimate results for a period and then when their reputation is high they can begin to report falsified information with maximum effect. By ensuring that reputation is increased slowly we hinder this type of attack. In order to incorporate the reputation function within the belief propagation framework we denote the reputation value as a compatibility function. The compatibility function represents the level of correlation between two secondary users. The compatibility function is heavily influenced by the distance between two secondary users. If two secondary users are located in close proximity their beliefs will correspond closely with each other, because their perspective of the transmitter is similar. We define the compatibility function as follows:

$$\psi i, j = \log_{10}\left(1 + \frac{9\omega_{i,j}}{10}\right) \tag{8.5}$$

The compatibility function can be seen as a measure of how much trust has been

established between SU_i and SU_j (how compatible two users are).

8.2 Belief Propagation

After a secondary user obtains their spectrum sensing results they are obligated to pass on their observations throughout the network. To do this each secondary user formulates a simple message as follows:

$$m_{i,j} = \phi_i(X_i) \tag{8.6}$$

We define $m_{i,j}$ as a message from SU_j to SU_i. After SU_i has received the message, the reputation of the sender is appended to the message as a weighing factor. We use the reputation as a weighting factor, which represents the level of trust that exists between the sender and the receiver. The message at the receiver is as follows:

$$m_{i,j} = \frac{\phi_i + \psi_{i,j}}{2} \tag{8.7}$$

Using Eq. (8.7) we ensure that the incoming messages are scaled appropriately according to the reputation value of the sender. If the reputation is low, the messages originating from the SU are not going to contribute in meaningful way to overall belief at the receiving SU. After all messages have been received at SU_i, a final message is computed using the following:

$$M_{f_i} = \frac{1}{n} \sum_{\substack{j=1 \\ j \neq i}}^{n} m_{i,j}, \tag{8.8}$$

where, n denoted the number of secondary users in the network and M_{f_i} can be thought of as the summation of all local observations scaled by the reputation of each secondary user. It represents the combined final belief of all neighbouring nodes of SU_i.

8.2.1 Final Belief

When all messages have been exchanged, a final message value is calculated. Using this in conjunction with the local observation at the receiving SU we are able to calculate the final belief about whether the primary user is active on the channel or not. We calculate the final belief using the following:

$$b_i(X_i) = \frac{\phi_i(X_i) + M_{f_i}}{2} \tag{8.9}$$

This final belief corresponds to a belief about the presence of a primary user within a frequency band. To calculate the final belief we use the average of the local belief and all received messages. If the final belief is 1 we are absolutely sure that a primary user is active and if the final belief is 0 we are absolutely sure that the primary user is inactive.

8.2.2 Special Features

We implement a number of key features within our method to mitigate against malicious nodes that could use more sophisticated ways to attack the network. In this section we present two new attack types and provide ways of mitigating their effects on the network. These attacks are overlooked in many SSDFA mitigation methods, but they pose a real threat and can be used to continue attacks even after the implementation of mitigation schemes. The mitigation of these attacks significantly strengthens our method making it a the most complete algorithm available. Without effective method of dealing with reputation mining and reset attacks, MUs can easily continue to depredate network performance.

8.2.3 Probation Function

An attack called a reset attack is used by a malicious node when their reputation value has decreased significantly, making their observations obsolete. Conventionally, the way

that reputation functions work is that as a user enters the network they receive a default reputation function. Their reputation is then modified according to the legitimacy of spectrum sensing results. In reset attacks a MU could send out falsified messages until their reputation was very low and then just exit and re-enter the network. This would reset their reputation and they could continue to send out falsified results. To combat reset attacks, a probation period ius introduced, during which a new user does not contribute to the overall belief. However, their reputation value is changed according to their belief. At the conclusion of the probation period, if a user has obtained a high enough reputation it would be allowed to contribute to the belief. If their reputation is low their results would be disregarded. The probation period is determined using a random number generator, it corresponds to the number of spectrum sensing periods that a new user must wait before their observations are deemed valid.

8.2.4 Back-off Period

The back-off function is another important feature of our method. A highly susceptible aspect of any reputation based function is reputation mining. Where a malicious user sends out legitimate reports to build up a reputation after which they proceed to send out falsified results with maximum impact on the network. To combat reputation mining attacks a random back-off period is introduced. We use a random backoff period to ensure that malicious users are not able to predict the backoff period and use it to their advantage. When a transmitter sends out spectrum sensing information that is identified as an outlier using the MTTODM, that secondary user must accept a mandatory random back off period, during which they cannot contribute the over consensus of the network. The random backoff period was used so that attackers are not able to predict the backoff period and use it to their advantage. During this period, they are not eligible to receive any spectrum sensing results from other secondary users. Once the back-off period has

concluded the transmitter will be subject to a probation period as discussed in the previous section to ensure that a reputation mining attack is not effective.

