Spring 2016

Heterogeneous Dynamic Spectrum Access in Cognitive Radio enabled Vehicular Networks Using Network Softwarization

Swetha R. Reddy

HETEROGENEOUS DYNAMIC SPECTRUM ACCESS IN COGNITIVE RADIO ENABLED VEHICULAR NETWORKS USING NETWORK SOFTWARIZATION

by

SWETHA REDDY

(Under the Direction of Danda B. Rawat)

ABSTRACT

Dynamic spectrum access (DSA) in cognitive radio networks (CRNs) is regarded as an emerging technology to solve the spectrum scarcity problem created by static spectrum allocation. In DSA, unlicensed users access idle channels opportunistically, without creating any harmful interference to licensed users. This method will also help to incorporate billions of wireless devices for different applications such as Internet-of-Things, cyber-physical systems, smart grids, etc. Vehicular networks for intelligent transportation cyber-physical systems is emerging concept to improve transportation security and reliability. IEEE 802.11p standard comprising of 7 channels is dedicated for vehicular communications. These channels could be highly congested and may not be able to provide reliable communications in urban areas. Thus, vehicular networks are expected to utilize heterogeneous wireless channels for reliable communications. In this thesis, real-time opportunistic spectrum access in cloud based cognitive radio network (ROAR) architecture is used for energy efficiency and dynamic spectrum access in vehicular networks where geolocation of vehicles is used to find idle channels. Furthermore, a three step mechanism to detect geolocation falsification attacks is presented. Performance is evaluated using simulation results.

INDEX WORDS: Cognitive Radio, Dynamic Spectrum Access, Vehicular Networks, Security, Software Defined Network, Cloud Computing.

HETEROGENEOUS DYNAMIC SPECTRUM ACCESS IN COGNITIVE RADIO ENABLED VEHICULAR NETWORKS USING NETWORK SOFTWARIZATION

by

SWETHA REDDY

B.S., Jawaharlal Nehru Technological University, India, 2014

A Thesis Submitted to the Graduate Faculty of Georgia Southern University in Partial Fulfillment

of the Requirement for the Degree

MASTER OF SCIENCE

STATESBORO, GEORGIA

HETEROGENEOUS DYNAMIC SPECTRUM ACCESS IN COGNITIVE RADIO ENABLED VEHICULAR NETWORKS USING NETWORK SOFTWARIZATION

by

SWETHA REDDY

Major Professor: Danda B. Rawat

Committee:

Mohammad Ahad

Fernando Rios-Gutierrez

Electronic Version Approved:

May 2016

DEDICATION

To my beloved family

ACKNOWLEDGMENTS

This work would not be done very efficiently without the support of all the remarkable individuals who I would like to acknowledge.

Firstly, I would like to express my deepest gratitude and honor to my research advisor Dr. Danda B. Rawat, director of CWINs Lab. Dr. Rawat has been highly supportive and encouraging during all the time of my thesis and provided me with ample opportunities to learn and develop my skills. I heartfully thank him for providing me an opportunity to be a part of CWINs Lab.

I would like to thank Dr. Mohammad Ahad and Dr. Fernando Rios-Gutierrez for their valuable suggestions which helped to improve my thesis.

I owe a special thanks to my colleagues and friends especially Nimish Sharma, Robin Grodi, Tanjil Amin and Chetan Ranade for providing their motivation and support since the first day of my journey at CWINs.

I would also like to thank the U.S. National Science Foundation (NSF) and Georgia Southern university for financially supporting my research. However, any opinion, finding, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NSF or Georgia Southern University.

TABLE OF CONTENTS

Page

DEDICATION 2

ACKNOWLEDGMENTS 3

LIST OF FIGURES 7

CHAPTER

1 INTRODUCTION 10

1.1 Vehicular Networks 11

1.2 Cognitive Radio and Dynamic Spectrum Access 14

1.3 Cloud Assisted Cognitive Radio Networks 17

1.4 Network Softwarization 18

1.5 Problem Statement 19

1.6 System Model 20

1.6.1 Physical Layer 20

1.6.2 Control Layer 20

1.6.3 User Layer 22

1.7 Outline of the Thesis 22

2 CLOUD ASSISTED COGNITIVE RADIO VEHICULAR NETWORKS 24

2.1 Related Work 24

2.2 System Model 27

2.3 Cloud Computing for Spectrum Processing and Heat Map . . . 29

2.4 Transmission Power vs. Range in CR Vehicular Network 30

2.5 Adaptive Channel Assignment And Communications In CR Vehicular Network 31

2.6 Simulation And Numerical Results 34

2.7 Chapter Summary 44

3 SECURING REAL-TIME SPECTRUM ACCESS IN COGNITIVE RADIO VEHICULAR NETWORKS AGAINST LOCATION FALSIFICATION ATTACKS 45

3.1 Related Work 46

3.1.1 GPS Vulnerabilities 46

3.1.2 Angle of Arrival Methods 47

3.2 System Model 49

3.2.1 Attack Model 50

3.2.2 Angle of Arrival 52

3.2.3 Received Signal Strength 54

3.2.4 Time of Arrival 54

3.2.5 Measurement errors in GPS 55

Probability of Misdetection 55

Probability of False Alarm 56

3.3 The Algorithm 58

3.4 Numerical Results and Analysis 60

3.5 Chapter Summary 71

4 OPTIMIZATION OF ENERGY EFFICIENCY USING NETWORK SOFTWARIZATION 73

4.1 Related Work 74
4.1.1 History 74
4.1.2 Architecture of SDN 75
Control Layer 75
Infrastructure Layer 76
Application layer 76
Interfaces 76
4.1.3 Energy Efficient Methods in SDN 77
Traffic Engineering 77
Rule Placement 77
Traffic monitoring 77
4.2 System Model 78
4.3 Simulation And Numerical Results 81
4.4 Chapter Summary 86
5 CONCLUSIONS, DISCUSSIONS AND FUTURE WORK 88
5.1 Future Work 89
REFERENCES 91

LIST OF FIGURES

Figure Page

1.1 Vehicle-to-Vehicle Communications (V2V) 11

1.2 Vehicle-to-Roadside Communications (V2R) 12

1.3 IEEE 802.11p WAVE Standard [1] 13

1.4 Dynamic Spectrum Access [2] 15

1.5 Cognitive Cycle 16

1.6 Overall System Model 21

2.1 System model for cloud-assisted GPS-driven dynamic spectrum access in cognitive radio enabled vehicular networks where roadside Wi-Fi users are treated as PUs 27

2.2 Distributed Remote Procedure Call (RPC) Work-flow. 29

2.3 Storm Topology for Real-time Processing in Cloud Computing Platform and Generating Spectrum Heat Map Framework. 30

2.4 Sample scenarios ($SC1$, $SC2$ and $SC3$) for available networks with their data rates (Mbps) for DSRC (802.11p) only and for CR networks (with DSRC and Wi-Fi 802.11a/b g/n) versus the time instances. 35

2.5 Variation of achievable rate in a channel n for variable probability P_{S1} (i.e., the probability of PUs being active in the given channel) for given data rate. 36

2.6 Variation of rates in a channel n for each CR enabled vehicular users for variable number of CR enabled vehicular users (N_n) and data rates (R_a) when $P_{S1} = 0.5$ 37

2.7 Variation of expected transmission count for different failure probability (p_f) values for a given channel. 38

2.8 Variation of expected transmission time (TT) vs. transmission count (TC) for transmission failure probability value p_f = 0, 0.1, 0.2, ..., 0.9, data rate R_a = 11 Mbps, and data size D = 100 KB 39

2.9 Variation of expected transmission time vs. variable data size for different transmission rates and probability of failure pf when probability of PUs being active P_{S1} = 0.5. 40

2.10 Variation of expected transmission time vs. variable data rate for different transmission rates and probability of failure pf when probability of PUs being active P_{S1} = 0.5. 41

3.1 A typical system model for securing opportunistic spectrum access in cognitive radio networks with Storm model for real-time parallel processing. 49

3.2 Attack Model 1 (Case I) 50

3.3 Attack Model 2 (Case II) 51

3.4 Uniform linear array for measuring angle-of-arrival for M number of antennas separated each by distance d and the signal incident angle θ. 52

3.5 Probability of Misdetection. 56

3.6 Probability of False Alarm. 57

3.7 The angle estimated at antenna array does not match with the angle based on geolocation coordinate in **Scenario 1** 61

3.8 Variation of angle spectrum, received signal strength and time of arrival for malicious user for **Scenario 2** 62

3.9 Variation of angle spectrum, received signal strength and time-of-arrival for a malicious secondary user for **Scenario 3**. 63

3.10 Variation of angle spectrum, received signal strength and time-of-arrival for a legitimate secondary user for **Scenario 4**. 64

3.11 Mobile transceivers (i.e., secondary users) and no. of available channels shown to secondary users for a given location and time for **Scenarios 1 – 4**. Only scenario 4 (legitimate one) has a list of channels for the secondary users but other scenarios (with fake locations) have 0 channels for the users. 67

3.12 Probability Of Misdetection in Cloud Assisted Cognitive Radio Networks when the Tolerance is ranging from 0 to 2 68

3.13 Probability Of False Alarm in Cloud Assisted Cognitive Radio Networks when the Tolerance is ranging from 0 to 10 69

4.1 Architecture of SDN 75

4.2 Typical System Model for Network Softwarization. 79

4.3 Conventional Network Power Consumption vs Software Defined Network Power Consumption 82

4.4 Total Power Consumption at BS_1 with varying number of SUs. 83

4.5 Total Power Consumption (P_t) vs Number of Users (L). 84

4.6 Total power consumed at all the BSs with varying load percentages . . . 85

CHAPTER 1

INTRODUCTION

In 2016, the National Highway Traffic Safety Administration (NHTSA) released a report on the number of deaths and injuries caused by vehicle crashes every year. The report showed that there were approximately 32,000 fatalities and 2.3 million injuries caused by accidents. Further, the percentage of fatalities rose by 9.3 % from 2014 to 2015 and the average economic burden due to accidents totaled 230.6 billion per year [3] [4] [5]. It is also estimated that about 95% of accidents are caused due to the human errors. The main reason behind more than half of these accidents caused by humans is due to lack of decision making abilities [6]. For instance, vehicle crashes are mostly involved with teen drivers with less experience and senior citizens with low reaction time [7]. Therefore, based on the information listed above vehicle accidents are becoming a bigger problem.

To overcome this problem, most newer vehicles are being embedded with advanced features such as auto brake and blind spot detection [8]. Though, these features were capable of avoiding crashes to some extent they did not significantly lower the collision percentages. To aid with this many research groups are focusing on the design of autonomous vehicles that require no assistance from drivers. One of the most popular example of autonomous cars is Google's self-driving car which uses cameras, sensors and radars to avoid crashes and reach the destination safely [9]. Although it may be true that autonomous vehicles can eliminate the vehicle crashes caused by human errors, it still has its own limitations. For example, autonomous vehicles are entirely dependent on GPS for driving, if the signal reception is low it can hinder the functionality of the car [10]. It is still important to have the role of humans in driving to avoid these circumstances. Additionally, providing the drivers with information regarding their surroundings can increase their ability to take rightful decisions to avoid crashes. Although drivers can be alerted with the information regarding the accidents using FM radio and display boards on the road, this process is not automatic

and timely. All these factors have raised interest in vehicular communication [11] [12] [13].

1.1 Vehicular Networks

In many developed countries such as the U.S., Japan and Europe, Intelligent Transportation Systems (ITS) is a growing area of research for developing road safety applications. Among the multiple disciplines of ITS, vehicular networks is a promising area of interest to improve road safety. In vehicular networks communication can be done using Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) [14] [15] [16].

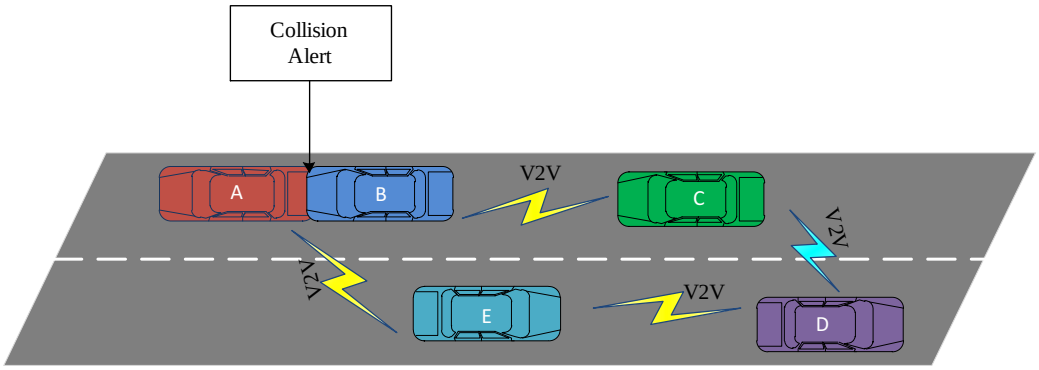


Figure 1.1: Vehicle-to-Vehicle Communications (V2V)

In V2V communications, all the vehicles located in a certain area communicate with each other and exchange information regarding road conditions, as shown in Figure 1.1. In Figure 1.1, all the vehicles are communicating with each other using a single hop or multiple hops. For instance, the vehicles A and B ended up in a collision and the vehicle D is being updated about the collision. It receives the information with two hops from vehicle B to vehicle C and vehicle C to vehicle D, or from vehicle B to vehicle E and vehicle E to vehicle D.

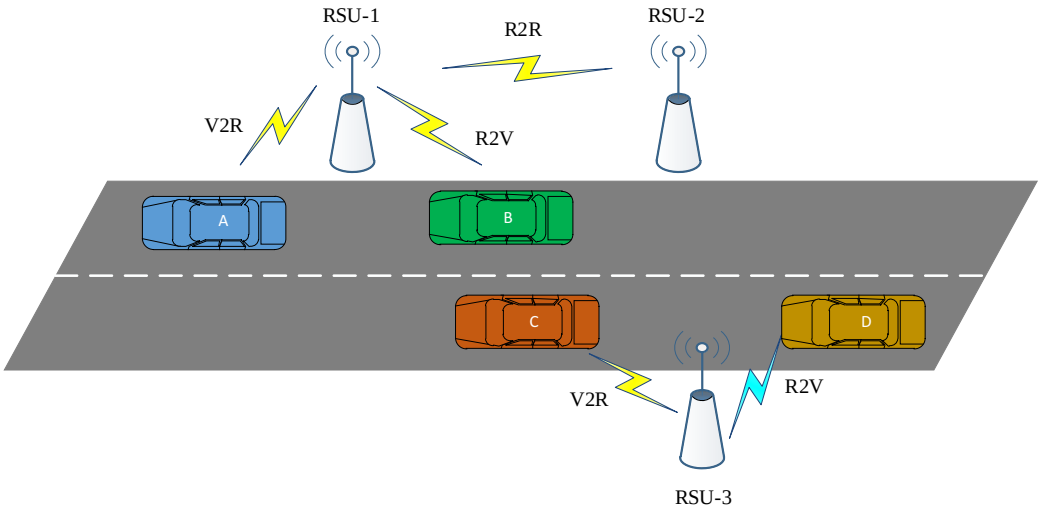


Figure 1.2: Vehicle-to-Roadside Communications (V2R)

In V2R, vehicles communicate with the infrastructures such as base stations and road side units (RSU), etc, [17] [15]. This type of communication is further divided into Vehicle-to-Roadside (V2R), Roadside-to-Vehicle (R2V) and Roadside-to-Roadside (R2R) as shown in the Figure 1.2. For instance, vehicle A reports the information to RSU-1 using V2R communication. The RSU-1 sends the information to vehicle B and RSU-2 using R2V and R2R communications respectively.

There are endless opportunities that can be achieved through the use of vehicular communications including assisting to avoid all types of collisions that could occur during intersections, lane changes and overtaking other vehicles. This type of communication can also alert the drivers by providing them with information regarding accidents, vehicle breakdowns, high traffic roads and bad weather conditions. Based on the information obtained, the user can avoid routes with high traffic and choose an alternative route to reach the destination safely [17] [15]. However, vehicular networks still face a large number of challenges that need to be addressed.

First, there is a tradeoff between the security and privacy in vehicular networks. In order to trust the users reported information the identity of the user must be known thereby compromising privacy. If there is no proper mechanism to verify the integrity of information obtained from other users, the entire network becomes vulnerable to fabrication attacks [18] [19].

Next, vehicular networks have to depend on some type of communication mechanism to exchange information. Moreover, while adopting the means of communication for vehicular networks features such as the ability to adapt to rapidly changing environments should be considered. Since, the communication in wireless systems is carried out by radio technology, it is considered more suitable for dynamic environments due to the lack of physical connections [20] [21]. With that knowledge, Federal Communications Commission (FCC) dedicated IEEE 802.11p Wireless Access in Vehicular Environment (WAVE) standard for vehicular communications. IEEE 802.11 p standard is shown in the Figure 1.3 comprises of 7 channels with equal bandwidth of 10 MHz. In the Figure 1.3, the channel 178 located between 5885 GHz and 5895 GHz is regarded as the control channel. The channels 172 and 184 are allocated for life safety and public safety applications while, the remaining channels are used as service channels [1] [22].

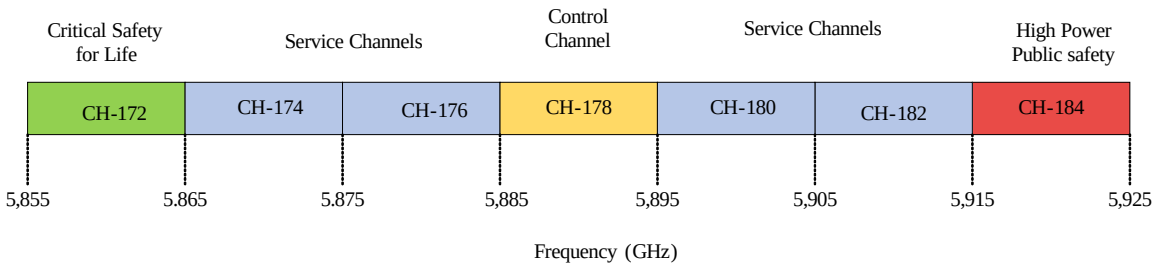


Figure 1.3: IEEE 802.11p WAVE Standard [1]

The major limitation of this standard is that it does not perform efficiently in urban areas where the vehicle density is relatively high. These 7 channels could be overcrowded

which results in the vehicular users experiencing a delay in receiving and transmitting messages thus degrading the Quality of Service (QoS) of the entire system. The problem described is not limited to vehicular networks but also persistent in other communication technologies such as cellular and Wi-Fi. The reports from cisco estimate upto 55% growth in mobile traffic by the end of 2020 [23]. The current static allocation of spectrum bands for wireless communications is inadequate to satisfy the requirements of growing traffic. On the other hand, significantly large portions of spectrum bands reserved for military, public safety and government bodies remain underutilized. The static spectrum allocation is the root cause for this problem but was originally created in 1920 to avoid interference to the primary users and provide them with high QoS [24]. While it did prevent interference for licensed users it has led to inefficient utilization of spectrum resources.

1.2 Cognitive Radio and Dynamic Spectrum Access

The concept of cognitive radio was developed by Dr. Joseph Mitola III in 1999 to resolve the problem of spectrum scarcity occurring due to underutilization of spectrum resources. Cognitive Radio (CR) is regarded as smart radio technology that can have knowledge about wireless spectrum utilization and adapts itself to change in the spectrum environment [25].

Dynamic spectrum access (DSA) is an emerging technology in CR that enables the efficient use of the spectrum resources. DSA can be used in the vehicular networks for overcoming the problem of spectrum scarcity and achieving uninterrupted communication between the vehicles [12]. This technology mainly comprises of two users i.e, primary users and secondary users (i.e, vehicular CR user in this case). Primary Users (PU) are the licensed users that are given high priority when accessing the allocated bands. Hence, the PU in the channel obtains high QoS compared to other CR users. While, secondary Users (SU) are unlicensed users having low priority over the PU. They are allowed to access the idle channels in the spectrum without creating interference to the PUs. Figure 1.4 depicts

the typical scenario of DSA comprising of PUs and SUs. From the Figure 1.4, the darker color blocks (i.e, grey blocks) are the frequency bands that are occupied by the primary users. The idle channels available are represented using lighter color blocks (i.e, orange blocks). The arrows indicates the SU users hopping from one channel to other in order to avoid interference for primary user.

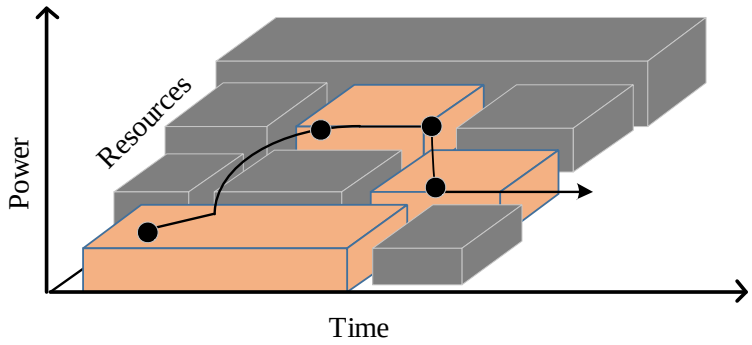


Figure 1.4: Dynamic Spectrum Access [2]

The three widely used techniques in DSA are interweave, spectrum underlay and spectrum overlay [26]. Interweave is the standardized method where PU gets the highest priority in the spectrum bands and SU will not be permitted to use the channel in the presence of PU. It is a suitable technique to avoid interference to the PU and helps to achieve high QoS. In underlay technique, the SU are allowed to share the spectrum with PU only if the interference caused is below the certain threshold value. Further, the overlay technique also permits the simultaneous sharing of spectrum between PU and SU. However, when the PU is transmitting in the channel, the SU has to add half of its transmit power to PU transmission. This will boost the performance achieved by PU. The four stages of cognitive cycle used in DSA shown in Figure 1.5 is generalized as follows:

Sensing Phase: In this stage, SU periodically scans the spectrum to search the available channels. Spectrum scanning is divided into two sensing techniques i.e, local sensing and cooperative sensing [26].