8.3 Analysis of Results

In this section we present simulation results that demonstrate the effectiveness of our algorithm to mitigate against SSDFA in CR networks. The primary goal of our method is to identify and nullify malicious users that endeavour to decrease overall efficiency or cause interference between the PU and the SUs. We use reputation to identify which users are legitimate and which are malicious. To effectively analyse the performance of our algorithm we create a 1000 meters by 1000 meters grid, 300 Secondary users are scattered randomly with a uniform distribution. A total of 1000 Monte Carlo runs were carried out to obtain the results.

The system model has one primary user situated in the center, with 300 secondary users randomly scattered around it. For our simulation we chose to have 210 legitimate secondary users. 10 are new user and 200 are established users. In addition we chose 90 malicious users, which corresponds to 30% of the total number. Spectrum sensing attacks are most prevalent in situations where there is a large groups of secondary users working together. The higher the percentage of secondary users the better the chance that they can convince legitimate secondary users of falsified spectrum sensing information. To demonstrate this we present Fig. 8.1. In Fig. 8.1 we see the effects of spectrum sensing data falsification attacks when 35% of the total users are malicious. Before the implementation of our method we note that the performance of the network is severely diminished, this is due to the distribution of falsified spectrum sensing reports by the attackers. For this scenario the primary user is active. So the belief should correspond to 1. However as we see in the first iteration (before implementation of BPBSRF) we

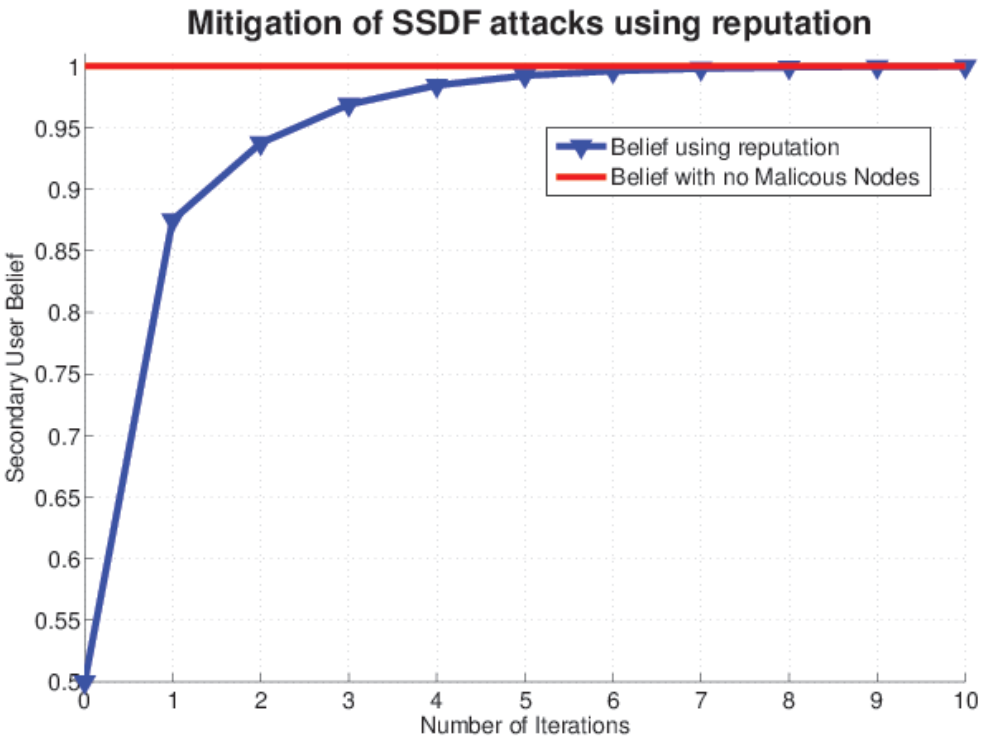

Figure 8.1: Mitigating SSDFA using reputation.

see that the belief drops by approximately 50 percent. As our method is introduced and begins to identify malicious nodes we see that the belief steadily increases until it is very close to 1.