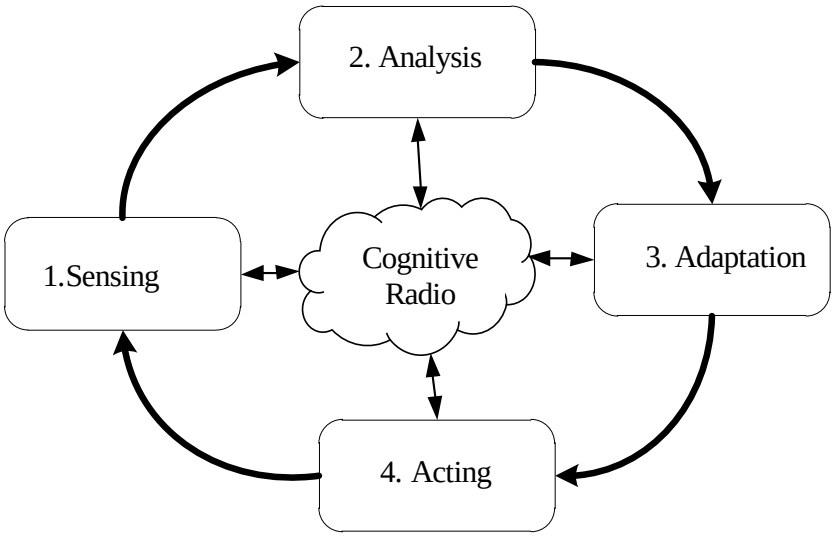


Figure 1.5: Cognitive Cycle

In local sensing, the user scans the entire spectrum individually to find the idle channels. Energy detection, matched filter detection and cyclostationary detection are the examples of local sensing. In energy sensing, the PU is assumed to be present in the channel if the received signal strength exceeds a certain threshold value. Whereas, the matched filter method uses prior information available to identify the presence of PU. The main drawback of the energy detection and matched filter detection is noise. On the other hand, the cyclostationary detection method is capable of overcoming this drawback as it uses the periodicity of the signal for detecting the PU.

In cooperative sensing, group of users scan the spectrum for the idle channels and share the information among themselves. It is classified into two different categories i.e, centralized approach and decentralized approach. In centralized approach one node acts as a controller and collects the information from all the users and allocates them with suitable channels. Whereas, in decentralized mode the SU gets to choose his own channel based on the information obtained. The cooperative sensing technique has many advantages such as accuracy, reduction in hidden node problem and false alarms.

Analysis Phase: In this stage, a suitable channel among the list of available channels is analyzed to meet the requirement criteria of SU. It helps to improve the QoS obtained by the SU and also avoid interference to the PU. The analysis of the suitable channel can be done individually or by using a fusion center. In individual analysis only the user is responsible for making the decision about channel selection. Whereas, in fusion center analysis, a centralized controller is responsible for allocating the suitable channels to the users.

Adaptation Phase: The adaptation stage is the switching phase in which SU adapts to transmission power, channel, data rate and modulation based on the analysis done in the previous stage. If the channel requested by the SU is unavailable at that point of time, spectrum mobility management is the special feature that supports dynamic spectrum access and allocates it to SU when the channel becomes available. Spectrum sharing is also an important feature of the adaptation stage where the spectrum resources are shared among all the available users.

Acting Phase: In this stage, the SU considers all the adapted features from the previous stage and communicates with the other SUs. This process is repeated to avoid interference to the primary users.

1.3 Cloud Assisted Cognitive Radio Networks

Although, spectrum sensing is popular method for finding the idle channels, it has several limitations that can affect the overall performance of SU. In spectrum sensing, SU has to continuously scan the entire spectrum to obtain the idle channels. However, SUs might not possess the ability to scan the entire spectrum of frequencies due to the lack of high end antennas with sufficient power. The SUs also have limited computational capacity as a result of which they will experience a delay in calculating the suitable channel. Moreover, while scanning the spectrum and using the idle channels SU might create interference to the

PU. For instance, 800 MHz frequency is allocated for public safety communications [7]. If the SUs use the idle channels operating at 800 MHz, they create interference and clog the channels making them unusable for emergency operations. Security is also a prime concern in spectrum sensing as it is highly prone to emulation attacks, where the attackers behave as PUs and prevent the legitimate SU from using the channels.

All these limitations of spectrum sensing motivated the FCC to mandate the use of geolocation database technique for idle channel selection [27]. The geolocation database consists of location (longitude, latitude, altitude) of idle bands and time; this information can be received/updated periodically either from primary infrastructures (such as base station in cellular networks, access points in Wi-Fi, etc.) or from dedicated spectrum sensors deployed in a distributed manner to report channel occupancy information. Then, the geolocation database of idle channels is queried by the secondary users to find the idle channels at given location and time for opportunistic communications [28, 29] [30]. Additionally, the geolocation database has to process a vast amount of idle channels and requires a platform that can handle the process without any latency. Under those circumstances, the cloud computing is the viable option as it is capable of delivering huge computational capacity. The cloud computing platform is used to find whether there is match between the location of idle bands with the location of secondary user for a given time [28, 29, 31]. If the secondary users are located within the contour of idle bands, secondary user receives a list of channels and chooses the best channel that meets its QoS requirements to communicate with its receiver opportunistically [30].

1.4 Network Softwarization

Despite of the numerous advantages delivered by cloud based cognitive radio networks (CRN), there is always a trade-off between the performance and the cost. For instance, the cloud based CRN requires enormous resources to provide the users with idle channels which

increases the complexity and energy consumed, thereby increasing the cost. Implementing smart network management for monitoring and controlling the network traffic is a reliable way to reduce the power consumption. However, conventional networking architectures used in cloud based CRN are closed systems and do not support any modifications to the architecture. Additionally, the decentralized structure of conventional networks make it even more difficult to track all the network activities [32] [33]. Alternatively, usage of software for controlling the network operations can reduce the complexity and overall cost of the system. Managing the functionality of the network using software is termed as softwarization of network. Flexible architectures such as SDN with decoupled data plane and control plane can be implemented for softwarization of network. This method helps to achieve easy manageability, high flexibility, programmability and energy efficiency in cloud based CRN [34].

1.5 Problem Statement

The main objectives of this thesis are:

- To design an efficient framework for enabling the dynamic spectrum access for cloud based cognitive radio vehicular users.
- To secure the dynamic spectrum access in cognitive radio networks from the location falsification attacks caused due to vulnerabilities in GPS.
- To reduce the probability of misdetection and probability of false alarm caused due to measurement errors in GPS thereby improving overall performance and efficiency.
- To design the softwarization architecture to achieve energy efficiency in the system.

1.6 System Model

The complete system model for the thesis is represented in Figure. 1.6. Since, the system is managed using SDN it is decoupled into three different layers i.e, physical layer, control layer and user layer.

1.6.1 Physical Layer

The first layer in the system is known as physical layer. It comprises of all the primary wireless infrastructures such as cellular, Wi-Fi, TV, Wi-MAX and satellite. It is assumed that, all these infrastructures are aware of PU state in the channel and take the responsibility of reporting the database with idle channel information.

1.6.2 Control Layer

The control layer is considered the backbone of entire network as it comprises of the logically centralized controller that is responsible for managing the tasks of the entire system. To handle the tasks efficiently without any delay, a high computational capacity is required. Therefore, storm topology based distributed cloud computing is used in the system. Storm topology platform is selected over other cloud computing platforms because it is capable of supporting the real time processing. The three prominent tasks in control layer are summarized as follows:

1. **Processing the idle channels**: The idle channels obtained from primary infrastructures are processed by using storm topology. The storm topology comprises of multiple bolts for handling different tasks. The channels obtained from various wireless infrastructures are processed by separate bolts. For instance, bolt1 processes Wi-Fi channels and bolt 2 handles cellular channels. This method decreases the overall processing time.

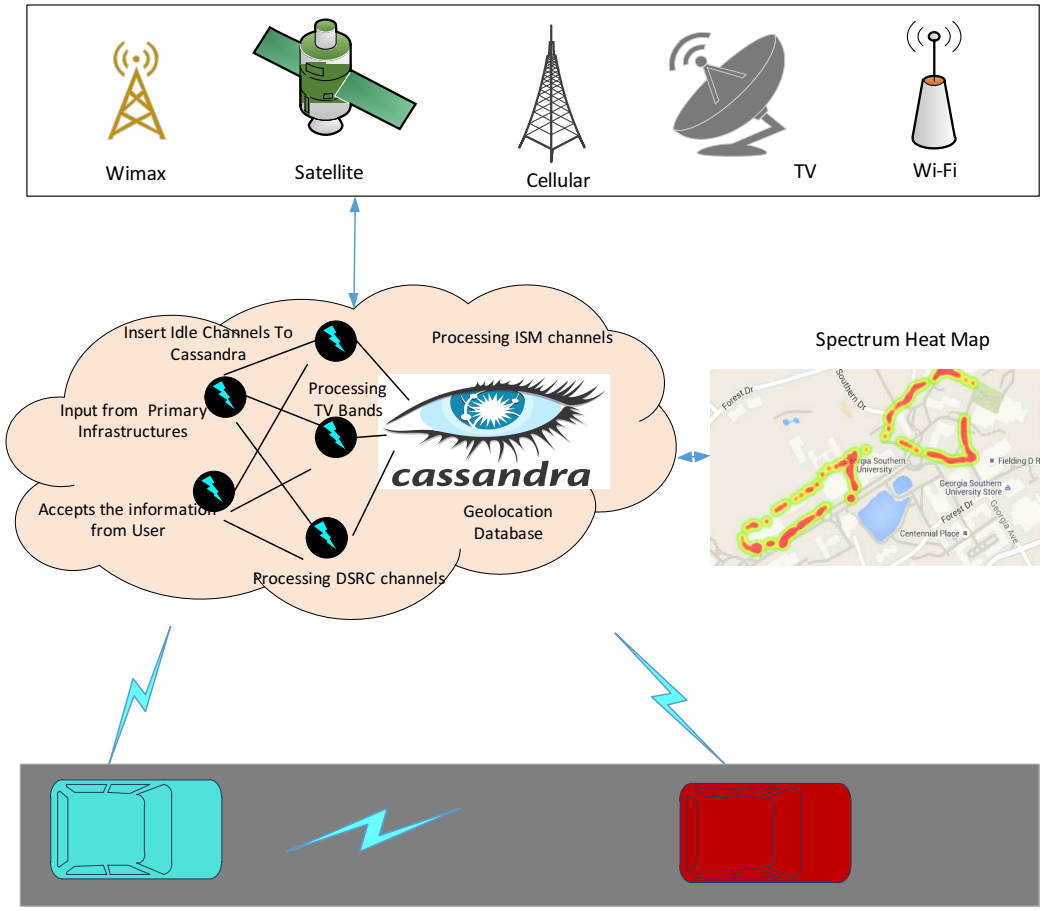


Figure 1.6: Overall System Model

2. **Network Softwarization**: All the idle channel reported by the primary infrastructures is combined into a single virtual resource using SDN. SDN is also responsible for determining the functionality of these primary infrastructures (i.e, BSs). If the CR enabled vehicular user wants to access any primary infrastructure, user sends the request to the database. The database allocates the idle channels from the virtual instances of primary infrastructures present in cloud. The primary infrastructures that remain unused by the SUs are powered off by the SDN controller to optimize the energy efficiency.

3. **Storing the idle channels**: Cassandra database is opted for storing the idle channels because it can deliver benefits such as high availability, performance and quick insertion of data. Moreover, these idle channel information stored in the cassandra database is updated continuously to avoid any interference to the PUs.

4. **Spectrum Heat Map**: To clearly visualize the available channels in a particular geolocation, the heat map is designed using Google API. The idle channel information updated in the database is automatically plotted on the map [35], [28].

1.6.3 User Layer

Finally, the SU's (i.e, vehicular CR user in our case) are present in the user layer and query the database by reporting their exact location. Based on the reported location, the CR enabled vehicular user are allocated idle channels for communicating with other vehicular users. Moreover, to protect the system from location falsification attacks, the legitimacy of the user is verified before allocating any idle channels.

1.7 Outline of the Thesis

Chapter 2 discusses a cloud-assisted GPS driven frame work for enabling dynamic spectrum access in vehicular networks. In this framework, each vehicle is comprised of a GPS unit and two transceivers. Using this equipment, the vehicular CR user queries the spectrum database periodically and finds the idle channels to use for communication. The chapter also investigates the impact of PU activities on spectrum database using simulations.

Chapter 3 presents the framework for securing the dynamic spectrum access of CR users from location falsification attacks. This chapter also investigates the probability of misdetection and probability of false alarm scenarios occurring in the system due to measurement errors in GPS. All the techniques presented in the system are evaluated using

simulations.

Chapter 4 presents the system model for network softwarization to improve the energy efficiency of the entire system. Further, the power consumption of SDN based system at various scenarios is evaluated using simulations.

Chapter 5 provides discussion of results from the previous chapters and also presents a final conclusion to the thesis along with recommendations on future research.

The part of research results from chapter 2 is published in 2015 IEEE Wireless Communications and Networking Conference (IEEE WCNC) held at new orleans, LA on March 9-12, 2015 [36]. The part of research results from chapter 2 is published in 2015 IEEE Global Communication Conference workshop on Security, Privacy, and Forensics in Wireless Mobile Ad Hoc Networks and Wireless Sensor Networks (IEEE Globecomm SPFMSNET) held at san diego, CA on Dec 6-10, 2015 [30]. The part of the research results from chapter 3 are under review in International Journal of Monitoring and Surveillance Technologies Research (IJMSTR) [37]. The part of the research results from chapter 4 is published in 2016 IEEE South East Conference (IEEE Southeastcon) to be held in norfolk,VA from 30 March - 03 April, 2016 [34].

CHAPTER 2

CLOUD ASSISTED COGNITIVE RADIO VEHICULAR NETWORKS

In this chapter, a cloud-assisted GPS-driven dynamic spectrum access for transportation cyber-physical systems (CPS) is presented where each vehicle is assumed to be equipped with (i) A GPS unit to find best route for the specified destination address and (ii) two coordinated transceivers: one is always connected to cloud (e.g. using 3G/4G link) to query spectrum database to find idle channels and the other one is used for actual communications (using for instance 802.11p 5.9 GHz bands, ISM 2.4GHz/5GHz bands).

First, each CR enabled vehicular user finds its best route based on its destination address using GPS. Then, the path computed using GPS is used to query the spectrum database by the CR enabled vehicular user for an idle channel set throughout the given route for communications. Furthermore, CR enabled vehicular users query the spectrum database periodically for updated information about spectrum opportunities so as not to harm any PU transmissions. Note that, when the previously found idle channel is not going to be idle anymore (based on the latest query result) by the time CR enabled vehicular user gets to the given location, the CR enabled vehicular user switches to new channel based on the latest response received from spectrum database [36].

The remainder of the chapter is organized as follows: The related work is discussed in Section 2.1. The system model for dynamic spectrum access in vehicular networks is presented in Section 2.2 and adaptive channel assignment for communication is discussed Section 2.5. Numerical results obtained from simulations are presented in Section 2.6. Finally, conclusions are presented in Section 2.7.

2.1 Related Work

Recent works in cloud assisted cognitive radio networks are discussed in [28] [38] [39]. A framework for cloud based cognitive radio networks was proposed in [28], where the authors

analyzed the spectrum overlay scenario in which PU and SU share same frequency band. In this system, authors use a storm topology based distributed cloud computing platform for allocating the spectrum resources efficiently. The spectrum sensors deployed in the primary infrastructures report the idle channel information. This reported information is processed by using storm topology bolts and stored in the dynamic hash table of cassandra database. All the reported locations have a time frame value indicating when the channel can be used by the SU. Moreover, when the channel is busy, the time frame value immediately updates itself to zero and information will be removed from the idle channel list. For accessing the idle channels, SU reports the current location (x_1, y_1, z_1) and queries the database to find the available channels (i.e, idle channels) in the reported location. The suitable channels are allocated by matching the reported location with the location of idle channels available in hash table. The list of available channels will be shortlisted based on the priorities mentioned by SU such as data rate. The distance between the SU reported location (x_1, y_1, z_1) and idle channel location (x_2, y_2, z_2) is calculated for determining the suitable channel.

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2} \tag{2.1}$$

If the obtained distance is below the certain tolerance, then the channel will be allocated to SU. In [38] [39] authors focus mostly on allocation of resources to unlicensed secondary users based on the revenue gained by spectrum providers.

The framework of geolocation database implemented in the thesis was borrowed from these papers. However, this thesis mainly focus on implementing geolocation based cognitive radio network for communication of vehicular networks.

The related works based on enhancing the performance of vehicular communications are discussed in [13] [11] [40] [41] [42] [43]. Authors in [13] proposed a system model to improve the connectivity of VANETS (Vehicular Ad-Hoc Networks) in both one way and two way traffic conditions. They also discussed the dynamic channel selection technique in

vehicular network to maximize the overall throughput. The authors in [11] also focused on providing high QoS to CR enabled vehicular users by calculating the best routing path with less delay using the relative velocity vectors.

Authors in [41] and [42] discusses a mechanism to enhance the performance by adjusting the power and contention window dynamically based on the surroundings. Authors in [43] proposes a game theoretic approach for selecting the most suitable channel with high data rate for vehicular communication.

The related works for dynamic spectrum access of vehicular networks is discussed in [44] [45] [40]. Authors in [44] analyzed a method to use the idle channels in highways for enabling DSA in vehicular networks. They opted machine learning techniques and designed a sophisticated mechanism that do not violate any FCC mandated rules and finds the suitable channel for vehicular communication.

Authors in [45] also discussed methods to use the white spaces in TV bands ideally for the communication of high speed vehicles. This system comprises of two important modules i.e, cognitive base station and access controller. The cognitive base station gathers the information about the white spaces in the spectrum and stores it in spectrum database. On the other hand, access controller allocates these idle channels to the high speed vehicular network based on the requirement. The system also uses a most stable channel for communication to obtain high QoS. The stable channel is selected by using the slot based hand off mechanism, where the route of travel is divided into equally spaced cells and the channel commonly available in all the cells is assumed to be stable and secure.

Authors in [40] discuss about the use of spectrum databases for establishing communication between the vehicles. The work mainly focused on designing a cost efficient architecture that does not compromise on the QoS provided to the users. In this system model, the authors considered that fixed base stations are installed at different locations according to the user density. These base stations are used for providing the DSA for

vehicles. Additionally, all the vehicles are embedded with certain features such as GPS, 3G connectivity for querying the database and sensing capabilities. The vehicles having the 3G connectivity obtain channels through querying. Whereas, few vehicles who lack this ability depend on other vehicles with querying capability or use sensing techniques to find idle channels.

However, none of these works available in the literature consider joint use of route determined by the GPS for a given destination to find spectrum opportunities, the impact of PUs ON/OFF activities along the route and spectrum query interval.

2.2 System Model

Typical system model discussed in this chapter is shown in Figure 2.1. Here, the system considers that the CR enabled vehicular users access different wireless channels of different networks (e.g., 802.11p, 802.11b/g, etc.) for communications and use GPS device to find the best route for a given destination.

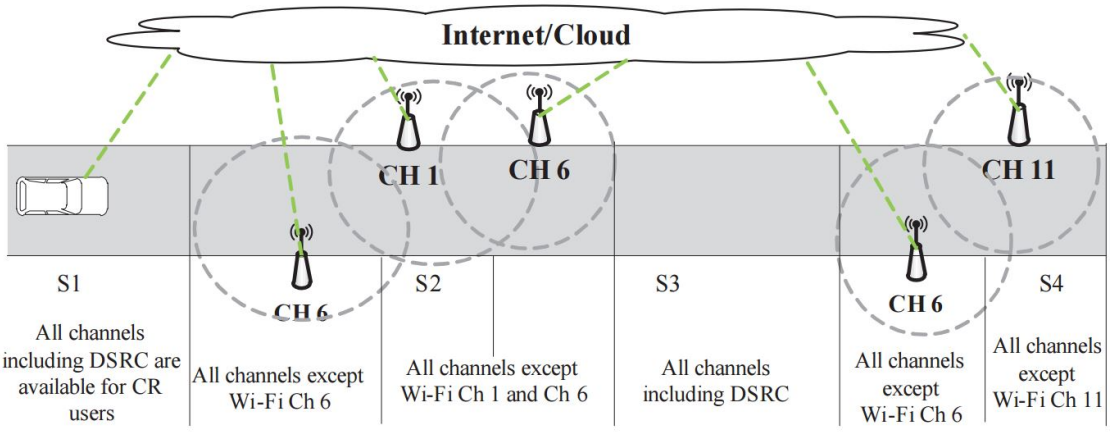


Figure 2.1: System model for cloud-assisted GPS-driven dynamic spectrum access in cognitive radio enabled vehicular networks where roadside Wi-Fi users are treated as PUs

Each vehicle is assumed to be equipped with 2 transceivers/radios: Radio 1 for searching spectrum opportunities and the other one (Radio 2) for actual communications which uses opportunistic spectrum access. Radio 1 is assumed to be always connected to the internet cloud through 3G/4G link so that it can query the spectrum database whenever needed or could serve as a GPS through an app (especially when actual GPS device cannot function in urban areas). Note that each CR enabled vehicular user can have same or different querying range and transmission range. It is considered that infrastructures of primary networks reports their channel occupancy information to cloud server where spectrum database is created using distributed cloud computing as shown in Figure 2.2 and Figure 2.3.