After 4 iterations, we see that we have successfully identified more than 90% of the malicious nodes. After 6 iterations, the algorithm stabilises and the belief converges to 1. As a result, we are now able to correctly deduce whether a primary user is active on the channel. A key aspect of spectrum sensing data falsification attacks that is often overlooked in reputation based schemes is an attack we classify as a reset attack. A reset attack involves a malicious user who after a number of iterations knows that their reputation is very low, meaning that their attacks have a minimal effect of the network, and so decides to reset and obtain the default reputation. Fig. 8.2 demonstrates the effects of this attack on network performance as well the effect of another attack we

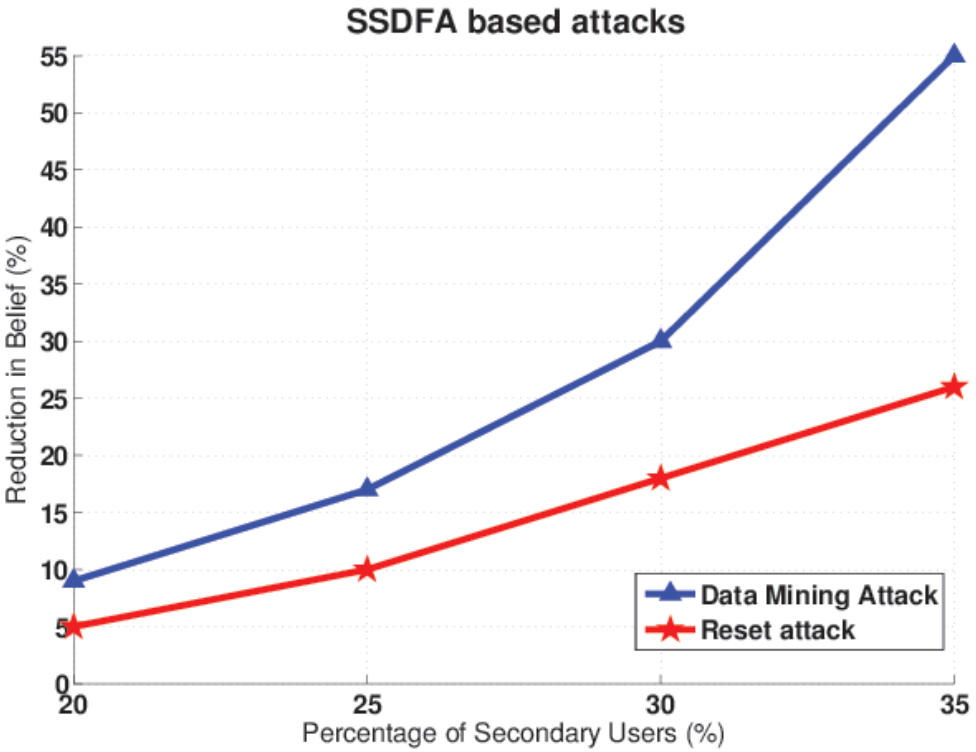

Figure 8.2: The effects of data mining and reset attacks.

classify as a reputation mining attack. In a reputation mining attack malicious nodes build up reputation over a period of time. Then when their reputation is large they begin spreading falsified reports throughout the network. This type of attacks is also shown in Fig. 8.2 and is extremely effective because secondary users on the network trust malicious reports.

Fig. 8.2 shows the effects of reset attacks on the network. It is evident from the simulation results that reset attacks have a significant effect on the performance of the network. Using our method we are able to completely eliminate the effects of this type of attack using a probation period as discussed in previous sections. Fig. 8.2 also demonstrates the effects of reputation mining attacks. As we can see the effects of this attack are greater because malicious nodes have developed a trust with malicious nodes. To mitigate against this type of attack a random back-off period is introduced which we discuss in

previous sections.

The effectiveness of reset attacks and reputation mining attacks has largely been overlooked in the literature. However, we have shown that both have a profound effect on the overall performance of the system. Our method is able to diagnose and completely eliminate both attacks with two simple algorithms. Their simplicity and effectiveness are key design features that enable our method to mitigate against spectrum sensing data falsification attacks efficiently.

Chapter 9

Discussion and Conclusion

Technological advancements have revolutionised our lives in almost every way imaginable. Over a relatively short period of time we have seen great advancements in health, education, travel, entertainment, economics as well as many other aspects of our lives. As a result of the rapid advancements in technology, many aspects of resource management and stainability were not considered in the early stages of its development. The allocation of frequency within the radio frequency spectrum is key in enabling the future growth and advancement of wireless technology. As a result of the unanticipated growth of wireless technology, certain frequencies within the radio frequency spectrum have become overpopulated. Whereas, other frequencies have been shown to be severely underutilised. This has led to a large push to find alternative methods to better utilise parts of the radio frequency spectrum. Many solutions have been proposed over the years, among them, the most promising is Cognitive Radio. Cognitive radio enables unlicenced users to share previously unusable licenced bands, alleviating congestion in unlicenced bands and increasing utilisations in licenced bands. However, its implementation has never been realised because of it susceptibility to a number of security threats.

Throughout this thesis we have developed a number of algorithms to mitigate against

physical layer attacks in cognitive radio. In particular, we concentrate our efforts on identifying and mitigating primary user emulation attacks and spectrum sensing data falsification attacks. These are seen as critical areas of vulnerability within the cognitive radio security framework. Primary user emulation attacks consist of a attacker mimicking the properties of a primary user to try and trick secondary users. If the attacker is successful secondary users would think that a primary user has become active and they would vacate the channel immediately leaving it available for the attacker to use uncontested. As a result, the overall efficiency of the network is decreased. This form of attack is especially potent when the attacker is working within a team. With power management and a optimised jamming policy, a small number of attackers can have significant effects of the performance of the network. To mitigate primary user emulation attacks, this thesis presents a novel belief propagation based approach. The proposed method uses Receive Signal Strength measurements to localise the transmitting node. This location is then compared to a known location of the primary user and if they match, the transmitter is thought of as a legitimate user. A belief is calculated corresponding to how likely a transmitter is a primary user based on their location. Each secondary user calculates their own local belief corresponding to their own observations about the identity of the transmitting node. After sensing and calculations are complete, each secondary user sends out their beliefs to all neighboring nodes. At which point, each secondary user calculates a final belief based on their own observations in conjunction with the observations of all their neighbors. Belief propagation methods are very effective. The proposed method's key contribution is the significant reduction in computational complexity, in situations where there are a large number of secondary users. It is able to reduce the convergence time from a few hours to less than a second. Traditionally, belief propagation protocols are iterative in nature. In belief propagation secondary users exchange information in the form of messages. With each iteration of exchange of messages, the algorithm converges

closer to the final belief. This thesis presents an algorithm based on belief propagation that is able to converge in a single iteration. Significantly reducing the efficiency of the algorithm, while preserving its effectiveness.

Spectrum sensing data falsification attacks involve an attacker spreading falsified spectrum sensing results to secondary users in order to change their perception on the status of the frequency spectrum band. From a power management perspective, this type of attack is more efficient. Its effects are also long lasting because each neighboring node not only modifies their belief but propagates that belief to all of their neighbors. It is therefore essential that mitigation methods are able to identify and ignore measurements from attacking nodes. This thesis not only presents novel mitigation methods it also identifies two novel attack types. These present a significant addition to the physical layer security framework of cognitive radio networks. Transmitting nodes that are not reporting legitimate spectrum sensing information are cast as outliers and have their reputation reduced. As a result, their future spectrum sensing results have a reduced influence on the final belief of legitimate secondary users. Reputation mining attacks consist of attackers mining their reputation until they have a large influence among their neighbours, at which point the begin to send falsified spectrum sensing reports which have a significant impact on the overall belief. In a reset attack, an attacker continuously sends out falsified information until their reputation is very low. At which point, they reset their node and are given the default value. Much like SSDFAs these can have significant effects if they are left unchecked. The following is a summary of the contributions of this thesis:

- A fundamentally new simplified belief propagation based algorithm to identify and mitigate against primary user emulation attacks. The convergence time of the algorithm was decreased significantly relative to the time reported in previous literature, with the introduction of a new local function. This is especially true when there is a large number of secondary users in the network. In some cases the convergence

time was decreased from hours to seconds.

- Development of a novel single iteration belief propagation algorithm to combat primary user emulation attacks. Previous belief propagation algorithms were iterative in nature and required as much as 10 iterations to reach a satisfactory result. The new algorithm presents a fundamental improvement and is able to achieve a same level of accuracy with a single iteration. This significantly reduces the complexity of the algorithm, which enables for easier implementation. This algorithm is most effective in large networks where many secondary users are exchanging information.

- An algorithm to combat spectrum sensing data falsification attacks in cognitive radio networks. Using the belief propagation framework in conjunction with a reputation based compatibility function, we are able to mitigate the effects of SSDFAs. This novel hybrid method increases detection rates, and outliers are identified using a modified Z-scores based function [30]. This algorithm is well rounded, fast, accurate and easy to implement.