When a vehicle leaves for a given destination, the GPS device (or Radio 1 connected through 4G link with the help of GPS app) is responsible for calculating the best route for it. This route information is used by the Radio 1 to search for spectrum opportunities along the route from vehicle's current position to its destination and provides a set of recommended channels to be used throughout the route. Then, CR enabled vehicular user periodically checks the database for updated channel information to avoid any harmful interference to PUs. For instance, when a CR enabled vehicular user queries the database based on the route calculated by GPS as shown in Figure 2.1, it observes that the vehicle cannot use Wi-Fi channels 1 and 6 in a road segment S2, and channels 6 and 11 in road segment S3 to avoid PUs (here residential Wi-Fi users are assumed to be PUs). Vehicles could use any channels including DSRC in segments S1 and S3. However, when a vehicle is about to enter the segment S3 it checks (as a periodic process) whether any PUs are popping up in the upcoming segment. If there is any PU using any channel (say channel 11), then CR enabled vehicular users would not be able to use that channel in the segment (where the channel is actively used by PUs).

2.3 Cloud Computing for Spectrum Processing and Heat Map

In order to process huge amount of data about spectrum occupancy information obtained from infrastructure of primary networks for different channels, there is a need for cloud based computing and storage resources for the purpose of distributed storage and distributed computation. Furthermore, to provide overall heat-map for different bands and spectrum access technology as a service for CR enabled vehicular users, cloud computing and storage are crucial. Similar to different cloud services, the cloud integration allows our technology to be adopted as a service. Moreover, in our approach, there is a need for real-time processing of spectrum occupancy information, for updating the Cassandra database and for querying the database. The algorithm is implemented in the Storm system, a real-time processing system, which is also currently used by Twitter to process trending topics. For cloud computing, among Riak [46], Cassandra [47] and Memcached [48], Cassandra was chosen due to its proven robustness, real-time performance and commercial adoption by Twitter.

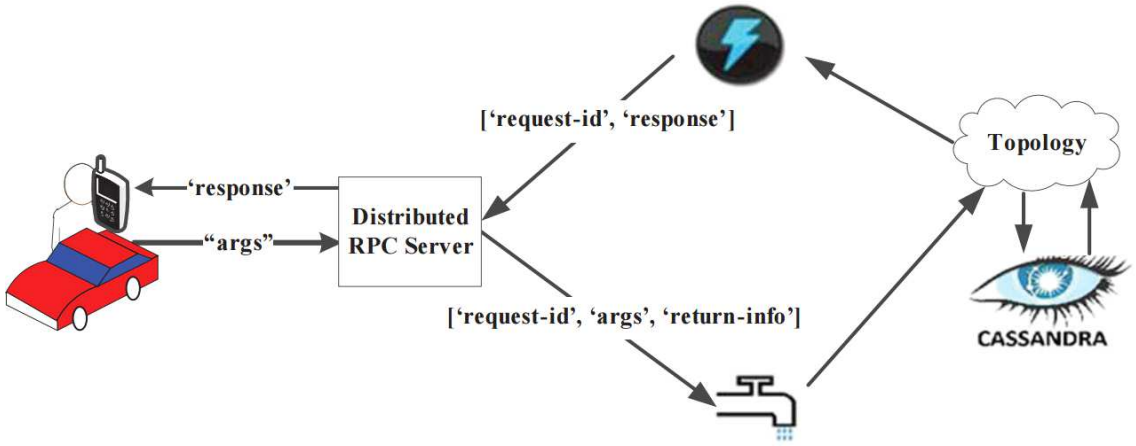


Figure 2.2: Distributed Remote Procedure Call (RPC) Work-flow.

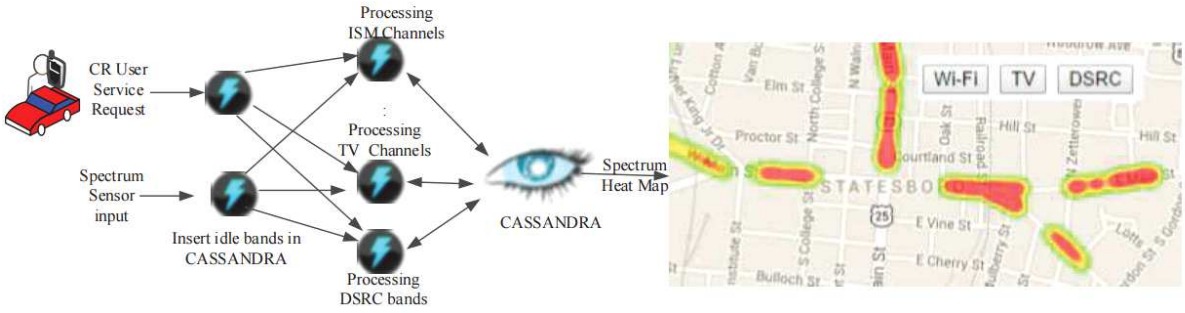


Figure 2.3: Storm Topology for Real-time Processing in Cloud Computing Platform and Generating Spectrum Heat Map Framework.

Storm and Cassandra [49] are integrated by provided generic and configurable backtype storm. Bolt implementation that writes Storm Tuple objects to a Cassandra Column Family for having separate bolts for processing massive data for different bands such as TV, DSRC and Wi-Fi as shown in Figure.2.2 and Figure.2.3. To clearly visualize the available channels in a particular geolocation, the heat map is designed using google API. The idle channel information updated in the database is automatically plotted on the map [35], [28].

2.4 Transmission Power vs. Range in CR Vehicular Network

For a given transmission power p_t, the power p_r at the receiver at a distance R can be expressed as [21]

$$p_r = \underbrace{p_t G_t G_r h_t h_r (\frac{1}{4\pi})^2}_{G_e} \frac{\lambda^2}{L^{\alpha_p}} = p_t G_e \frac{\lambda^2}{L^{\alpha_p}} \tag{2.2}$$

where G_t and G_r are, respectively, transmit and receive antenna gains, h_t and h_r are, respectively, height of transmit and receive antenna, λ is the wavelength (i.e,λ =5.08cm for 5.9GHz DSRC band and λ=12.50cm for 2.4GHz ISM band),and $\alpha p \in [2, 4]$ is the path loss

exponent [21] for vehicular communications. Then, from eq.2.2, the transmission power is expressed as [13]

$$p_t = \frac{p_r}{G_e \lambda^2} L^{\alpha_p} \tag{2.3}$$

This shows that the transmit power p_t depends on the frequency/wavelength that the CR enabled vehicular users choose to communicate and the range they want to cover in cognitive radio vehicular network. When CR enabled vehicular user switches channel, transmission power can be adapted to keep the same transmit range as they had before as long as they do not exceed the upper bound of power limit set by the FCC. It is assumed that each CR enabled vehicular user queries the spectrum database for the entire route (from current location to the destination address) in a regular interval of distance or time to ensure that the CR enabled vehicular users are not creating any harmful interference to PU's [38] [50].

2.5 Adaptive Channel Assignment And Communications In CR Vehicular Network

Several independent channels (e.g., 7 channels in 5.9 GHz DSRC band, 11 channels in 2.4 GHz ISM band and so on) which are used in vehicular communications are considered. It is assumed that each CR enabled vehicular usersearches the spectrum database for idle channels and it sees the primary network states as busy or idle. This process of monitoring a channel (by querying a database) can be modeled as a semiMarkov model. As presented in [51], the PU being ON and being OFF are exponentially distributed with parameters α and β respectively. The probability of PU being present is represented by p_p

$$p_p = \frac{\alpha}{\alpha + \beta} \tag{2.4}$$

The probability of PU being absent p_a respectively and are given as

$$p_a = \frac{\beta}{\alpha + \beta} \tag{2.5}$$

Based on the activity of primary networks, An estimation method [52] that uses probability of sensing/identifying channels based on periodic query time $t$was adopted. Let P_{S0} represents that the primary channel will be idle after t seconds where $S \in 0, 1$ with $S = 0$ if the channel is idle and $S = 1$ if the channel is used by the primary network. Then, the probability P_{S0} can be expressed as

$$P_{S0} = \begin{cases} p_a + p_p.e^{-(\alpha+\beta)t} for S = 0 \\ p_a - p_p.e^{-(\alpha+\beta)t} for S = 1 \end{cases} \tag{2.6}$$

Similarly, the probability P_{S1} for $S \in 0, 1$ that the channel will be used by PU's after periodic query time t second is given as

$$P_{S1} = \begin{cases} p_a - p_p.e^{-(\alpha+\beta)t} for S = 0 \\ p_a + p_p.e^{-(\alpha+\beta)t} for S = 1 \end{cases} \tag{2.7}$$

where the time t is a query interval either it is obtained based on the distance or it is set for every given time interval (e.g. $t = 1$ second or so) or whichever comes first.

For a given transmission range L meter and vehicle speed v, each CR enabled vehicular user should query the spectrum database with a given period

$$t = min\{\frac{L}{v}, t_p\} second \tag{2.8}$$

where t_p is query interval. Note that when a vehicle travels with a speed of 75 mph, it could travel 33.5 meter in a second. Thus, it has been considered in the system model that each vehicle queries spectrum database for every 33.5 meter distance or every t_p = 1 second or whichever comes first.

The expected channel capacity R_n for a given channel n based on the achievable data rate R_a (e.g. 11 Mbps, 24 Mbps, 54 Mbps, etc.) and the channel used probability by PU P_{S1} is given as

$$R_n = R_a(1 - P_{S1}) \tag{2.9}$$

Then, data rate per CR enabled vehicular user can be computed as

$$R_n = \frac{R_n}{N_n} \tag{2.10}$$

where N_n is the total number of CR enabled vehicular users in a channel n within a given radio range that is estimated based on the periodic broadcast status message (refer to [53] for further detail). To choose the best channel, CR enabled vehicular user selects the channel among available ones that offers highest data rate and satisfies its minimum data rate (R^T) requirement as

$$c = arg \max_n R_n, \forall n \tag{2.11}$$

$$\text{s.t } R_n \geq R^T$$

For instance, for a given scenario in Figure 2.1, a CR enabled vehicular user can select channel 11 up to the middle of segment S4 to get high data rate. Then CR enabled vehicular user can not select the channel 11 for the rest of the segment S4 as it creates harmful interference to PU's and could get low data rate.

Because of the error in transmission, each CR enabled vehicular user may have to retransmit the information. Thus, the expected transmission count is adopted [13] which is the average number of transmissions needed to transfer a packet between vehicles. Considering the probability of transmission errors in forward link (down link) and reverse link (uplink) respectively as p_d and p_u, a probability of transmission failure can be written as

$$p_f = 1 - (1 - p_u)(1 - p_d) \tag{2.12}$$

and the expected transmission count (TC), which tells us how many times the data has to be retransmitted for successful delivery, can be expressed as

$$TC = \sum_{m=1}^{\infty} m p_f^{m-1}(1 - p_f) = \left\lceil \frac{1}{1 - p_f} \right\rceil \tag{2.13}$$

where [.] is a ceiling operator. The eq.2.13 shows that when failure probability p_f is 1 (all transmissions failure all the time), TC will be infinitely large. Along the line of [13], the average time for successful data delivery could be expressed in terms of expected transmission time (TT) for data of size D bits with a data rate R_1^n over a link n as

$$TT = TC \frac{D}{R_n} \tag{2.14}$$

To be able to deliver the packet of size D bits successfully, vehicles traveling with a relative speed of v meter-per-second and overlap transmission range of O_r meter in vehicle-to vehicle communication or vehicle-to-roadside communication should satisfy the following condition

$$\frac{O_r}{v} \geq TT \tag{2.15}$$

Otherwise, complete message/data will not be transferred between communicating vehicles using given data rate. CR enabled vehicular users may have to switch to another channel for higher data rate so that they could exchange complete message.

2.6 Simulation And Numerical Results

It is considered that the CR enabled vehicular users use (i) DSRC bands and (ii) CR network with 802.11 Wi-Fi (and DSRC) if DSRC bands are highly congested and Wi-Fi channels idle as shown in Figure 2.4. The plot depicts three scenarios where SU is continuously switching between DSRC bands and Wi-Fi bands to obtain high data rate. It is evident from the $SC3$ that the 802.11n Wi-Fi channels are capable of provides the high data rate compared to 802.11a/b/g Wi-Fi channels and 802.11p DSRC.

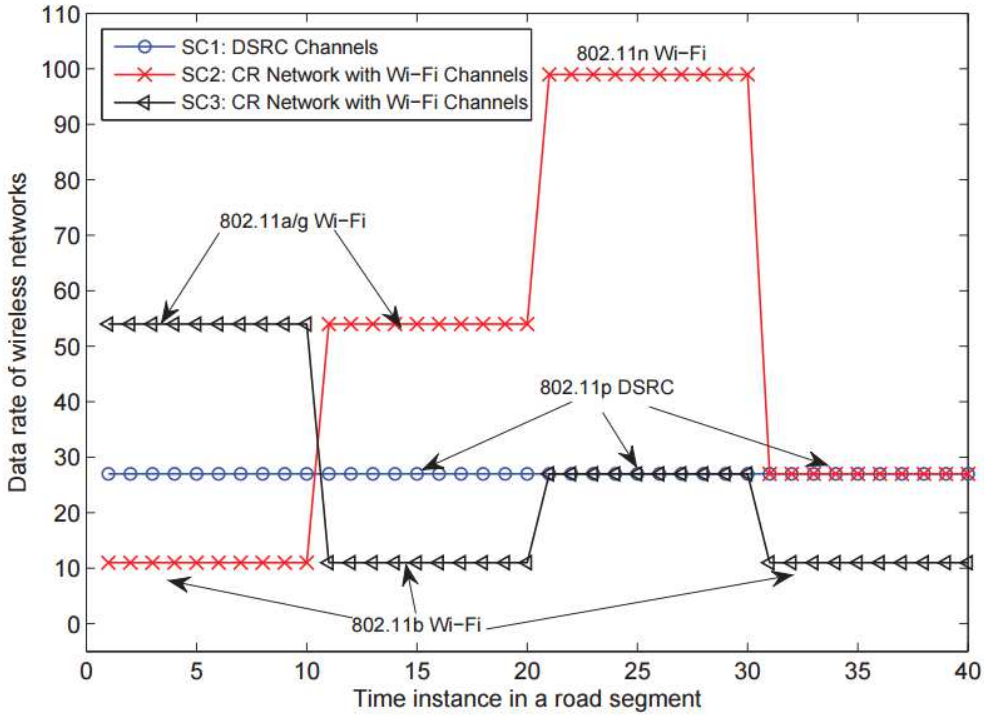


Figure 2.4: Sample scenarios ($SC1$, $SC2$ and $SC3$) for available networks with their data rates (Mbps) for DSRC (802.11p) only and for CR networks (with DSRC and Wi-Fi 802.11a/b g/n) versus the time instances.

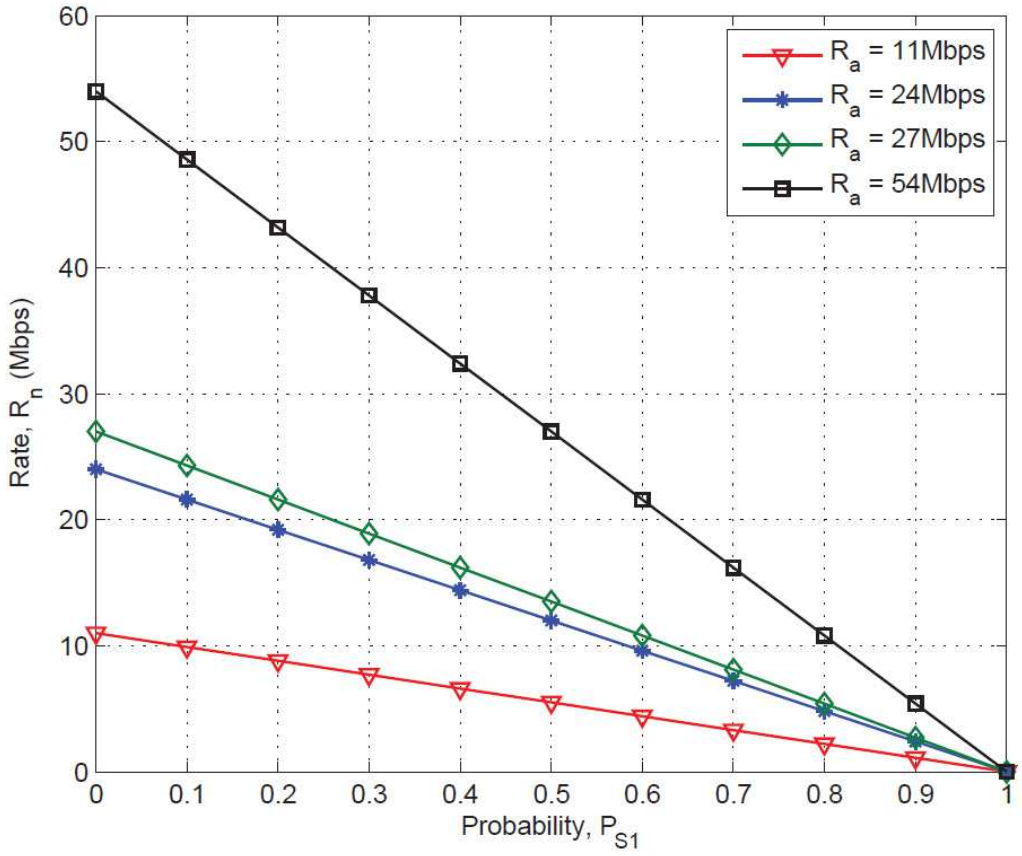


Figure 2.5: Variation of achievable rate in a channel n for variable probability P_{S1} (i.e., the probability of PUs being active in the given channel) for given data rate.

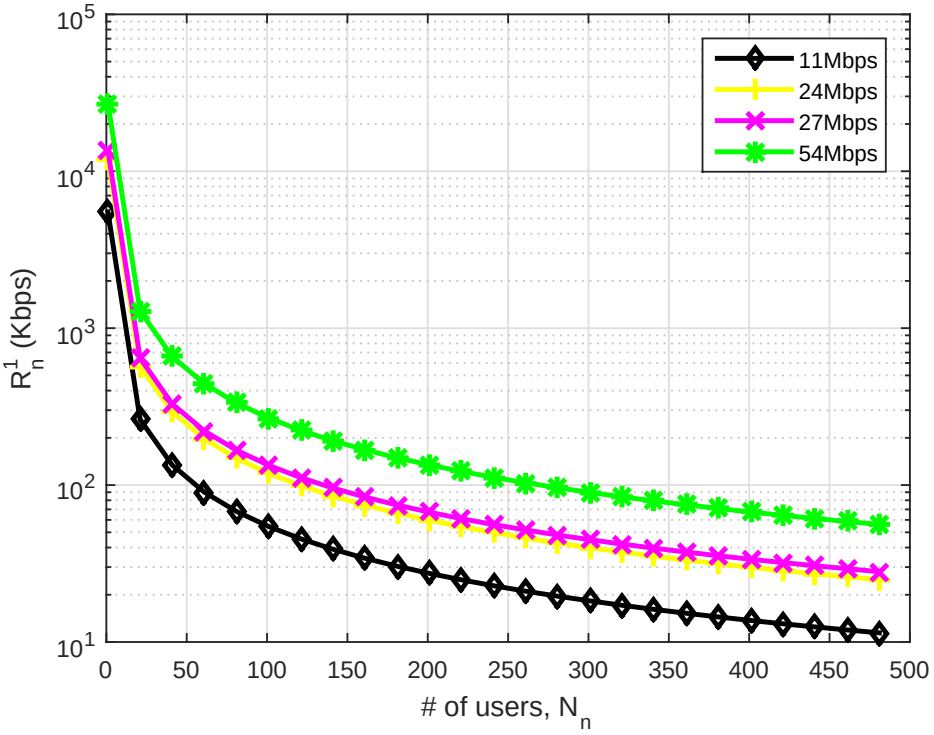


Figure 2.6: Variation of rates in a channel n for each CR enabled vehicular users for variable number of CR enabled vehicular users (N_n) and data rates (R_a) when $P_{S1} = 0.5$

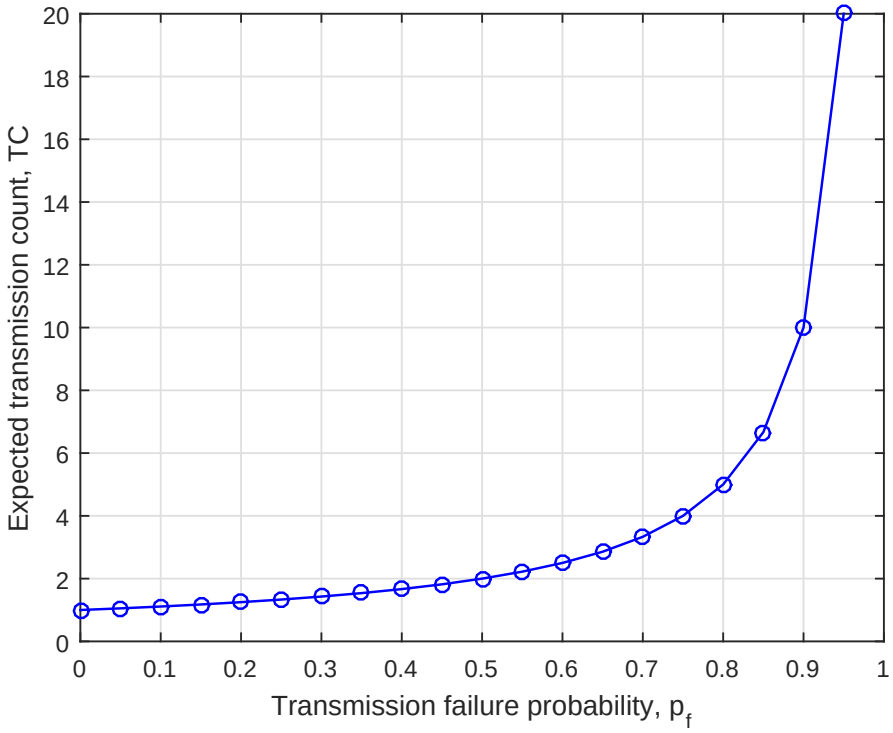


Figure 2.7: Variation of expected transmission count for different failure probability (p_f) values for a given channel.