- A revolutionary hybrid compressive sensing belief propagation algorithm that greatly improves the accuracy. Compressive sensing increases the localisation accuracy of the transmitter. This allows for better comparison with the primary user location, greatly increasing accuracy. This algorithm can be implemented in both a centralised and distributed architecture.

- A highly accurate novel Belief Propagation Based Statistical Reputation Function (BPBSRF) algorithm to combat Spectrum Sensing Data Falsification Attacks in Cognitive Radio networks. We use a dynamic reputation function that can be adjusted to reflect the degree of punishment and reward to be given out to secondary users. This is the best and most complete algorithm to combat SSDFAs. It is a complete mitigation algorithm that completely neutralised SSDFAs.

- The identification of a novel type of attack called a reputation mining attack. A reputation mining attack involves an attacker pretending to be a legitimate user to build up its reputation to the point where they are trusted by other secondary users. Then it begins to transmit falsified results with maximum impact on the network. We characterise this new type of attack and present a method to alleviate it. To combat this a three strike policy is introduced, with a mandatary suspension to users who report falsified reports.

- The identification of a novel attack, called a reset attack. This thesis introduces a probation function to deal with this type of attack. A reset attack involves an attacker sending out falsified results until their reputation is low, at which point they reset and are given a default reputation. This type of attack is characterised within this thesis and a method to mitigate its effects is presented.

- A unified physical layer algorithm able to effectively mitigate both SSDFA and PUEAs. This novel unification approach to the mitigation of physical layer attacks simplifies implementation and decreases the overall complexity of processing to mitigate these attacks by the secondary user.

The algorithms presented in this chapter were designed to be low computational complexity and practical for implementation in highly distributed networks, which consist of users with limited computational ability and power. The algorithms that are proposed are highly flexible and effective. They can also be implemented in a number of systems outside the cognitive radio framework.

9.1 Future Work

There are several natural extensions of this thesis. User localisation and authentication are security issues concerned in almost all wireless technology. We hope to extend the application of our algorithms into V2X (vehicle to everything) technology. Authentication and confidentiality are key concepts in V2X, autonomous vehicles continuously rely on the information relayed to them by other vehicles and road side units to make decisions about its operation. It is therefore key that vehicles know which information is coming from a legitimate source and which is coming from malicious nodes. Reputation based methods such as the ones presented in this thesis enable vehicles to make informed decisions about which information to use and which to discard.

We hope to extend our work into wireless sensor node(WSN) which form the backbone of future IoT networks, which we believe will be integrated into the 5G framework. The Internet of Things (IoT) refers to the inter-connectivity of the already existent Internet and the newly formed physical networks [80]. The Internet of Things envisions a future where physical and digital devices are linked together to form one network. Smart homes, hospitals and shopping centres will all be connected to ensure optimum conditions for their users. Wireless sensor networks are fundamentally at the center of this vision, IoT is the method of connecting WSN networks together into one big network. The IoT vision of connecting smart devices/sensors all over the world to create one large network introduces a number of security concerns for its users.

The IoT infrastructure is extremely vulnerable to attacks. Its sheer size means that it is almost impossible to monitor all devices on the network. Devices are usually left unattended which makes them easy targets for both cyber and physical attacks [81]. The IoT is also based on wireless technology, which makes it easy for eavesdroppers to intercept communications. Man in the middle attacks and data theft are seen as major security threats as far as wireless communications are concerned. Mitigation of these security

attacks becomes all the more challenging when we consider that many of the devices connected to the IoT are simple and have low capacity, making it difficult for them to perform complicated computations. In essence, any algorithm designed to prevent attacks must be extremely lightweight in order to be practical in such networks.

The implementation of the IoT within the existing Internet architecture requires consideration of a number of security aspects, chief among them being data confidentiality and privacy. A basic requirement for the implementation of the IoT would include the definition of suitable mechanisms to access data on devices. Access to devices such as medical records and machines must only be done by authorised personnel. The sensitive nature of data within some industries means that tt is therefore essential that security algorithm are effective in keeping out unwanted users. Our algorithms form a basis for a security framework in cognitive radio networks. However, much of the work can be applied to IoT security as well. In particular, our reputation based algorithms can be used to identify and authenticate legitimate users. Hash authentication protocols can also be used to provide added security. The algorithms that were presented in this thesis were designed for reliability, effectiveness and most importantly low complexity.

Bibliography

[1] S. Latif, F. Pervez, M. Usama, and J. Qadir, "Artificial intelligence as an enabler for cognitive self-organizing future networks," *CoRR*, vol. abs/1702.02823, 2017.

[2] B. O'Keefe, "Finding location with time of arrival and time difference of arrival techniques," *ECE Senior Capstone Project 2017 Tech Notes*, 2017.

[3] A. Biswas and S. Reisenfeld, "New high resolution direction of arrival estimation using compressive sensing," in *2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp. 1–6, June 2017.

[4] Tevfik Yucek and Huseyin Arsla, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications ," *Communications Surveys & Tutorials, IEEE (Volume:11, Issue:1), pp. 116 – 130*, Mar. 2009.

[5] Federal Communications Commission, "Spectrum policy task force," *Rep. ET Docket no. 02-135, Nov. 2002.*

[6] M. Pätzold, "5g developments are in full swing [mobile radio]," *IEEE Vehicular Technology Magazine*, vol. 12, pp. 4–12, June 2017.

[7] X. Liu, M. Jia, Z. Na, W. Lu, and F. Li, "Multi-modal cooperative spectrum sensing based on dempster-shafer fusion in 5g-based cognitive radio," *IEEE Access*, vol. PP, no. 99, pp. 1–1, 2017.

[8] I. Kakalou, K. E. Psannis, P. Krawiec, and R. Badea, "Cognitive radio network and network service chaining toward 5g: Challenges and requirements," *IEEE Communications Magazine*, vol. 55, pp. 145–151, NOVEMBER 2017.

[9] J. Rodriguez, *Cognitive Radio for 5G Wireless Networks*, pp. 336–. Wiley Telecom, 2014.

[10] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, pp. 1850–1860, November 2012.

[11] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25–37, Jan 2008.

[12] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, pp. 110–119, Sept 2006.

[13] X. Zhou, Y. Xiao, and Y. Li, "Encryption and displacement based scheme of defense against primary user emulation attack," in *4th IET International Conference on Wireless, Mobile Multimedia Networks (ICWMMN 2011)*, pp. 44–49, Nov 2011.

[14] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *2009 IEEE International Conference on Communications*, pp. 1–5, June 2009.

[15] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics," *IEEE Transactions on Wireless Communications*, vol. 9, pp. 3566–3577, November 2010.

[16] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pp. 1–5, Dec 2010.

[17] K. M. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2935–2939, May 2013.

[18] Mai Abdelhakim, Lei Zhang Jian and Ren Tongtong Li, "Cooperative sensing in cognitive networks under malicious attack," *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3004–3007, Sept. 2011.

[19] Mohammad Akbari and Abolfazl Falahati, "Ssdf protection in cooperative spectrum sensing employing a computational trust evaluation algorithm," *Telecommunications (IST), 2010*, pp. 23–28, Sept. 2010.

[20] Feng Zhu and Seung-Woo Seo, "Enhanced robust cooperative spectrum sensing in cognitive radio," *Journal of Communications and Networks (Volume: 11, Issue: 2)*, pp. 122–133, Sept. 2009.

[21] Shameek Bhattacharjee, Saptarshi Debroy and Mainak Chatterjee, "Trust computation through anomaly monitoring in distributed cognitive radio networks," *Journal of Communications and Networks (Volume: 11, Issue: 2)*, pp. 593–597, Sept. 2011.

[22] Boris Iglewicz and David C. Hoaglin, "How to detect and handle outliers: Vol 16," *The ASQC Basic References in Quality Control: Statistical Techniques*, Sept. 1997.

[23] L. Li, F. Li, and J. Zhu, "A method to defense against cooperative ssdf attacks in cognitive radio networks," in *2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013)*, pp. 1–6, Aug 2013.

[24] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, pp. 774–786, Feb 2011.

[25] Y. Han, Q. Chen, and J. X. Wang, "An enhanced d-s theory cooperative spectrum sensing algorithm against ssdf attack," in *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, May 2012.

[26] M. Akbari and A. Falahati, "Ssdf protection in cooperative spectrum sensing employing a computational trust evaluation algorithm," in *2010 5th International Symposium on Telecommunications*, pp. 23–28, Dec 2010.

[27] S. Althunibat, B. J. Denise, and F. Granelli, "Identification and punishment policies for spectrum sensing data falsification attackers using delivery-based assessment," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 7308–7321, Sept 2016.