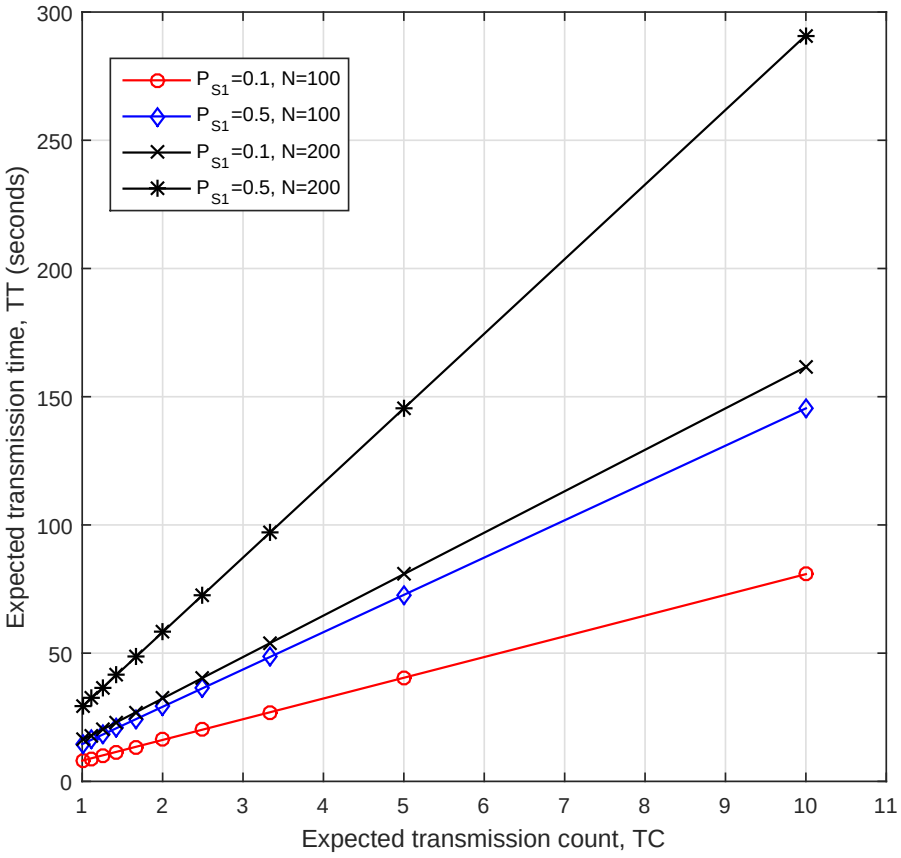


Figure 2.8: Variation of expected transmission time (TT) vs. transmission count (TC) for transmission failure probability value $p_f = 0, 0.1, 0.2, ..., 0.9$, data rate R_a = 11 Mbps, and data size D = 100 KB

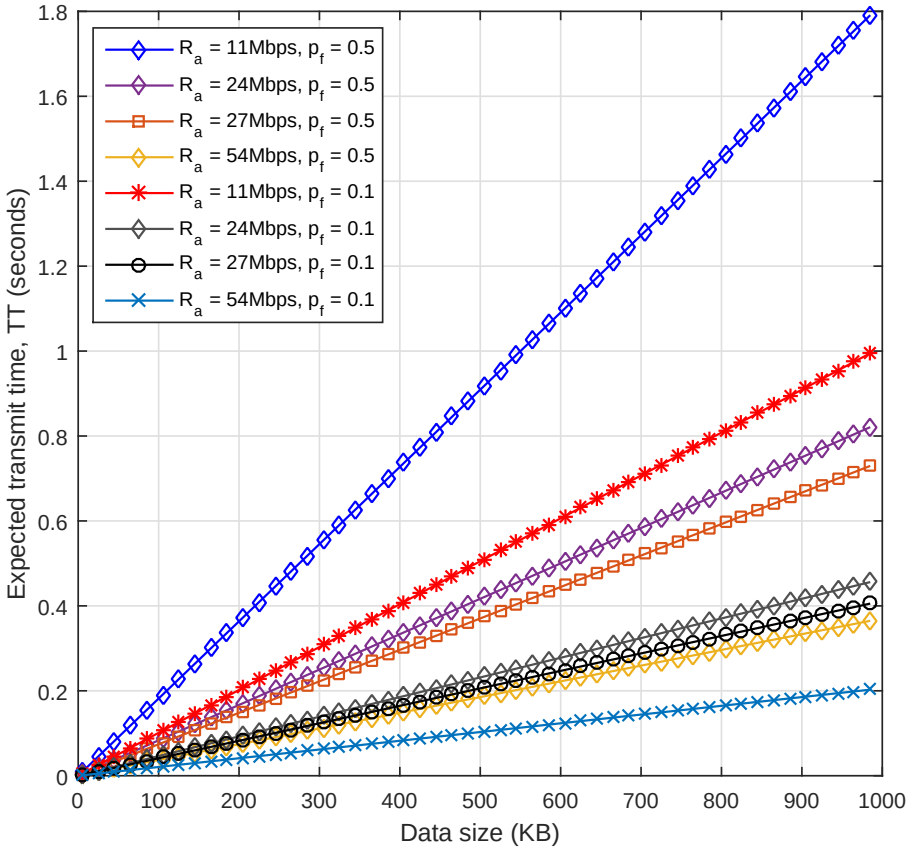


Figure 2.9: Variation of expected transmission time vs. variable data size for different transmission rates and probability of failure pf when probability of PUs being active P_{S1} = 0.5.

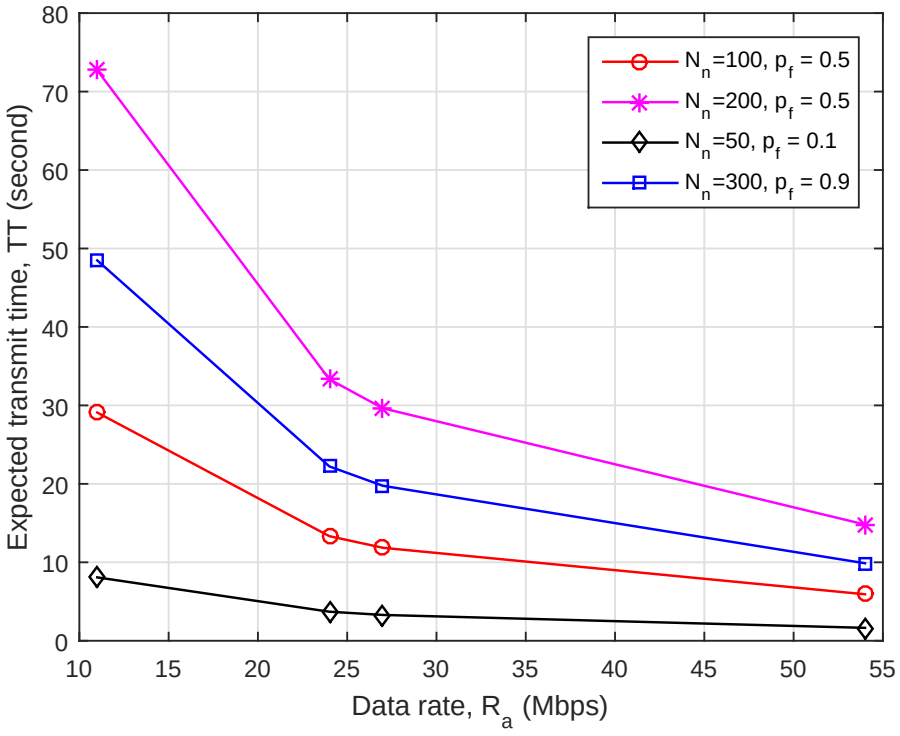


Figure 2.10: Variation of expected transmission time vs. variable data rate for different transmission rates and probability of failure pf when probability of PUs being active P_{S1} = 0.5.

In the first experiment, the variation of total achievable rates in a channel n versus the probability P_{S1} (i.e., probability of PUs being active in a given channel) for given achievable data rates that are available in 802.11p DSRC and 802.11 Wi-Fi networks is shown in Figure 2.5. It is noted that when primary channel is used by PUs, i.e., P_{S1} = 1, CR enabled vehicular users are not allowed to access the channel which results in zero total achievable rate as shown in Figure 2.5. When channel access probability of PU P_{S1} decreases, the achievable data rate obtained by CR enabled vehicular users increases as CR enabled vehicular users gets more channel access opportunities. As expected, CR enabled vehicular users gets higher achievable rate when the data rate is higher. For instance, the R_n obtained by the CR enabled vehicular users at 54 Mbps is almost double than the R_n obtained at 27 Mbps.

Next, the variation of per CR enabled vehicular users rate R_1^n in a channel n versus the number of CR enabled vehicular users (N_n) is plotted for different data rates (R_a) when P_{S1} = 0.5 as shown in Figure 2.6. The rate R_1^n decreases when the number of users increases and vice versa. For instance, at a data rate R_a=11Mbps the rate R_1^n of the channel for 80 users is less than 100Kbps. Whereas, at a higher data rate R_a=54 Mbps the rate of the channel R_1^n for 80 users is around 500 Kpbs. From the Figure 2.6, it is evident that for a given number of users, higher the data rate R_a, higher the user rate R_1^n.

Then, the variation of expected transmission count versus the different probability of failure (p_f) for a given channel is shown in Figure 2.7. The plot depicts that the expected transmission count increases exponentially with increase in probability of failure as shown in Figure 2.7. Furthermore, the expected transmission count is infinity when probability of failure is 100% (i.e., (p_f = 1). This implies that the there would not be successful transmission when p_f = 100% in the network.

Next, the variation of expected transmission time versus the expected transmission count is plotted for transmission failure probability values $p_f = 0, 0.1, 0.2, \ldots, 0.9$, data rate

$R_a = 11Mbps$, and data size D = 100 KB as shown in Figure 2.8. For a given data size, when expected transmit count increases (which increases with probability of transmission failure), expected transmission time increases as shown in Figure 2.8. Furthermore, the plot depicts that the expected transmission time increases with increase in number of CR enabled vehicular users for a given P_{S1} as shown in Figure 2.8. When transmission failure probability p_f = 1, the expected transmit count becomes infinity and thus expected transmit time becomes infinity implying that there would not be successful transmission.

Then, the variation of expected transmission time versus the variable data size is plotted. The different transmission rates and probability of failure p_f values are considered in the plot and probability of PUs being active is considered as P_{S1} = 0.5. As expected, transmission time increases when data size to be transmitted increases as shown in Figure 2.9. Similarly, for a given data size (e.g., 500 KB), the expected transmission time increases when data rate decreases and vice versa for a given failure probability p_f value. Furthermore, for given data size (e.g.,500 KB) and data rate (e.g., 11 Mbps), when p_f increases from 0.1 to 0.5, expected time is almost doubled as shown in Figure 2.9.

Finally, the variation of expected transmission time versus the variable data rate was plotted for different number of CR enabled vehicular users (N_n) and probability of transmission failure (p_f) when probability of PUs being active is P_{S1} = 0.5 as shown in Figure 2.10. From the results it is observed that, for lower data rate, the expected transmission time is higher as shown in Figure 2.10. For a given scenario, expected transmission time is lower for the higher number of CR enabled vehicular userss in a given channel. For instance, for a data size 100 KB with transmission data rate of 27 Mbps, expected transmission time is lower by half for $N_n = 100$ than that for $N_n = 200$ as shown in Figure 2.10. Similarly, when the number of CR enabled vehicular users $N_n = 300$ and the transmission failure probability p_f is 0.9, expected transmission time is almost twelve times greater than that when the number of CR enabled vehicular users $N_n = 50$ and the transmission failure

probability p_f is 0.1. It is observed that when there are few users competing for channel access, there could be less transmission failure and given data could be transmitted faster and vice versa.

2.7 Chapter Summary

In this chapter, a cloud-assisted GPS driven dynamic spectrum access in cognitive radio vehicular networks for transportation CPS has been presented. Each CR enabled vehicular users present in the system calculates the best route to its destination using GPS device and queries the spectrum database for spectrum opportunities for a given route. To receive updated spectrum occupancy information, CR enabled vehicular users query database periodically to make sure that the band is still available and use of the band is not creating any harmful interference to PUs. The performance of the proposed approach has been evaluated using numerical results obtained from simulations. The effect of PUs activities in the cloud-assisted GPS-driven dynamic spectrum access have been analyzed. When PUs were active most of the time with high probability P_{S1}, data rate of CR enabled vehicular users decreased significantly as there were less spectrum opportunities for CR enabled vehicular users. Effect of number of CR enabled vehicular users in a given channel in terms of data rate has been analyzed where increase in number of CR enabled vehicular users resulted in decrease in data rate as they had to share the same channel. Furthermore, expected transmit count increased exponentially with increased in transmission failure probability that resulted in high expected transmission time for given data size. As expected, the results showed that the transmit time increased when transmission rate decreased. To conclude, there should be some trade-off between number of users per channel, delay introduced by query process and data rate in cognitive radio enabled vehicular networks to get reliable wireless communications for transportation CPS.

CHAPTER 3

SECURING REAL-TIME SPECTRUM ACCESS IN COGNITIVE RADIO VEHICULAR NETWORKS AGAINST LOCATION FALSIFICATION ATTACKS

In the previous chapter, the cloud-based framework for enabling dynamic spectrum access for CR enabled vehicular users was proposed. This chapter deals with addressing the location falsification attacks and measurement errors caused due to Global Positioning System (GPS) and improving the performance of the overall system [30].

GPS plays a crucial role in the system as it is used by secondary users to find their present location for reporting to database. Furthermore, allocation of the suitable channels to SU depends on the location reported by GPS. GPS is prominent for the location-based services in telecommunication, transportation, and tracking applications [54]. Besides, the numerous number of applications, there are many limitations of GPS that can affect the performance and security of the system [30].

First, GPS has no security mechanisms embedded in it which make it easily vulnerable to spoofing attacks [55, 56]. While querying geolocation database to find idle channels for given location and time, malicious secondary users can fake their geolocations using GPS spoofing techniques to pretend to be in a place where more/better idle channels are available. This type of attacks are commonly known as location falsification attacks. Note that, in geolocation database based opportunistic spectrum access, secondary users get a list of channels based on the reported geolocation. The GPS information should be accurate to allocate the suitable channels for the users. If GPS spoofing occurs and the reported location is fake, then the user gets idle channels based on the reported false location and will create interference to other active users or primary users in the region [30].

Second, the other drawback of GPS is the measurement errors caused while determining the location of the user. The prime reason for the measurement errors is due to the obstruction of GPS signal by various objects present in the environment [57] [58]. Further-

more, these errors in GPS can result in reporting the inaccurate location to the database because of which the probability of misdetection (P_{MD}) and the probability of false alarm (P_{FA}) in the system can increase. The probability of misdetection (P_{MD}) and the probability of false alarm (P_{FA}) should be reduced because it will impact the overall performance of the system [37].

In this chapter, two attack scenarios for location falsification attacks are formulated. Next, the three-step mechanism for detecting the malicious users in the above discussed scenarios is presented. Then, the probability of false alarm and the probability of misdetection that arose due to GPS uncertainties are discussed using two different scenarios.

The remainder of this chapter is organized as follows: Section 3.1 presents the related work. Section 3.2 presents the system model followed by the algorithm in Section 3.3. The simulation results are presented in Section 3.4 followed by the conclusion in Section 3.5.

3.1 Related Work

3.1.1 GPS Vulnerabilities

GPS is the prime target for attacks as it is being used in various applications. Spoofing attacks are the most common type of attacks in GPS where the identity of the legitimate user is misused for conducting attacks. The authors in [54] provided a detailed explanation of the different types of GPS spoofing generation techniques such as GPS signal simulator, receiver-based spoofing and sophisticated receiver based spoofing. They also proposed various anti-spoofing methods for mitigation of these attacks. This paper was able to provide the understanding on how attacks occur in GPS.

Authors in [59] and [60] discuss the GPS spoofing techniques in database driven cognitive radio networks. In [59] authors propose prispectrum (Privacy Preserving Spectrum Retrievial And Utilization For White Space Database) method for protecting the SU loca-

tion from primary user coverage complement attack and enforced channel switch attack. Prispectrum algorithm is further divided into two parts i.e, PSAIR and PCU. PSAIR (Private Spectrum Availability Information Retrieval) is implemented to secure the location of the SU while accessing the database to find idle channels. Whereas, PCU (Private Channel Utilization) is used for protecting the privacy while utilizing the channels. The best way to preserve the privacy is to select the most stable channel for utilization. Continuous Markov model can be used to estimate the stable channel from the list of available channels.

Authors in [60] proposed three main schemes for detecting the optimal and random attacks in GPS. The three methods include centralized detection scheme (CLV), environmental-radio-based location verification (ELV) and peer location verification (PLV).

Though, this thesis also uses the spoofing detection techniques to protect the legitimate secondary users. The techniques implemented for detection of the attacker are different from the above discussed papers. The angle of arrival, time of arrival and received signal strength parameters are used for detection of spoofing.

3.1.2 Angle of Arrival Methods

Angle of arrival has found its applications in many fields such as localization and tracking. The two types of systems used for determining the angle of arrival are switched beam systems (SBS) and adaptive array system (AAS). Though switched beam systems(SBS) were developed earlier than adaptive array system (AAS), SBS are not commonly used because of their failure in determining the AOA at lower signal powers.

Adaptive antenna system are the intelligent array of antennas that can avoid interference by dynamically adapting to the environment. AAS are classified into non-subspace and subspace techiques [61].

1. **Non-Subspace Techniques**: In non-subspace techniques (a.k.a classical AOA techniques), the AoA is determined based on the peaks of spatial spectrum. These

techniques are not capable of providing high resolution angle of arrival. Bartlett and capon minimum variance are the examples of non-subspace techniques. The equation for AOA using Bartlett method is given as

$$P_{Bartlett}(\phi) = a^H(\phi) R_{xx} a(\phi) \tag{3.1}$$

Here R_{xx} and H represents the autocovariance matrix and Hermitian matrix respectively.

The equation for AOA estimation using capon minimum variance method is given as

$$P_{Capon}(\phi) = \frac{1}{a^H(\phi) R_{xx}^{-1} a(\phi)} \tag{3.2}$$

2. **Subspace Techniques**: The subspace technique comprises of noise subspace and signal subspace that are perpendicular to each other. These techniques are capable of offering high resolution angle. Espirit and MUSIC algorithms are the examples of subspace techniques. ESPIRIT (Estimation of signal parameter via rotational invariance technique) is a subspace technique proposed by Roy and Kailath in 1989 [62]. The equation for angle of arrival in ESPIRIT algorithm is given by

$$P_{ESPIRIT}(\phi) = sin^{-1}[c\frac{arg(\hat{\theta})}{\beta \delta x}] \tag{3.3}$$

MUSIC (MULTIPLE signal classification) is the popular subspace technique proposed by schmidt in 1986. It is capable of finding various parameters such as angle of arrival, polarization, interferences and number of signals [63]. Other main advantage of MUSIC algorithm is its capability to support real-time processing. The music algorithm is represented by the equation

$$P_{MUSIC}(\phi) = \frac{1}{a^H(\phi) B_n B_n^H a(\phi)} \tag{3.4}$$

In this thesis, MUSIC algorithm is selected over other algorithm as it is more accurate and precise compared to other direction of arrival (DOA) algorithms. A significant

amount of work has been conducted in comparing the performance of DOA algorithms. The authors in [64] provided numerical simulations for determining the resolution of three techniques i.e, Bartlett, Capon and MUSIC. The results clearly depicts that, MUSIC algorithm has more precise estimation compared to other algorithms. MUSIC algorithm is dependent on many factors and accurate results can be obtained when there are large number of snapshots, antenna elements and low SNR [64].

3.2 System Model

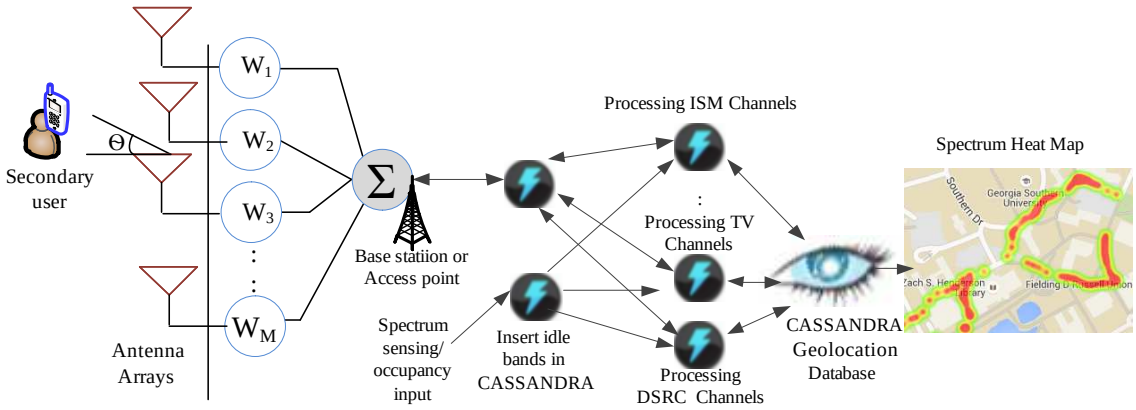


Figure 3.1: A typical system model for securing opportunistic spectrum access in cognitive radio networks with Storm model for real-time parallel processing.

A typical system model is shown in Figure 3.1 where secondary users are assumed to be equipped with GPS and connected to Internet to query the geolocation database through antenna arrays. The secondary users get their location using GPS and report that information to the database to get idle channels for opportunistic spectrum access through access point or base station. The secondary users are verified for their reported locations using Storm based cloud computing [28, 49] before giving any idle channel information

to them as shown in Figure 3.1. It is assumed that the spectrum occupancy information is received either from primary infrastructures or from dedicated spectrum sensors and processed to store geolocation of idle bands. SU depend on GPS for finding the location and reporting to database.

3.2.1 Attack Model

In this chapter, two kinds of spoofing attack scenarios that may occur in geolocation database driven opportunistic spectrum access in cognitive radio networks are discussed. Here, it is assumed that the malicious secondary user reports the fake location to the database requesting for the idle channels.

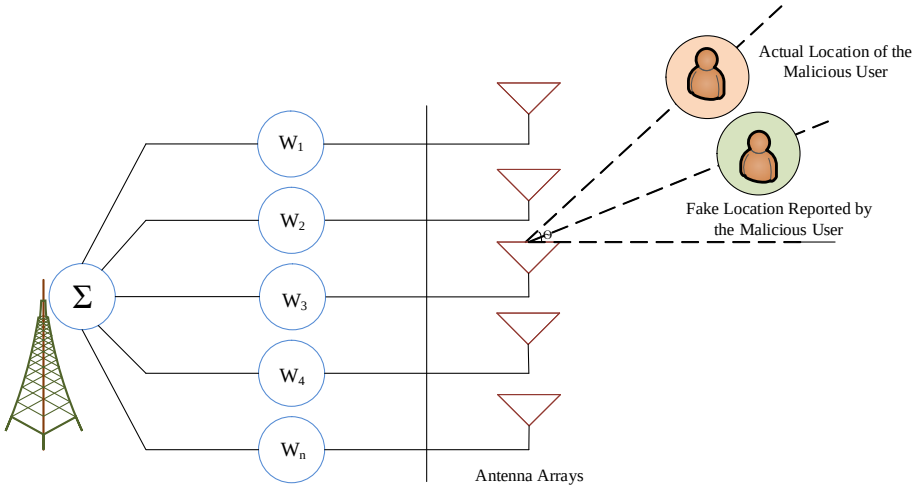


Figure 3.2: Attack Model 1 (Case I)

1. *Case I*: The malicious secondary user is present in the different location and spoofs the GPS to report the wrong location to cloud-based spectrum database. In this case, the malicious secondary user is communicating from the location present at a different angle to the actual reported location as shown in Figure 3.2. The green circle in the

Figure 3.2 represents the fake location reported to the database and the orange circle represents the actual location of the user.

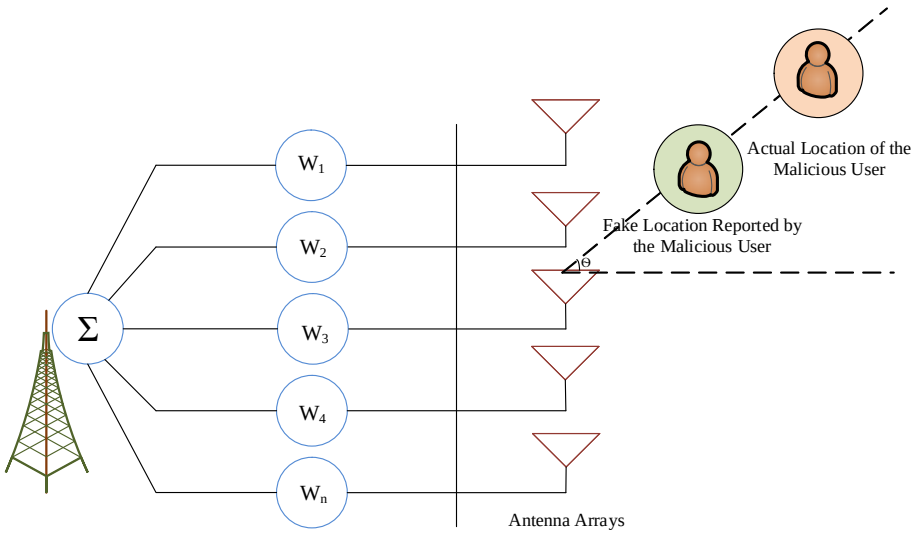


Figure 3.3: Attack Model 2 (Case II)

2. *Case II*: From the typical scenario of case II shown in Figure 3.3, it is evident that the actual location and reported fake location are present in the same angle. In this case, the malicious secondary user is assumed to be communicating on the same angle of the reported location but is present on the location that is far away from the reported location.

The channels in the geolocation database are allocated based on the reported location. If the reported location is fake, this may cause harmful interference to primary users or create harm to the other legitimate secondary users who will not be able to use that idle channels assuming that they are already occupied by some other user. This may lead the controversy to the concept of cognitive radio, because most of the channels spoofed by the attackers remain unutilized/underutilized. Using the system model in Figure 3.1, three steps are implemented to find malicious secondary users who report their fake geolocations.

3.2.2 Angle of Arrival

Angle of arrival can help to determine whether location is spoofed or not by checking two angles 1) actual angle based on the received signal using antenna array and 2) angle based on the reported geolocation that the malicious user claims to be at. To implement angle-of-arrival, the basic components are discussed below to make this chapter self-content.

The uniform linear array consists of the M antenna elements arranged linearly on the plane as shown in Figure 3.4. The separation between each of the antenna elements is represented by d and is assumed to be half of the wavelength $\frac{\lambda}{2}$ [65]. Let us consider that

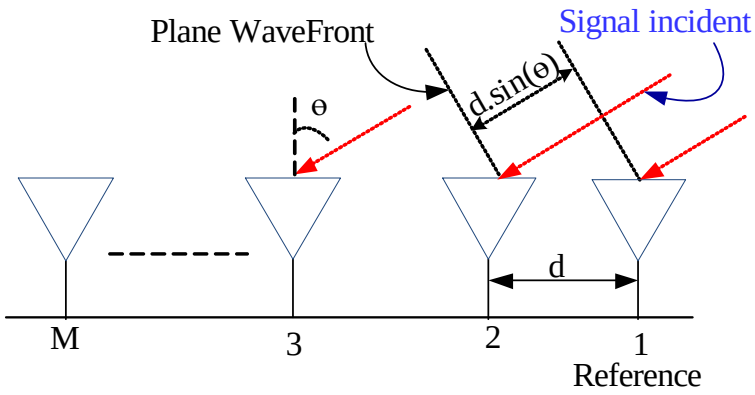


Figure 3.4: Uniform linear array for measuring angle-of-arrival for M number of antennas separated each by distance d and the signal incident angle θ.

the signal incident on the surface of kth antenna at time instance t is $s_k(t)$. Then, the received signal at second antenna compared to the signal received at the first antenna is

$$s_2(t) = s_1(t - t_d), \tag{3.5}$$

where t_d represents the time delay occurring at the adjacent antenna while receiving the signal. The time delay t_d is computed as

$$t_d = \frac{d.sin(\theta)}{c} \tag{3.6}$$

where θ=angle of incidence and c is the speed of light.

The adaptive array techniques can be employed in uniform linear arrays for finding the direction of arrival of a signal using different techniques such as MUSIC, ROOT MUSIC and ESPIRIT algorithms [61]. The resolution of the angle estimation depends on factors such as number of antenna elements, SNR and the number of snapshots. The system is expected to work more efficiently under low signal to noise ratio and achieve high resolution when high number of antenna elements are equipped in the system. To determine direction of arrival of the multiple signals, the MUSIC (Multiple Signal Classification) algorithm is used, where Eigen decomposition of the values is done for differentiating between the signal subspace and noise subspace [63]. The signal obtained by the MUSIC algorithm can be written as

$$x(t) = A.s_k(t) + n(t) \tag{3.7}$$

$$A = [a(\Phi_1), a(\Phi_2), a(\Phi_3), ..., a(\Phi_{D-1})]$$

where A consists of steering vectors with respect to the direction of arrival of the signal at the antenna array, and $n(t)$ is the noise at the receiver that corrupts the received signal. The power spectrum in MUSIC algorithm is given as [65]

$$\theta_1 = P_{MUSIC}(\phi) = \frac{1}{a^H(\Phi)B_nB_n^Ha(\Phi)}, \tag{3.8}$$

where B_n consists of Eigen vectors associated with the noise subspace. The spectrum function is defined as

$$P(\theta) = 10\log_{10}\frac{Pmusic}{max(Pmusic)} \tag{3.9}$$

The angle (in degrees) between secondary user's reported location and receiver location with their longitudes and latitudes, i.e., (L_1, L_2) and (L_3, L_4) can be calculated as

$$\theta_2 = \text{atan2}(\beta_1, \beta_2) \tag{3.10}$$

where $\beta_2 = \cos(L_2)\sin(L_4)\sin(L_2)\cos(L_4)\cos(L_3 - L1)$ and $\beta_1 = \sin(L_3 - L1)\cos(L_4)$.

The angle of arrival obtained using the reported coordinate information is compared with the angle obtained at antenna arrays equipped in the system.

3.2.3 Received Signal Strength

When legitimate location and reported fake location are in the same reference line, the angle based on reported fake location and angle based on angle-of-arrival are same. In this case angle-of-arrival technique cannot detect the malicious secondary users.

The malicious secondary user can be in the same angle-of-arrival but at a different location. The received signal strength is used to estimate tentative position of the user. The power calculated based on the distance of the user with the help of the reported geolocation is compared with the power received at the receiver. The distance between a secondary user and receiver with their longitudes and latitudes, i.e., (L_1, L_2) and (L_3, L_4) can be calculated using Haversine distance as [66]

$$d = 2R \sin^{-1} \sqrt{\sin^2(\frac{L_3 - L_1}{2}) + \cos(L_3) \cos(L_1) \sin^2(\frac{L_4 - L_2}{2})} \tag{3.11}$$

here $R = 6371$km is the mean radius of the Earth. Then, the received signal strength is calculated using free space path loss equation

$$P_{r_2} = P_t G_t G_r \frac{\lambda^2}{(4\pi d)^2} \tag{3.12}$$

where G_t and G_r are transmit and receive antenna gains respectively, and P_t and P_{r_2} are the transmit and the receive power respectively.

3.2.4 Time of Arrival

Received signal strength approach may fail to detect the faked location when malicious user changes its transmit power to make the power level (calculated based on Euclidean distance) and actual received power equal. Then, time of arrival of arrival can be used.

Time-of-arrival based on reported location vs the time of arrival based on the actual signal reception can help to determine whether user is malicious or not. The time of arrival can be calculated based on reported location is

$$T_a = \frac{d}{c} \tag{3.13}$$

The time T_a can be compared with time computed based on reference location to make judgment on the user.

3.2.5 Measurement errors in GPS

Measurement errors in GPS occur due to factors such as the number of available satellites in that location, the position of satellites and signal multipath. Different GPS receivers have accuracy ranging from $3m$ to $100m$ [57]. Due to the error in GPS, the location reported will not match with the actual location obtained at the antenna arrays. This creates harm to legitimate secondary user and also increase the probability of misdetection and probability of false alarm degrading the efficiency of the system [37].

Probability of Misdetection

The probability of detection is the number of users belonging to the desired location that are being detected. The probability of misdetection is the scenario where the number of legitimate users belonging to the desired location and still remain undetected due to the error in GPS. It is represented as

$$P_D + P_{MD} = 1 \tag{3.14}$$

$$P_{MD} = 1 - P_D \tag{3.15}$$

Where, P_D is the probability of detection and P_MD is the probability of misdetection. The secondary user (SU) report the location to the database using GPS. If there is a

measurement error in determining the location, it will harm the legitimate secondary user, as they are not granted permission the database.

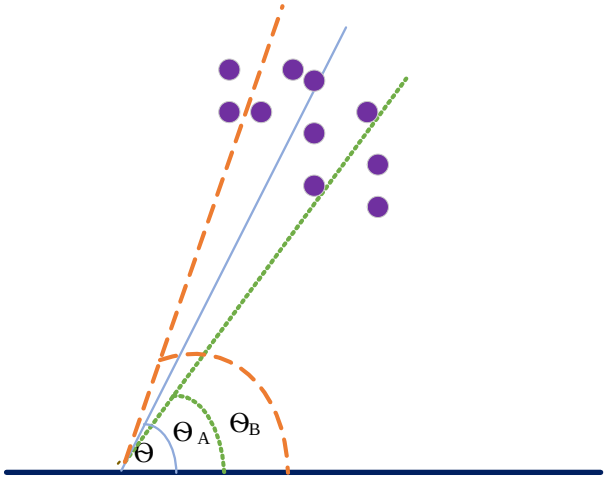


Figure 3.5: Probability of Misdetection.

Figure 3.5 represents typical scenario of misdetection. The solid blue line is the reference angle of the user's location. If the users present in that angle are considered to be legitimate, then most of the other users remain undetected due to the small angular error. To avoid these uncertainties and provide high QoS to the legitimate secondary users the tolerance of the reference angle is increased. The dotted lines represent the increased tolerance levels of the reference angle. All the users within the tolerance limit are allowed to access the database.

The range of the reference angle is represented as

$$\theta_{ref} = [\theta_A, \theta_B] \tag{3.16}$$

Where, $\theta_A = \theta_{ref} - \epsilon$, $\theta_B = \theta_{ref} + \epsilon$ and ϵ is acceptable tolerance limit.

Probability of False Alarm

The probability of false alarm in our scenario, is the users not belonging to particular location but, are assumed to be present in that location. The high tolerance level is one of

the major cause for rise in probability of false alarm P_{FA}.

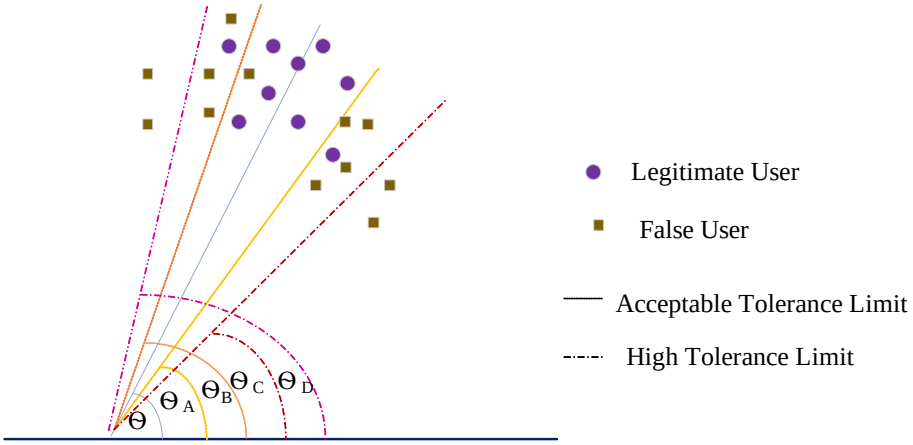


Figure 3.6: Probability of False Alarm.

Figure 3.6 represents typical scenario for the false alarm. In the Figure 3.6, the purple dots represent legitimate secondary users belonging to the location of interest and the yellow diamonds represent the users that do not belong to that location. The dotted lines with an angle of θ_A and θ_B represent the acceptable tolerance levels. The dashed represent the high tolerance levels causing the false alarm.

The θ'_{ref} is the angle with high (P_{FA}) represented as

$$\theta'_{ref} = [\theta_C, \theta_D] \tag{3.17}$$

Where, $\theta_C = \theta'_{ref} - \epsilon'$ and $\theta_D = \theta'_{ref} + \epsilon'$ and ϵ' is the high tolerance limit.

With the increase in tolerance level, the number of unwanted users is exceeding legitimate users belonging to that location. The tolerance level for considering the users should be limited within certain threshold value for minimizing false alarm in the system.

3.3 The Algorithm

When a secondary user queries for the idle bands, it sends its demands along with its geolocation (longitude, latitude) to the geolocation database through access points as shown in our system model (Figure 3.1).

First Step: The direction of arrival θ_1 is estimated using (3.8) and the angle θ_2 in (3.10) is calculated using reported coordinate information. Then, the angles θ_1 and θ_2 are compared to check whether the secondary user is at legitimate location. If the angles θ_1 and θ_2 are not within the tolerable limit, no channels will be allocated to the given secondary users as it spoofed the location.

Second Step: If both the angles are similar then user is assumed to be in the same angle-direction. The power obtained at the receiver is considered as P_{r1} and the power calculated based on the distance is considered as P_{r2}. If the difference of two power values $P_{r1} - P_{r2} > \epsilon$ is not within the tolerable limit, the secondary user is assumed to be malicious and it will get no permission to access any channels.

Final Step: If the power values P_{r1} and P_{r2} are within the tolerable limit, the user could be the legitimate user. However, secondary users could be smart and could adjust its transmit power to make P_{r1} equal to P_{r2}. Thus, time-of-arrival step is used for further verification. If time of arrival of the signal received from a secondary user and the reference point are not matching, the user is assumed to be malicious and the malicious user will not get any idle channels to access. Whereas if the user passes all three steps, it is assumed to be legitimate and will get all idle channels. It chooses the best channels from the list to communicate opportunistically.

Based on the analysis above, the algorithm is presented as **Algorithm 1** which is executed for each request from secondary users.

Algorithm 1 Securing Dynamic Spectrum Access

1: **Input**: Geolocation of access point (L_3, L_4), geolocation database of idle spectrum and tolerance ϵ.
2: **Output**: A list of idle channels for legitimate secondary users (and NO channel access for malicious users).
3: **for** Each request from secondary user **do**
4: Receive geolocation of secondary user (L_1, L_2), received signal P_{r_1}, time of arrival based on reference location T_{a_r}.
5: Calculate angle θ_1 using (3.8) and θ_2 using (3.10).
6: **if** $(|\theta_1 - \theta_2| \leq \epsilon)$ **then**
7: Calculate P_{r_2} using (3.12).
8: **if** $(|P_{r_2} - P_{r_1}| \leq \epsilon)$ **then**
9: Calculate time of arrival T_a
10: **if** $(|T_a - T_{a_r}| \leq \epsilon)$ **then**
11: The secondary user is legitimate and RELEASE a list of available idle channels for that location.
12: **else**
13: Location is spoofed. GO TO Step 19.
14: **end if**
15: **else**
16: Location/power is spoofed. GO TO Step 19.
17: **end if**
18: **else**
19: STOP. The secondary user is malicious. Do NOT send any idle channel info.
20: **end if**
21: **end for**

3.4 Numerical Results and Analysis

The performance of the proposed method summarized in **Algorithm 1** is evaluated using simulations and experiments. The numerical results are presented in this section to validate the efficiency of the proposed system model. For the MUSIC algorithm, the parameters considered are number of antenna arrays $M = 10$, signal to noise ratio SNR=20dB, number of snapshots equal to 200, and the angle from 0° to 90° (i.e., first quadrant for a sake of simplicity). However the angle can be varied from 0° to 180° to 360°.

First, the **Scenario 1** presented in Figure 3.7 considers (*Case I* in Section 3.2) where a secondary user sends its fakes geolocation making different angle of arrival than estimated by the antenna array. The angle variation is plotted in Figure 3.7 clearly depicts that angle θ_1 obtained from antenna arrays is 40° whereas θ_2 obtained from reported location is about 65°. When two angles θ_1 and θ_2 are not within the tolerable limits it can be concluded that the given secondary user is malicious. In this case, other parameters such as received power and time of arrival are not verified.

Second, the **Scenario 2** considers (*Case II* in Section 3.2) where a secondary user reports its fake geolocation for searching idle channels making same angle of arrival with the angle estimated at the antenna array. For this scenario, the results are plotted in Figure 3.8. The fake geolocation reported by the user has angle of arrival of about 46° closely matching with the angle obtained from antenna arrays as shown in Figure 3.8(a). However, the received power has a large variation as shown in Figure 3.8(b) and time of arrival was also different as shown in Figure 3.8(c). This observation concluded that the secondary user was malicious one and it did not get channels to access them opportunistically.