[28] A. A. Sharifi and M. J. M. Niya, "Defense against ssdf attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach," *IEEE Communications Letters*, vol. 20, pp. 93–96, Jan 2016.

[29] F. R. Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *MILCOM 2009 - 2009 IEEE Military Communications Conference*, pp. 1–7, Oct 2009.

[30] Kanthakumar Pongaliur and Li Xiao, "Multi-fusion based distributed spectrum sensing against data falsification attacks and byzantine failures in cr-manet," *2014 IEEE*

22nd International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems, pp. 443–452, Sept. 2014.

[31] International Telecommunications union Report ITU-R SM.2152, "Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS) ," 2009.

[32] Nemanja Vucevic, Ian F. Akyildiz and Jordi Perez-Romero, "Dynamic Cooperation selection in cognitive radio networks," 2011.

[33] Khaled Ben Letaief and Wei Zhang, "Cooperative Communications for Cognitive Radio Networks," 2009.

[34] Bruce Fette, "Cognitive Radio Technology," 2006.

[35] Hüseyin Arrssllaann , "Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems," 2007.

[36] Khattab A. Perkins D. Bayoumi M., "Chapter 2 Cognitive Radio Networks from Theory to Practice," 2013.

[37] P.Kolodzy, "Proceedings of the Defense Advanced Research Projects Agency," 2001.

[38] Rehan Ahmed, Yasir Arfat Ghous, "Detection of vacant frequency bands in cogntive radio," 2010.

[39] Tevfik Yucek and Huseyin Arsla, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications ," 2009.

[40] Marija Matinmikko (editor), Marko Höyhtyä, Miia Mustonen, Heli Sarvanko, Atso Hekkala, Marcos Katz, Aarne Mämmelä, Markku Kiviranta, Aino Kautio, "Cognitive radio: An intelligent wireless communication system," 2008.

[41] I.F. Akyildiz, B.F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," Physical Communication, vol. 4 no. 1 pp. 40-62," 2011.

[42] A. Garhwal, and P. P. Bhattacharya, "A Survey on Dynamic Spectrum Access Techniques for Cognitive Radio," International Journal of Next-Generation Networks, vol. 3, no. 4, pp. 15-32,," September 2012.

[43] S. Ziafat, W. Ejaz, and H. Jamal, "Spectrum sensing techniques for cognitive radio networks: Performance analysis," 2011 IEEE MTT-S International Microwave Workshop Series on Intelligent Radio for Future Personal Terminals," 2011.

[44] S.Shobana, R.Saravanan and R.Muthaiah, "Matched Filter Based Spectrum Sensing on Cognitive Radio for OFDM WLANs," 2013.

[45] Pradeep Kumar Verma, Sachin Taluja and Rajeshwar Lal Dua, "Performance analysis of Energy detection, Matched filter detection and Cyclostationary feature detection Spectrum Sensing Techniques," 2013.

[46] D. Čabrić, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios, in Proceedings of Asilomar Conference 2004, pp. 772–776," November 2004.

[47] Tevfik Yucek and Huseyin Arslan, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications," 2014.

[48] S. Arkoulis L. Kazatzopoulos C. Delakouridis G.F. Marias, "Simulation framework for security threats in cognitive radio networks," 2011.

[49] O. ARVIDSSON and L. WALLGREN, "Q-learning for a simple board game," *Royal Institute of Technology School of Computer Science and Communication, Bachelor of Science Thesis Stockholm, Sweden*, 2010.

[50] Wireless-innovation, "Wireless innovation, software defined radio SDR[online]," 2012.

[51] Maksym Girnyk, "Cooperative Communication for Multi-User Cognitive Radio Networks," 2012.

[52] Kevin Chan, "Spectrum sensing, detection and optimization in cognitive radio for non-stationary primary user signals PDH thesis," 2012.

[53] R. S. Campos, "Evolution of positioning techniques in cellular networks, from 2g to 4g," *Wireless Communications and Mobile Computing*, pp. Article ID 2315036, 17 page, 2017.

[54] I. Amundson and X. D. Koutsoukos, "A survey on localization for mobile wireless sensor networks," in *Mobile Entity Localization and Tracking in GPS-less Environments* (R. Fuller and X. D. Koutsoukos, eds.), (Berlin, Heidelberg), pp. 235–254, Springer Berlin Heidelberg, 2009.

[55] L. Cheng, C. Wu, Y. Zhang, H. Wu, M. Li, and C. Maple, "A survey of localization in wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 8, no. 12, p. 962523, 2012.