Third, the **Scenario 3** also considers (*Case II* in Section 3.2) where a secondary user reports its fake geolocation for searching idle channels and adjust the power level so that received signal power matched with the estimated one. Simulation results were plotted in Figure 3.9. In this scenario, angle of arrivals obtained are about 63 ° in both the cases as

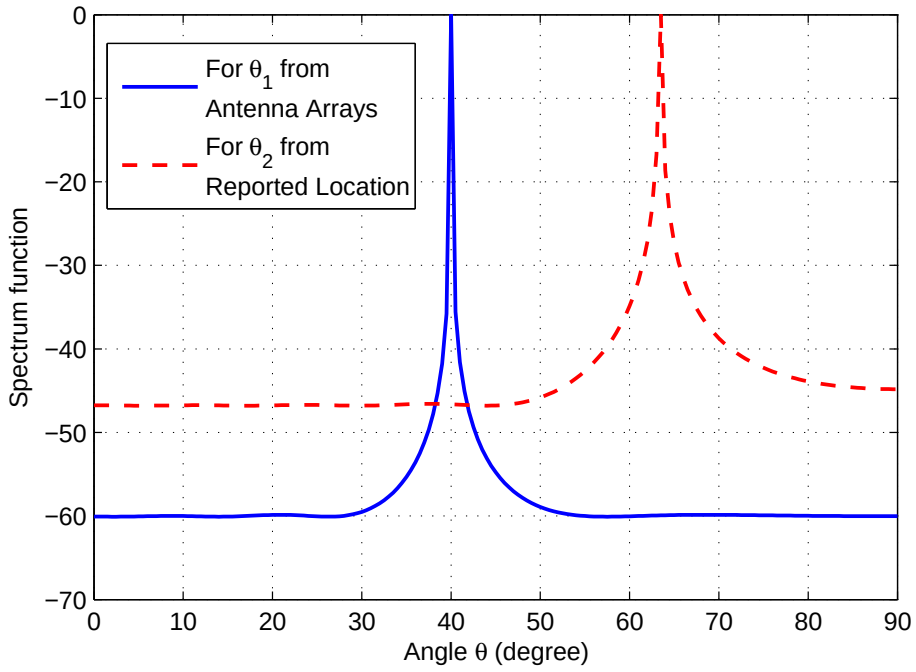
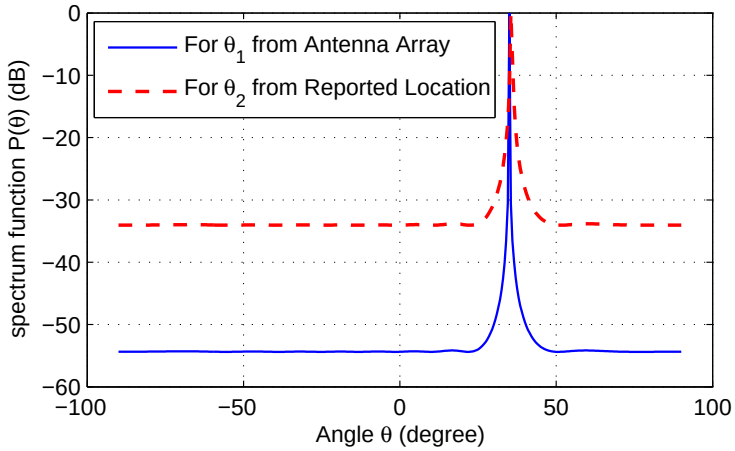
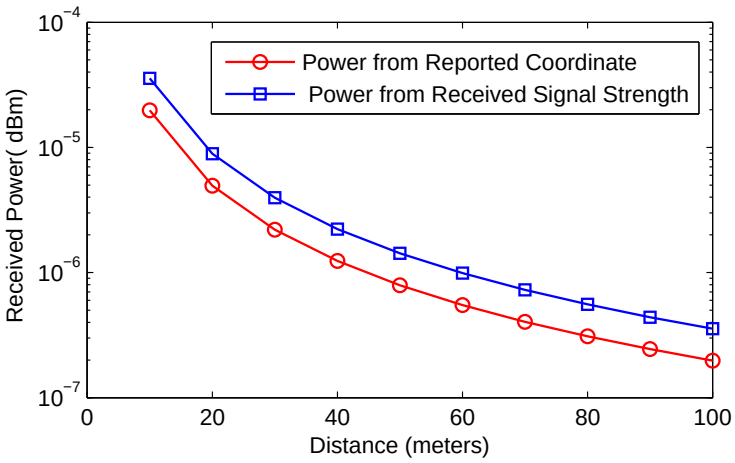


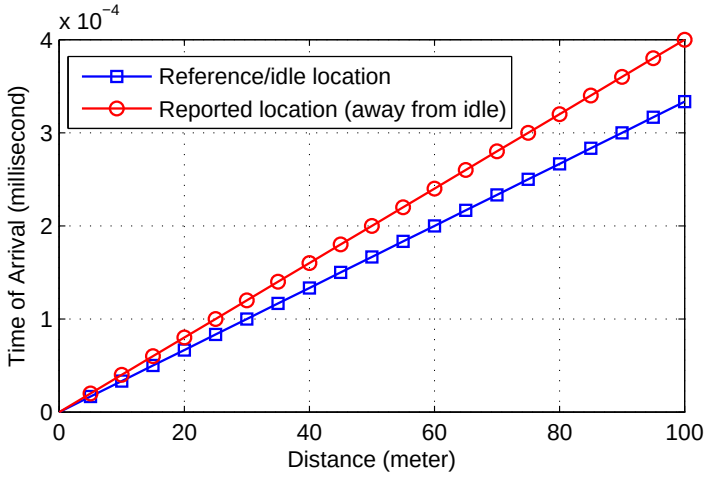
Figure 3.7: The angle estimated at antenna array does not match with the angle based on geolocation coordinate in **Scenario 1**



(a) Spectrum for θ_1 and θ_2

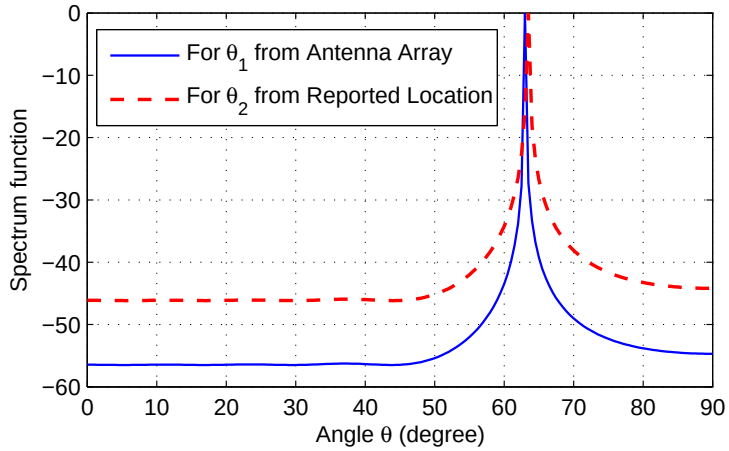


(b) Received Signal Strength vs Distance

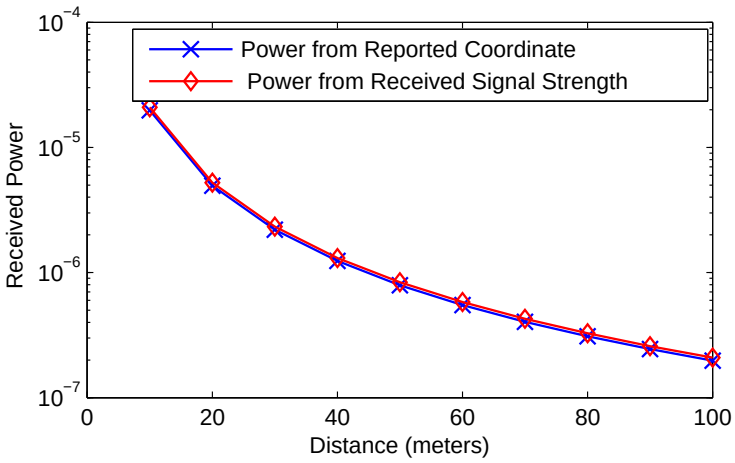


(c) TOA from Secondary Users

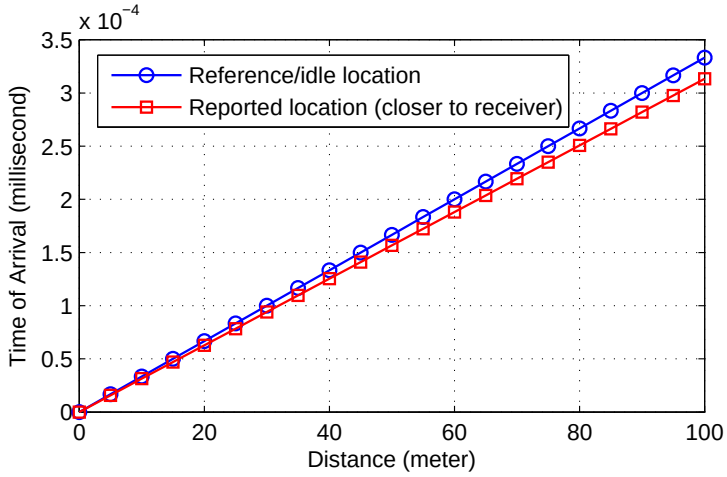
Figure 3.8: Variation of angle spectrum, received signal strength and time of arrival for malicious user for **Scenario 2**



(a) Spectrum for θ_1 and θ_2.

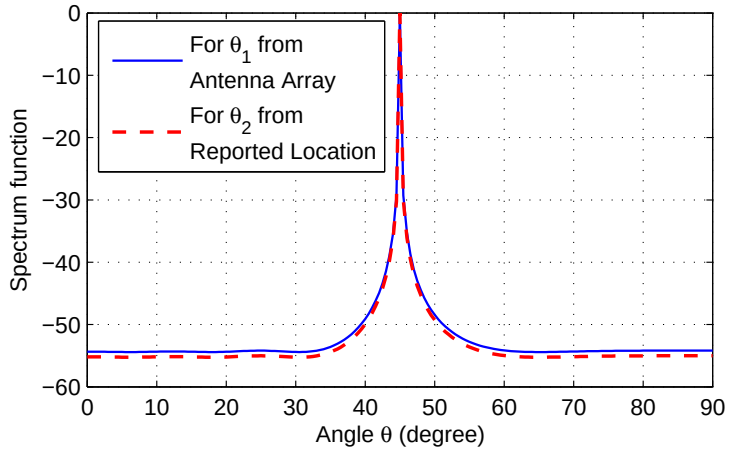


(b) Received signal strength vs distance.

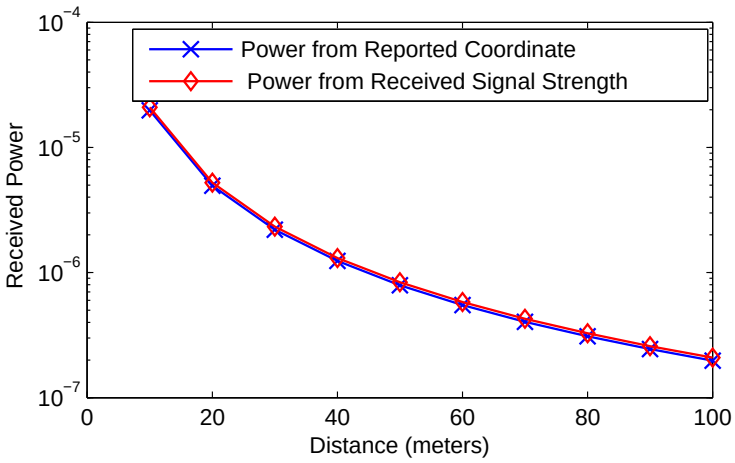


(c) TOA from secondary users.

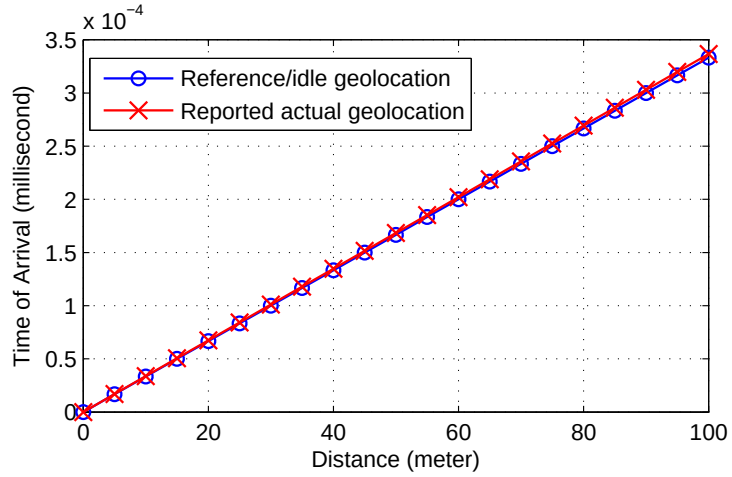
Figure 3.9: Variation of angle spectrum, received signal strength and time-of-arrival for a malicious secondary user for **Scenario 3**.



(a) Spectrum for θ_1 and θ_2.

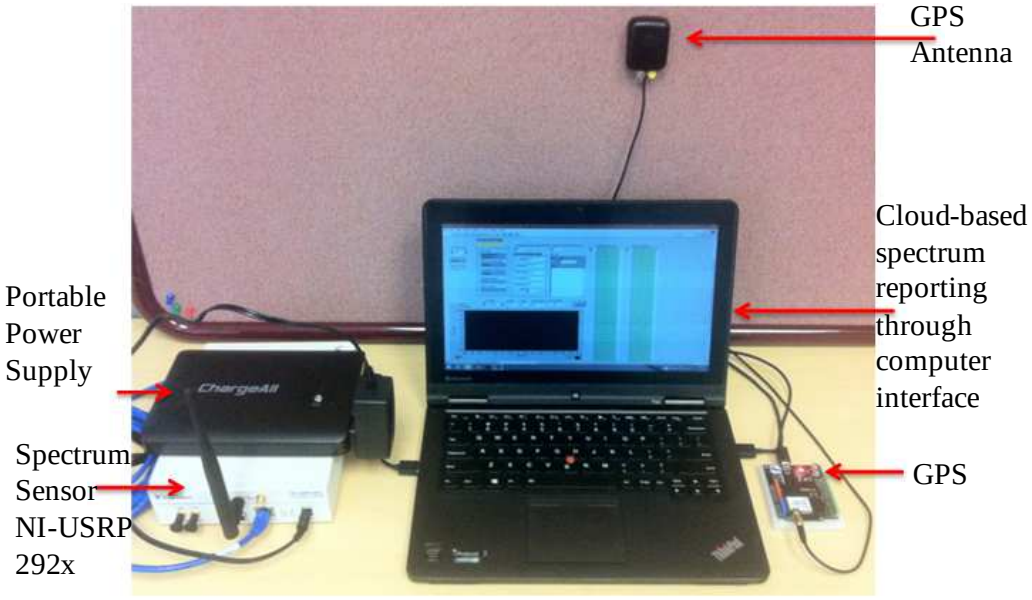


(b) Received signal strength vs distance.

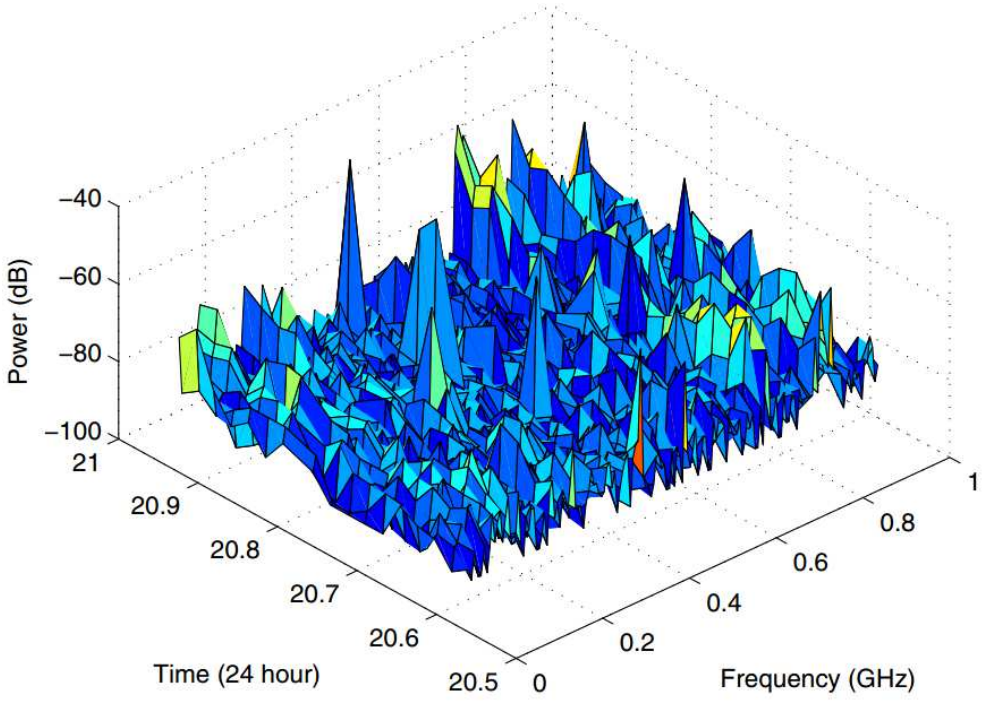


(c) TOA from secondary users.

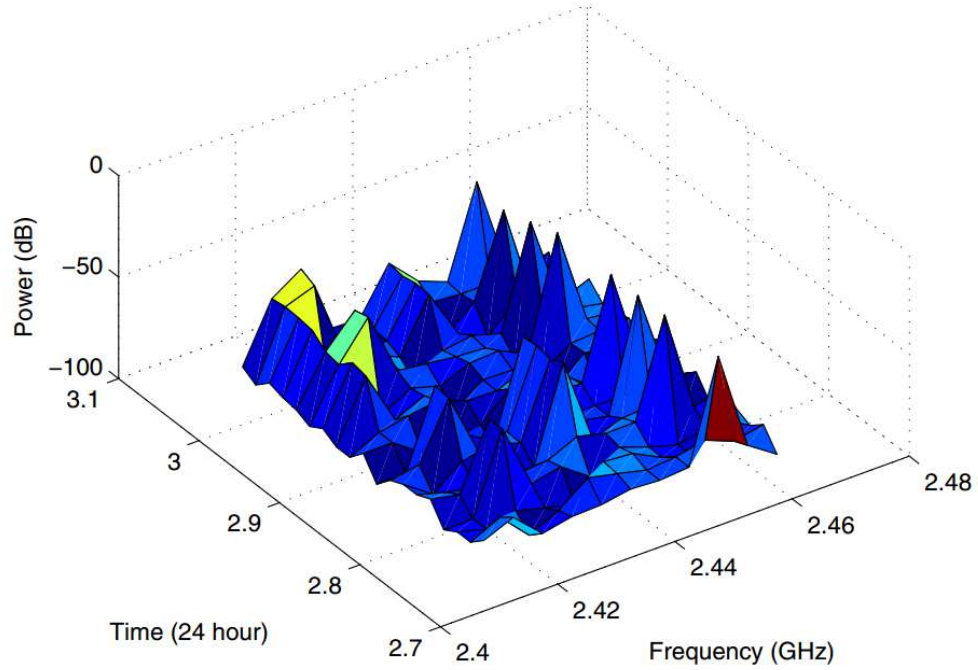
Figure 3.10: Variation of angle spectrum, received signal strength and time-of-arrival for a legitimate secondary user for **Scenario 4**.



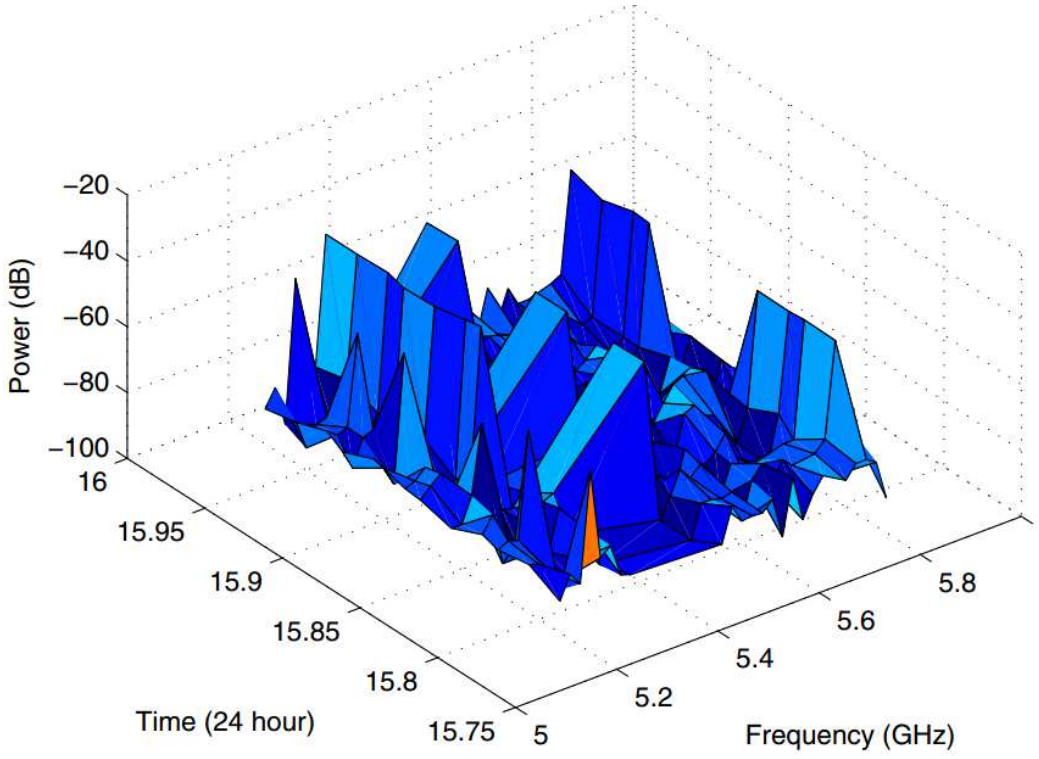
(a) Mobile RF Spectrum Sensor.



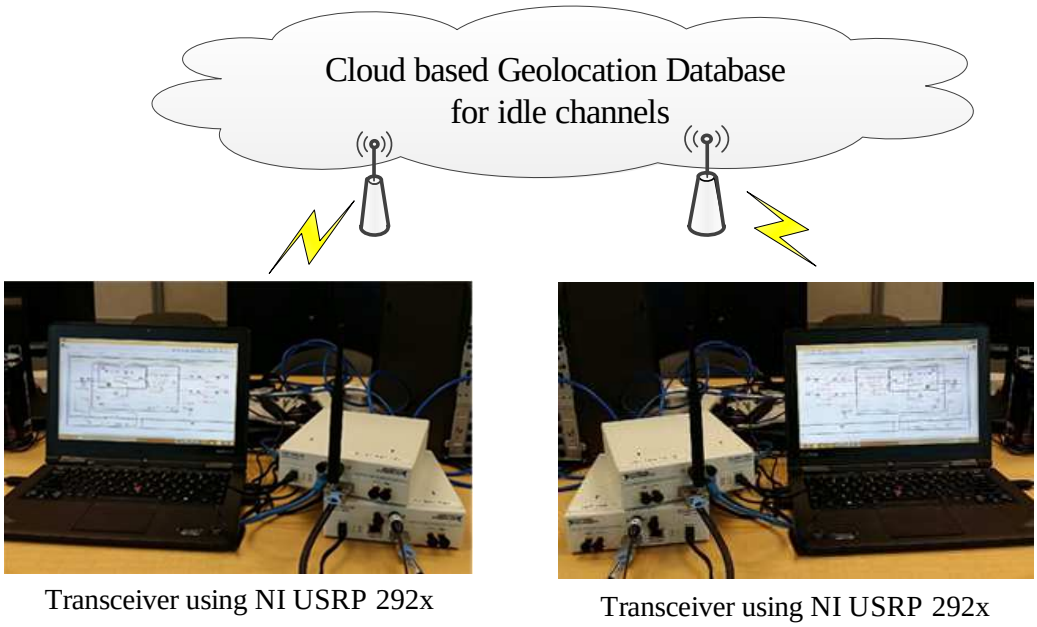
(b) Spectrum occupancy in 50MHz-1GHz.



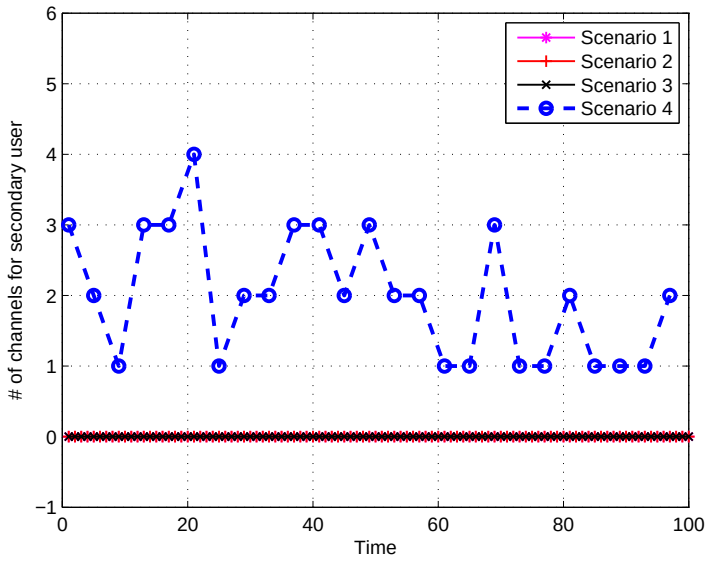
(c) Spectrum occupancy in Wi-Fi 2.4GHz.



(d) Spectrum occupancy in Wi-Fi 5GHz.



(e) Mobile transceivers using NI USRP 292x.



(f) No. of available channels.

Figure 3.11: Mobile transceivers (i.e., secondary users) and no. of available channels shown to secondary users for a given location and time for **Scenarios 1 – 4**. Only scenario 4 (legitimate one) has a list of channels for the secondary users but other scenarios (with fake locations) have 0 channels for the users.

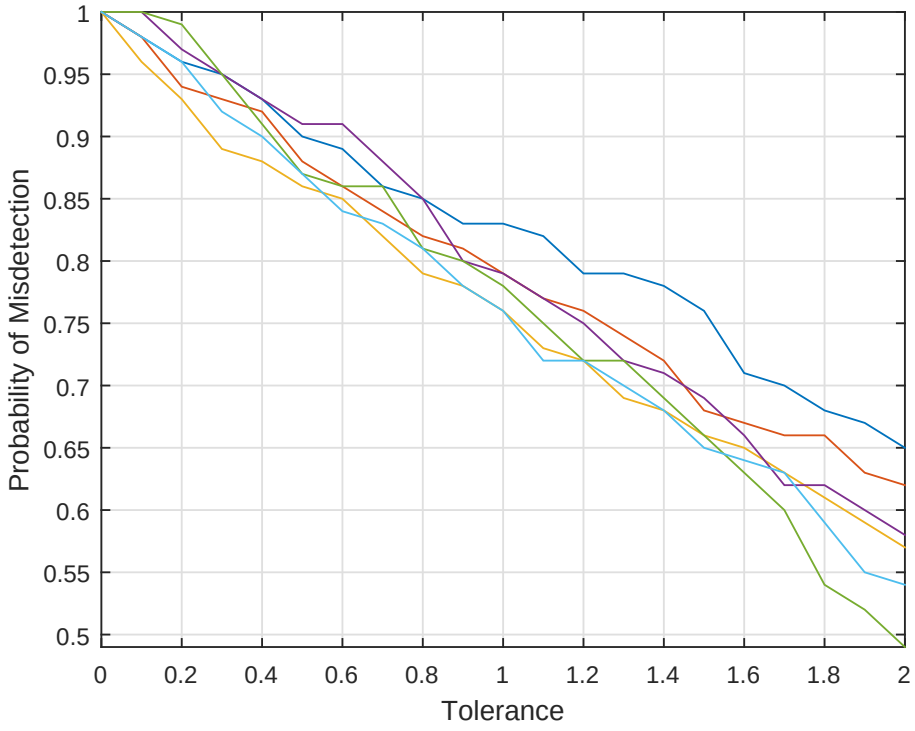


Figure 3.12: Probability Of Misdetection in Cloud Assisted Cognitive Radio Networks when the Tolerance is ranging from 0 to 2

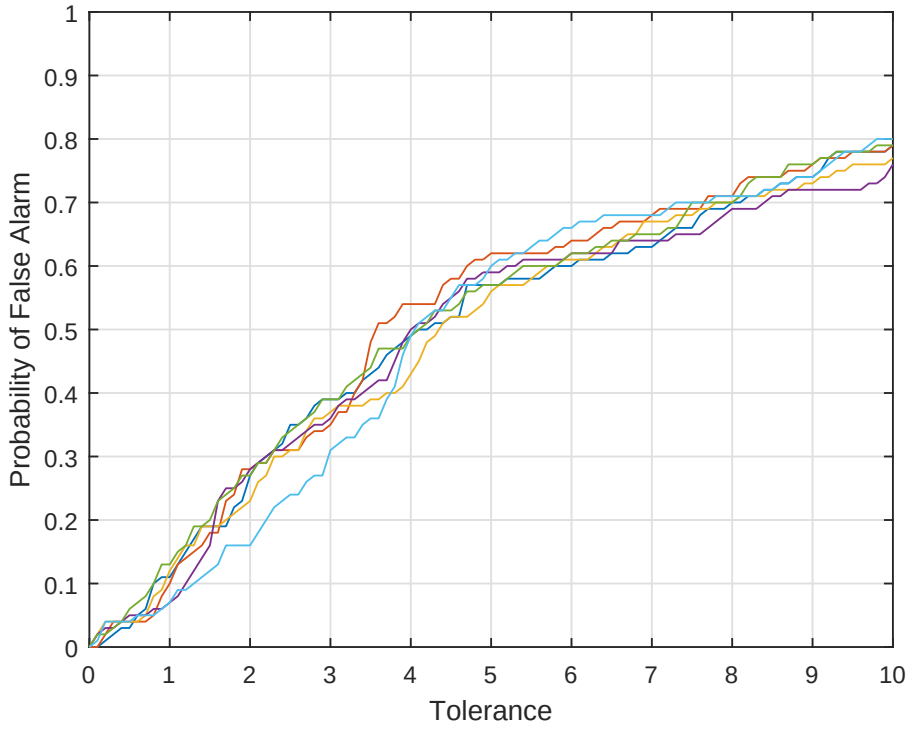


Figure 3.13: Probability Of False Alarm in Cloud Assisted Cognitive Radio Networks when the Tolerance is ranging from 0 to 10

shown in Figure 3.9(a) and received signal power matched with corresponding estimated values as shown in Figure 3.9 (b) respectively. However, estimated time of arrival is different from observed one as shown in Figure 3.9(c). This indicates that secondary user faked its location and power and thus is malicious.

Finally, the **Scenario 4** considers a legitimate scenario where a secondary user reports its legitimate geolocation while searching for idle channels. The variation of angle spectrum vs angle, received signal strength vs distance and time-of-arrival vs distance for a legitimate secondary user is represented in Figure 3.10(a), (b) and (c) respectively. In this case, angle of arrival, received signal power and time of arrival of the signal matches accurately. Hence, the user is assumed to be legitimate and granted access to the idle channels in the database.

Among these four scenarios, the given secondary user was able to get a list of idle channels only in **Scenario 4** as the secondary user was legitimate in Scenario 4. All other scenarios, the secondary user was faking location and/or power and was denied access to idle channels for opportunistic communications.

Further, all the above discussed scenarios are implemented on the real test bed designed for enabling opportunistic spectrum access to the legitimate secondary users. The geolocation database is designed for storing the idle channels. The idle channels information is obtained from the spectrum using the B200 GNU Radio, NI USRP 2920, 2921, 2932 devices that can function as spectrum sensors. The system assumes that there is no GPS spoofing during sensing process. Alternatively, primary infrastructures can provide authentic spectrum occupancy information to the cloud database. Then, RF spectrum sensor presented in Figure 3.4(a) is used to scan given range of frequency bands periodically and identify the idle bands based on energy detection. Here, the USRP is attached with GPS module to get the locations of idle channels. Geolocations of $idle$ channels were reported to the database. Sample spectrum occupancy information for 50 MHz to 1GHz, 2.4 GHz and 5GHz bands are shown in Figures. 3.4(b) and (c) respectively.

Then, the transmitter and receiver that function as secondary users were also designed using USRP 292x as shown in Figure 3.11(a). Then, the SU's send their geolocations to get list of channels available to their respective reported locations. All the four above mentioned scenarios are considered on the testbed. The experimental results confirmed the simulation results presented in Figures [3.6-3.9]. Figure 3.11(b) shows that the secondary users in legitimate **Scenario 4** are allowed to see the list of available channels and can choose the best one for opportunistic communications [67].

The probability of misdetection and false alarm scenarios are also evaluated using numerical simulations. Figure 3.12 represents the probability of misdetection vs tolerance. In this case, reference angle is considered as 75 degrees. Here, the tolerance ranges from 0 to 2 degrees. From the Figure 3.12, it is clear that the probability of user's getting misdetected or undetected is high in low tolerance level and decreases continuously with increase in tolerance value. The results were obtained considering some random values around the reference value.

Figure 3.13 represents probability of false alarm vs tolerance. The reference angle is considered as 75 degrees. The tolerance in this scenario is assumed to be ranging from 0 to 10 degrees to analyze the effect of false alarm at high tolerance ranges. The probability of false alarm is exponentially growing and reaches up to 0.8 at 10 degrees. This clearly shows that, at high tolerance level, the probability of false alarm will be greater.

3.5 Chapter Summary

The FCC mandated geolocation database approach was implemented in which secondary users search database to find idle channels to avoid channel sensing uncertainties. This chapter focused on proposing a solutions to spoofing attacks and measurement errors caused due to GPS. First, malicious secondary users is assumed to fake the location using GPS spoofing techniques and pretends to be in a place where more idle channels are available.

A three step mechanism that uses angle of arrival, received signal strength and time of arrival techniques was proposed to secure cloud based cognitive radio networks from malicious. The proposed approach was illustrated through simulations and experiments to check the legitimacy of geolocations reported by the secondary users before releasing any idle channels to them. From the obtained results,it is clear that the malicious secondary user who spoofed geolocation and/or transmit power was not able to receive any channels, however the legitimate secondary user was able to get a list of channels from database for opportunistic communications. Next, the probability of misdetection and probability of misdetection was also analyzed using numerical simulations. The results obtain depict that probability of misdetection and probability of false alarm can be reduced by setting the tolerance limit within a certain threshold value.

CHAPTER 4

OPTIMIZATION OF ENERGY EFFICIENCY USING NETWORK SOFTWARIZATION

In the previous chapters of thesis, the system model was designed using cloud computing for dynamic spectrum access of cognitive radio vehicular networks. Then, the three step mechanism was implemented in the system for securing it from location falsification attacks. However, the system design would be incomplete without optimizing the overall energy efficiency [34].

High energy consumption of networks is the major problem in many telecommunication infrastructures. With the advent of applications like big data, fortune 500 companies including telecommunication companies invested large portion of revenue to create data centers (DCs) for storing the information. It is estimated that the power consumed by the DCs alone accounted for 2 percent of the total power consumption in U.S. [68]. Moreover, the power consumption of networking infrastructures has increased from 420 TWh in 2008 to 616 TWh in 2013. By the end of 2025, it is expected to reach as high as 1140 TWh per year. The high power consumption of the network is a result of inefficient network management and poor resource management. However, the reports also estimated that using the present day smart networking technology, 65% of the total power savings can be achieved [69].

Therefore, softwarization of the network has gained large attention for simplifying the network management and lowering the cost. Softwarization of network can be done using Network Function Virtualization (NFV) or Software Defined Network (SDN). However, when the management of the network is the prime concern, SDN is the most viable option. SDN is regarded as the future networking paradigm which can adapt itself to support the advanced applications. In the beginning, SDN was implemented for the traffic management in data centers. It was able to reduce the operational expenses (OPEX) of data centers to a great extent without affecting the performance [70]. This paved away for SDN to branch

out its applications into various fields. Few notable areas where SDN was implemented includes cloud computing, network virtualization and LAN [71] [34].

In this chapter, softwarization method using SDN is incorporated in the system for optimizing the energy efficiency at the SUs base stations. The number of BSs required to serve the users is not same at all times because traffic density of SUs in the system varies continuously over a period of time. The conventional networking architectures donot support any techniques for flexible allocation of resources leading to the increase in power consumption of the network. Whereas, SDN based controller on the other hand can dynamically configure the BSs based on the number of users.

The remainder of the chapter is organized as follows: Related Work is discussed in Section 4.1. System model of the chapter is presented in Section 4.2. The simulation results are presented in Section 4.3 followed by conclusions in Section 4.4.

4.1 Related Work

4.1.1 History

The idea for development of SDN is not entirely new. It is the combination of ideas from the networking architectures proposed earlier [72]. Programmability in the networks was discussed in Active Networks. Programmable Switches and Capsule Model stand as examples for active networks [73]. The concept of network virtualization was obtained from the VINI and Tempest architectures [74]. The centralized control framework was discussed in Routing Control Platform Model [75]. 4D distributed architecture proposed in [76] divides the network into four planes i.e., decision plane, dissemination plane, discovery plane and data plane. The data plane and decision plane perform operations of forwarding the packets and managing the network respectively. The discovery plane monitors the link connections and dissemination plane enables smooth communication between these layers.

Ethane [77] and Open Flow [78] are also among the notable architecture that favored this innovation [34].

4.1.2 Architecture of SDN

SDN is a flexible architecture that simplified the network by decoupling data plane and control plane and managing them using a single centralized controller. The basic SDN architecture comprising of three different layers i.e, Infrastructure layer, Control layer and Application layer is represented in Figure 4.1. These layers communicate with each other using interfaces [79] [34].

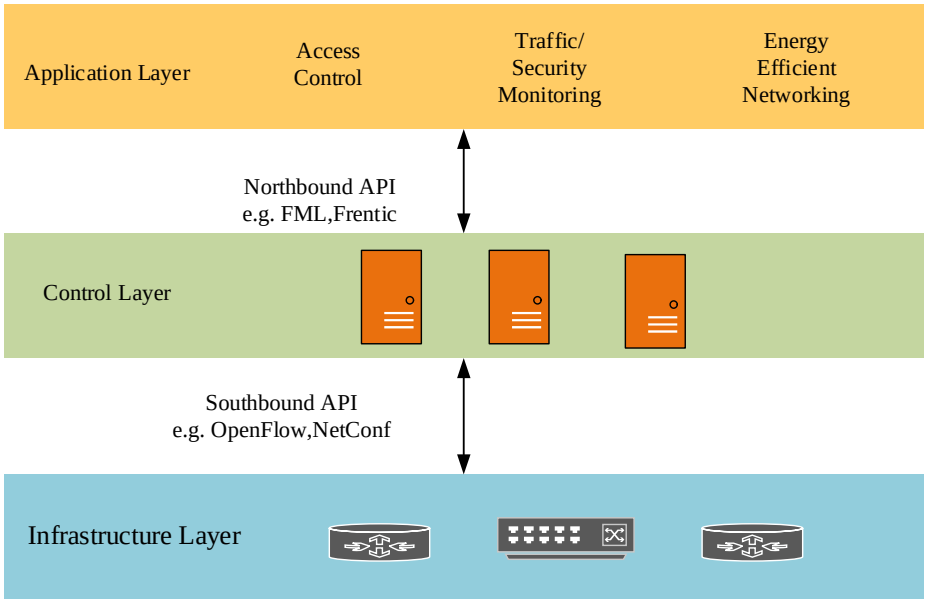


Figure 4.1: Architecture of SDN

Control Layer

The control layer consists of logically centralized controller that manages the entire network. The main functions of controller includes allocation of flow table rules to open flow switches,

configuration and updating the policies. FloodLight and NOX are examples of widely used SDN controllers.

Infrastructure Layer

The infrastructure layer (aka Data Layer) consists of hardware and software switches, which performs the task of forwarding the packets. The packet arrives into the network comprises of header that includes action to be performed, source and destination addresses. OpenFlow switches matches this action to the flow table entries provided by the controller and executes the operation. Open vSwitch, Pica8, HP and brocade are examples of some data plane switches.

Application layer

The application layer manages all the business related applications. It has a programmable API (Application Interface) through which administrator can modify the operations of networks based on the necessity.

Interfaces

- A-CPI: The communication between application layer and control layer is carried out by A-CPI (Application-Control Plane Interface) aka Northbound Interface. The most widely used northbound interface is FML and Frentic.
- D-CPI: The communication between infrastructure layer and control layer is carried out by D-CPI (Data-Control Plane Interface) or Southbound Interface. The most widely used southbound interface is OpenFlow.
- Eastbound and Westbound interfaces: There may be multiple controllers in the network to manage huge amount of traffic. These controllers communicate with the

master controller using eastbound and westbound interfaces.

4.1.3 Energy Efficient Methods in SDN

The different methods that are used in SDN for achieving the energy efficiency are summarized as follows:

Traffic Engineering

In this technique, the traffic in the network is dynamically routed into several paths for attaining proper link utilization. This technique that is mostly used in data centers. The authors in [80] proposed a method to reduce the energy consumption by opting the sleep awake mechanisms using Open Flow network (i.e, SDN). Mahout [81] and Hedera [82] are the other examples of traffic engineering methods.

Rule Placement

In this technique, rules in the network are modified reduce the energy consumption. Cache flow [83] and joint optimization [84] are the examples of this method.

Traffic monitoring

In this technique, the resources are allocated based on the traffic conditions prevailing in the network. This helps to improve the resource utilization in the network. The authors in [85] proposed a system model for software defined cloud computing framework for mobile cloud applications using traffic monitoring technique. The architecture is divided into four different layers i.e, user layer, application layer, control layer and physical layer. The system also comprises of various modules for handling specific functions in the network.

The functionality of important modules is summarized as follows:

- Admission Control: This module is responsible for enabling security in the system. It authorized the legitimacy of the users before providing admission into the network.
- Performance Modeler: This module analyzes the performance in the system that can be obtained by the addition of new module such as virtual machine.
- Energy Modeler: This modules is responsible for improving energy efficiency by providing the information regarding the energy consumed by each task in system

This paper was able to provide the awareness on the concept of using SDN in cloud computing. The decoupled structure implemented in system model of this thesis was borrowed from this paper.

4.2 System Model

The system model discussed in previous chapters assumes that CR enabled vehicular user (i.e, SU) continuously queries the geolocation database to find the idle channels in the particular route. The user is allocated with the suitable channel based on the location. Note that, the previous models do not include network softwarization in the system. Therefore, while managing the network using the conventional networks the base stations (BS) used by secondary users are completely turned on at all times irrelevant to the presence of the user. This increases the overall power consumption of the network thereby increasing the cost.