[56] K. Tong, "Location estimation in wireless communication systems," *Electronic Thesis and Dissertation Repository. 3110.*, 2017.

[57] S. Ragan, "Raising awareness quickly: The ebay data breach."

[58] H. W. Kim and S. Lee, "Design and implementation of a private and public key crypto processor and its application to a security system," *IEEE Transactions on Consumer Electronics*, vol. 50, pp. 214–224, Feb 2004.

[59] M. Singh and D. Garg, "Choosing best hashing strategies and hash functions," in *2009 IEEE International Advance Computing Conference*, pp. 50–55, March 2009.

[60] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, pp. 54–62, Oct 2002.

[61] Wired, "GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED, url = https://www.wired.com/story/github-ddos-memcached/, urldate = 27-04-2018."

[62] F. Seco, A. R. Jimenez, C. Prieto, J. Roa, and K. Koutsou, "A survey of mathematical methods for indoor localization," in *2009 IEEE International Symposium on Intelligent Signal Processing*, pp. 9–14, Aug 2009.

[63] S. Maric, S. Reisenfeld, and L. Goratti, "A single iteration belief propagation algorithm to minimize the effects of primary user emulation attacks," in *2016 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, pp. 1–6, Oct 2016.

[64] S. Maric, S. Reisenfeld, and L. Goratti, "A simple and highly effective ssdf attacks mitigation method," in *2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–7, Dec 2016.

[65] K. C. Chilukuri and S. Devrapalli, "Common control channel design schemes in cognitive radio networks," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 11, pp. 962–969, 2016.

[66] M. Wannemacher and W. A. Halang, "Gps-based timing and clock synchronisation for real time computers," *Electronics Letters*, vol. 30, pp. 1653–1654, Sep 1994.

[67] P. L. Mothersole, "Time-base synchronization and associated problems," *Radio Engineers, Journal of the British Institution of*, vol. 20, pp. 57–72, January 1960.

[68] S. Maric and Reisenfeld, "Mitigation of primary user emulation attacks in cognitive radio networks using belief propagation," in *Cognitive Radio Oriented Wireless Networks*, (Cham), pp. 463–476, Springer International Publishing, 2015.

[69] J. S. Yedidia, W. T. Freeman, and Y. Weiss, "Understanding Belief Propagation and its Generalizations," in Exploring Artificial Intelligence in the New Millennium, Chap. 8, pp. 2282-2312, Science and Technology Books," 2003.

[70] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electronics Letters*, vol. 27, pp. 2145–2146, Nov 1991.

[71] Matthias Patzold, Nurilla Avazov and Van Due Nguyen, "Defense against primary user emulation attacks in cognitive radio networks," *The 2010 International Conference on Advanced Technologies for Communications*, vol. 26, pp. 112–117, Oct. 2010.

[72] A. Biswas, S. Reisenfeld, M. Hedley, and Z. Chen, "Effective sensor positioning to localize target transmitters in a cognitive radio network," *EAI Endorsed Transactions on Cognitive Communications*, vol. 16, 4 2016.

[73] I. Dokmanić, M. Kolundžija, and M. Vetterli, "Beyond moore-penrose: Sparse pseudoinverse," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 6526–6530, May 2013.

[74] T. Fawcett, "An introduction to {ROC} analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861 – 874, 2006. {ROC} Analysis in Pattern Recognition.

[75] R. Kumar and A. Indrayan, "Receiver operating characteristic (roc) curve for medical researchers," *Indian Pediatrics*, vol. 48, no. 4, pp. 277–287, 2011.

[76] K. Jaafar, N. Ismail, M. Tajjudin, R. Adnan, and M. H. F. Rahiman, "Z-score and feedforward neural network (ffnn) for flood modelling at kuala krai station," in *2016 7th IEEE Control and System Graduate Research Colloquium (ICSGRC)*, pp. 92–97, Aug 2016.

[77] Boris Iglewicz and David C. Hoaglin, "How to detect and handle outliers: Vol 16," *The ASQC Basic References in Quality Control: Statistical Techniques*, Sept. 1997.

[78] A. Goldsmith, "Wireless communications," 2008.

[79] S. M. Mahmoud, H. A. Alabbasi, and T. E. Abdulabbas, "Monitoring and detecting outliers for elder's life activities in a smart home: A case study," in *2017 E-Health and Bioengineering Conference (EHB)*, pp. 458–461, June 2017.

[80] "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497 – 1516, 2012.

[81] "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010.