To overcome this issue the typical system model for softwarization of network using SDN is shown in Figure 4.2. As discussed earlier, SDN has a centralized control which makes it easy to manage the network. In Figure 4.2, all the primary BSs (i.e, carrier networks) in a certain geographical area are assumed to be controlled by single SDN controller. All these BSs are capable of allowing any user to connect to it. They have two modes of functionality i.e, idle mode and used mode. The BSs that has no active users

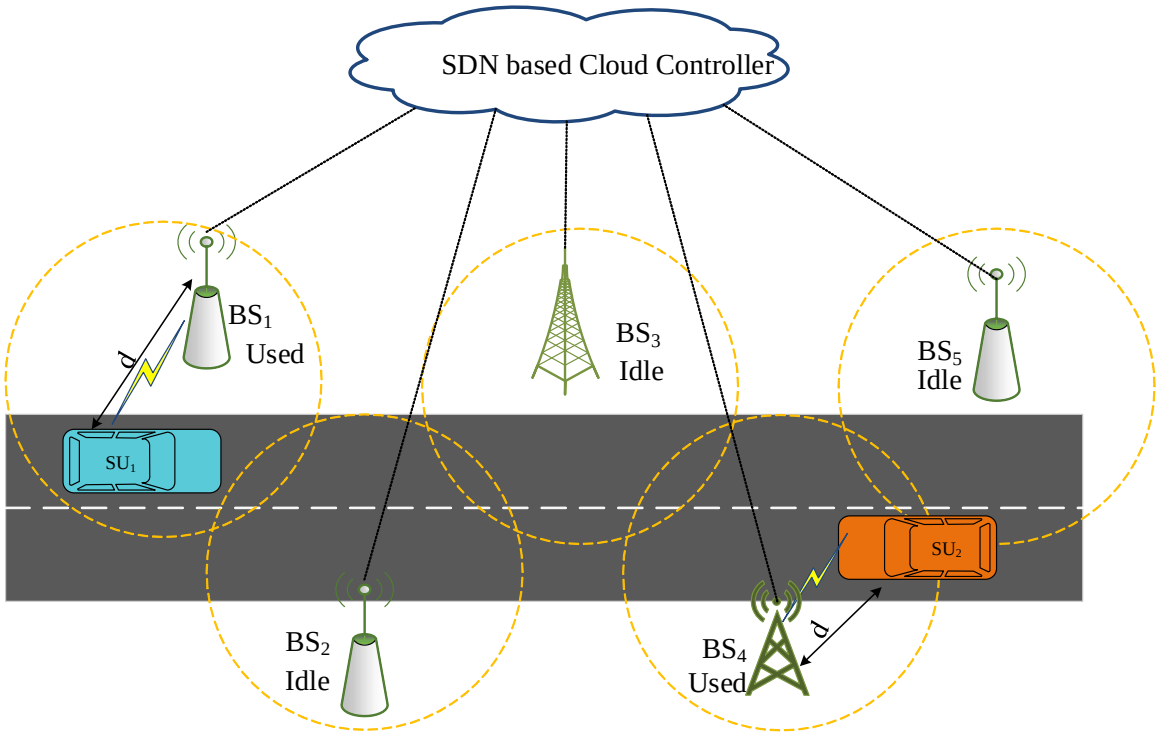


Figure 4.2: Typical System Model for Network Softwarization.

are placed in the idle mode (i.e, sleep mode) to reduce the power consumption and also increase the longevity. The BS with atleast one active user is kept in the used mode (i.e, active mode). These modes in BSs are continuously monitored and configured by SDN based on the presence of the users. Hence, power consumed by the base stations will not be same at all times.

The total power consumed by the K base stations is given by the equation

$$P_{total} = \sum_{i=0}^{K} P_i^{idle} + \sum_{i=0}^{K} L_i \alpha_i P_i^{used} \tag{4.1}$$

Here the P_i^{idle} represents the power consumed by BS in the idle state. P_i^{used} is the power consumed by the BS when the users are active. L_i is represents the number of active SUs

for a given BS. α_i represents the state of the BS.

$$\alpha_i = \begin{cases} 1, \text{for BS is sensing SU} \\ 0, \text{for BS is not sensing SU} \end{cases} \tag{4.2}$$

When the SU requests the idle channels from the database, suitable BS for serving the SU is calculated by SDN cloud controller based on the users location. For instance, for calculating the suitable BS for SU_1 distance and power received is used. From the Figure 4.2 BS_1 and BS_2 are the closest BSs to the SU_1. The distance of the SU_1 from the BS_1 is given as

$$d_1 = \sqrt{(x_1^s - x_1^b)^2 + (y_1^s - y_1^b)^2 + (z_1^s - z_1^b)^2} \tag{4.3}$$

In the eq. 4.3, (x_1^s, y_1^s, z_1^s) is the location reported by the SU_1 and (x_1^b, y_1^b, z_1^b) is the location of the first base station.

$$d_2 = \sqrt{(x_1^s - x_2^b)^2 + (y_1^s - y_2^b)^2 + (z_1^s - z_2^b)^2} \tag{4.4}$$

In the eq. 4.4, (x_1^s, y_1^s, z_1^s) is the location reported by the user and (x_2^b, y_2^b, z_2^b) is the location of the second base station.

The received power from the BS_1 is calculated using free space path loss equation is given as

$$P_{r_1} = P_t G_t G_r \frac{\lambda^2}{(4\pi d_1)^2} \tag{4.5}$$

The received power from the BS_2 is given as

$$P_{r_2} = P_t G_t G_r \frac{\lambda^2}{(4\pi d_2)^2} \tag{4.6}$$

Where, G_t,G_r are the transmitter and receiver gains.λ is the wavelength, P_t is the transmit power. d_1 and d_2 represents the distances of SU_1 from BS_1 and BS_2.

The BS selection by SDN based cloud controller for a given SU (say SU_1) is given as

$$BS_{SU_1} = \begin{cases} BS_1, \text{for } d_1 < d_2 \text{ OR } P_{r1} > P_{r2} \\ BS_1, \text{for } d_1 > d_2 \text{ OR } P_{r1} > P_{r2} \\ BS_2, \text{for } d_2 < d_1 \text{ OR } P_{r2} > P_{r1} \\ BS_2, \text{for } d_2 > d_1 \text{ OR } P_{r2} > P_{r1} \end{cases} \tag{4.7}$$

From eq. 4.7, it is clear that, the BS with less distance and high transmit power is considered to be the suitable BS. However, received power P_r has high priority over the distance because even though the base station is located closer if the received signal strength is weak then, the user will obtain low QoS. Provided that, BS_1 is most suitable for the communication of SU_1. Later, when the SU user is no longer within the coverage area of the BS_1, the mode of BS_1 changes from used mode to idle mode. This process is continuously repeated for other BSs in the system which helps to achieve energy efficiency.

4.3 Simulation And Numerical Results

The number of BSs in the system are considered as $K = 5$ and it is assumed that each base station covers a distance of $2km$. The power consumed by the BS in active mode and idle mode are considered as $P_i^{used} = 1w$ and $P_i^{idle} = 10mw$ respectively.

First, Figure 4.3 represents the distance d vs total power P_t. In this scenario, it is assumed that there is only a single SU user travelling from point A to point B. Figure 4.3 depicts that the total power P_t consumed by the BSs in conventional network is constant $5W$ because all the BSs are operating with full power. Whereas, the total power P_t consumed by the SDN based BSs is significantly low compared to conventional networks. In SDN, only the BS closest to the SU is operating with full power i.e, $P_i^{used} = 1w$ and other BSs are operating with idle power $P_i^{idle} = 10mw$. Hence, from the Figure 4.3 it is clear that, SDN is highly efficient in reducing the power consumption.

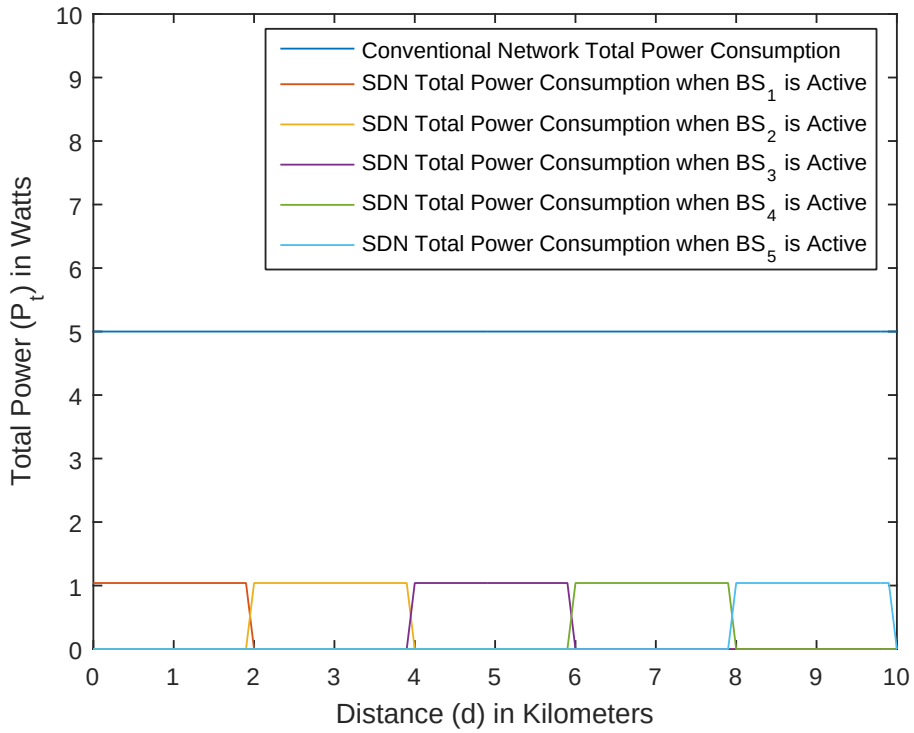


Figure 4.3: Conventional Network Power Consumption vs Software Defined Network Power Consumption

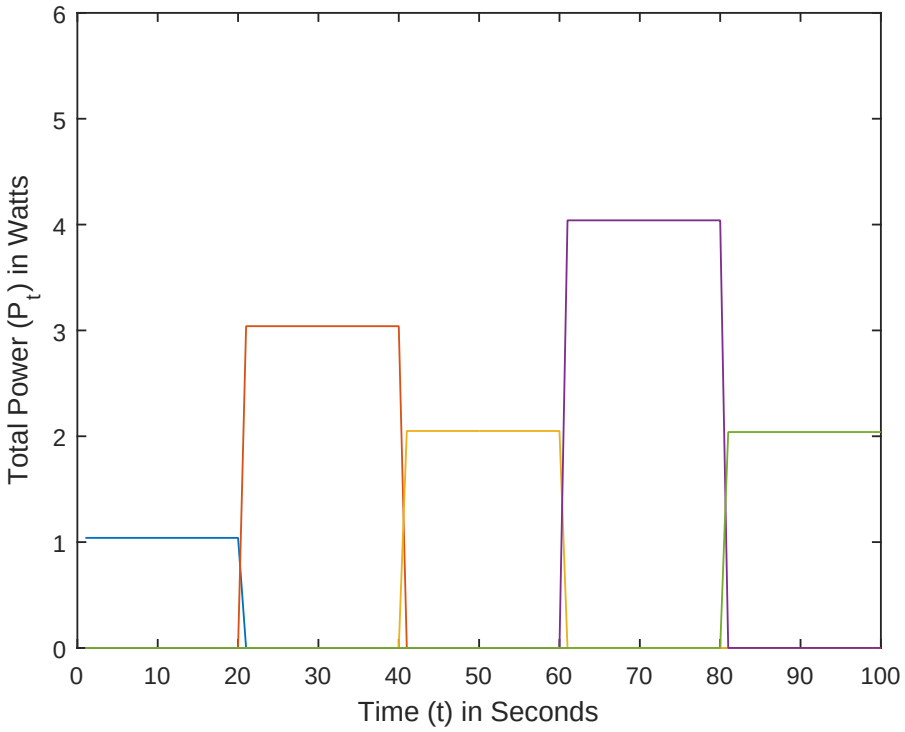


Figure 4.4: Total Power Consumption at BS_1 with varying number of SUs.

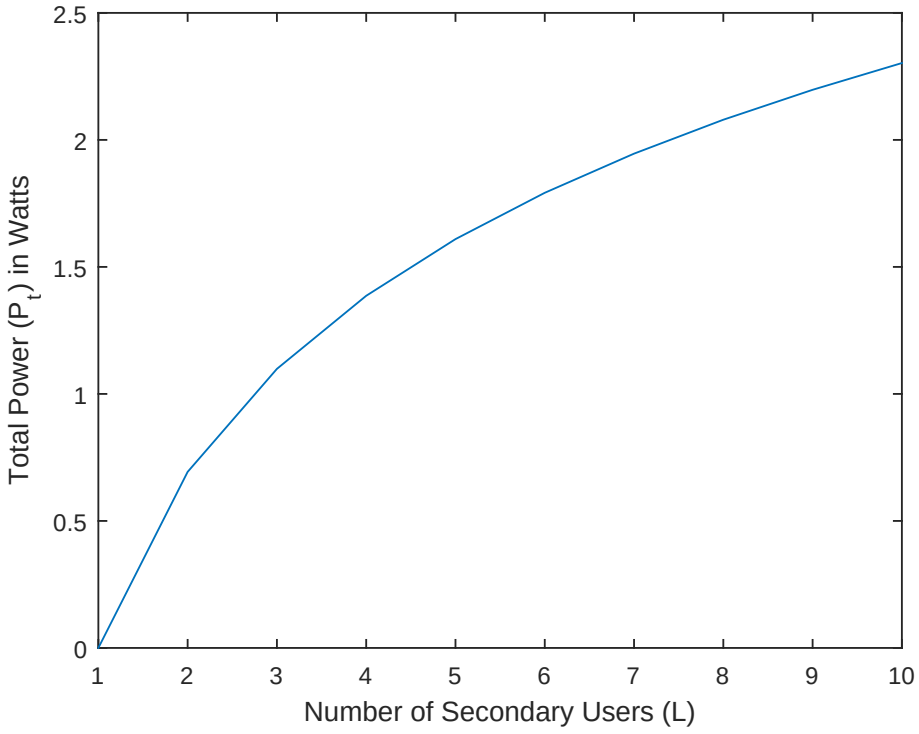


Figure 4.5: Total Power Consumption (P_t) vs Number of Users (L).

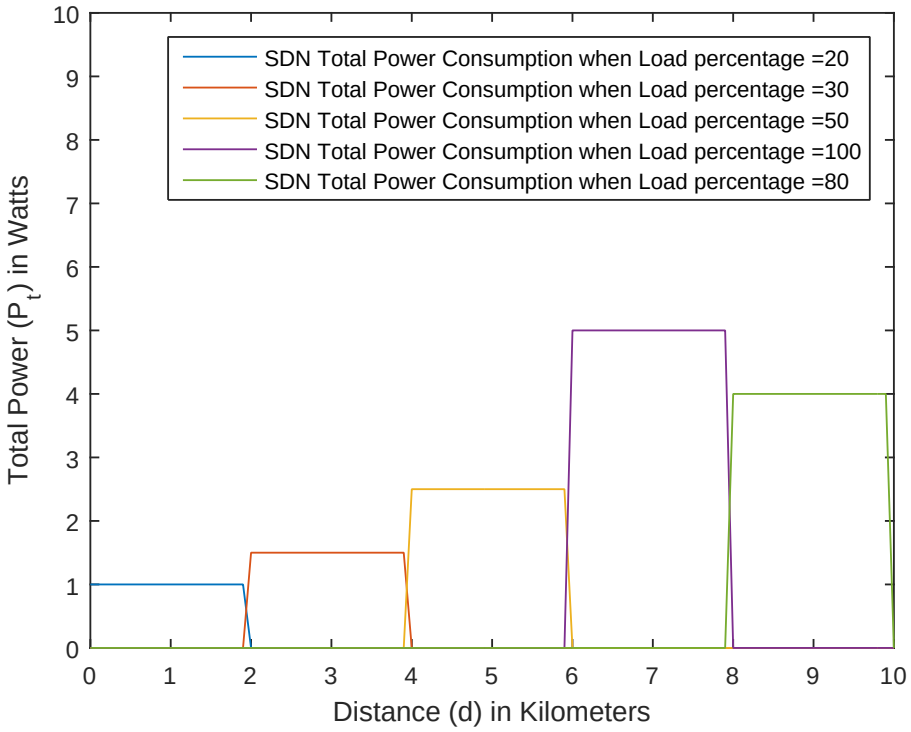


Figure 4.6: Total power consumed at all the BSs with varying load percentages

In Figure 4.4, the power consumption of the BS_1 with varying number of users is considered. The distance covered by the BS_1 is assumed to be $2km$. The power consumption of the base station is not constant and is fluctuating rapidly based on the number of active SUs at different times. For instance, the number of active users are greater at $60 - 80seconds$. Hence, power consumed by the BS_1 is highest at that time.

Next, Figure 4.5 represents the number of SUs vs total power consumption P_t in the entire system. From the Figure 4.5, it is clear that the total power consumed is dependent on the number of users present in the system. For instance, if the SU_1 is located near BS_1 and the SU_2 is located close to BS_5. Both the BSs should be operated with full power $P_i^{used} = 1w$ for providing service to the users. This increases the overall power consumption as shown in Figure 4.5.

The Figure 4.6 depicts the power consumed at all the BSs located within the area of $10km$. Each BS might not be able to handle same number of users. It is dependent on number of antennas present in the BS. From the Figure 4.6, the power consumed is greatly dependent on the load percentage at each BS. For instance, the highest power is consumed at the BS_4 because the load percentage is 100%.

4.4 Chapter Summary

In this chapter, the problem of high energy consumption in cloud based CRN is discussed in detail. Then, the system model for network softwarization using SDN is presented to address this issue of high energy consumption. SDN incorporated in the system uses smart management techniques for achieving the energy efficiency through softwarization of network. The proposed system assumes that all the secondary user base stations are configured to exhibit two modes of operation i.e., idle mode and used mode. The BS usually exhibits idle mode and the used mode is activated only when there is atleast one active user. The power consumed by the base stations in different scenarios is analyzed

using simulations. The obtained results depict that network softwarization through SDN can significantly lower the power consumption in the network. Since, power consumed by the BSs is dependent on the number of active users, the power consumption increases with increase in the users.

CHAPTER 5

CONCLUSIONS, DISCUSSIONS AND FUTURE WORK

Increasing accidents in the U.S. has motivated the development of vehicular networks. FCC dedicated IEEE 802.11p standard is not very efficient in the crowded areas. Alternatively, cognitive radio technology is implemented in vehicles to resolve this issue. In first chapter 1, the introduction of overall system is provided using a complete system model diagram to provide an idea of the topic. Further, detailed explanation of the system functionality is explained in multiple chapters.

In chapter 2, a cloud-assisted cognitive radio framework for allowing DSA in vehicular networks is proposed. In this framework, geolocation database stores the idle channel information reported by primary infrastructures. The CR enabled vehicular user (i.e, SU) equipped with GPS, reports its location to the database and queries it periodically to find idle channels in the reported location. In the system, PU user is given highest priority and SU should adapt accordingly to the activities of the PU. For, instance if the PU becomes active in the channel currently being used by the SU, then SU immediately hops to the next available channel to avoid any interference to the PU. Various activities of the PU that show its impact on the geolocation database is analyzed using simulations. To begin with, the scenario of the SU switching back and forth between the DSRC and Wi-Fi channels is represented in Figure 2.4. Next, Figure 2.5 represents a scenario where the data rate obtained by the SU is decreasing with the increase in the probability of the PU being present in the system. Moreover, the data rate is divided multiple SUs present in the system. Higher the number of SU's lower the data rate obtained by each user is shown in Figure 2.6. Then, the Figure 2.7 and Figure 2.8 shows that the transmission count is directly proportional to the transmission failure probability and expected transmission time. Furthermore, the analysis presented in Figure 2.9 and Figure 2.10 shows that data size and data rate have an impact on the transmission time. When the data rate is high, then the transmission time decreases

and when the data size increases the transmission time also increases.

A system model for securing the dynamic spectrum access of SUs from location falsification attacks in cloud based cognitive radio networks is discussed in chapter 3. First, the two attack scenarios of location falsification attacks in cloud based CRN is presented. Next, the three step mechanism that uses angle of arrival, time of arrival and received signal strength is proposed for detecting the malicious users in those two attack scenarios. Then, the proposed technique is evaluated in four scenarios using simulations. Among all the four cases only the user in the scenario 4 represented in Figure 3.10 is assumed to be legitimate. All these scenarios are tested on the real testbed created using USRP 2920 and 2921. Further, the probability of misdetection and probability of false alarm caused due to errors in GPS is also evaluated using simulations presented in Figure 3.7 and Figure 3.12. From the obtained results, it is clear tolerance level of the user's angle should be limited within certain threshold to reduce the probability of misdetection and probability of false alarm in the system.

In chapter 4, a system model for network softwarization using SDN is presented. In this system, the SDN controller is responsible for the managing all the BSs and uses sleep and awake mechanisms in BSs for reducing the power consumption. Further, the power consumption of the network in the various scenarios is evaluated using simulations. Figure 4.3 shows that power consumption of the SDN is relatively lower than the power consumption of the conventional network. From the Figures 4.4, 4.5, 4.6, it is evident the power consumption of the BSs is proportional to the number of active users in the system.

5.1 Future Work

The thesis mainly focused on three main objectives i.e, creating a cloud-based DSA for vehicular networks, securing the system from GPS spoofing attacks and optimizing the energy efficiency of the system. However, they are still many issues that are prevailing

in the system. For instance, the thesis only considers to secure the system from location falsification attacks. Whereas, cloud based CRN are prone to several other attacks such as jamming and DoS. The future research should be focused on the developing a highly secure system that defends itself from all types of attacks and provides high performance to the vehicular CR users. Moreover, while developing the security mechanisms the power consumption of the system should also be considered so that the security mechanisms implemented doesnot impose any cost overheads.

REFERENCES

[1] P. K. Sahoo, M.-J. Chiang, and S.-L. Wu, "SVANET: A Smart Vehicular Ad Hoc Network for Efficient Data Transmission with Wireless Sensors," *Sensors*, vol. 14, no. 12, pp. 22 230–22 260, 2014.

[2] "Interference Management in Cognitive Radio Networks," http://www.gonzalo-vazquez-vilar.eu/cognitive-radio.html., Accessed: 2016-02-23.

[3] "Fatality Analysis Reporting System," http://www.nhtsa.gov/FARS, accessed: 2016-02-23.

[4] "Auto Crashes," http://www.iii.org/issue-update/auto-crashes, accessed: 2016-02-23.

[5] "Annual United States Road Crash Statistics," http://asirt.org/initiatives/informing-road-users/road-safety-facts/road-crash-statistics, accessed: 2016-02-23.

[6] S. Singh, "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey," National Motor Vehicle Crash Causation Survey, Tech. Rep., 2015.

[7] "Reasons Why Teenagers and Older People Are the Riskiest Drivers". Accessed: 2016-02-23. [Online]. Available: http://www.consumerreports.org/cro/magazine/2012/10/teenagers-and-older-people-are-the-riskiest-drivers/index.htm

[8] (2016, Feb) "Crash Avoidance Features". [Online]. Available: http://www.iihs.org/iihs/ratings/crash-avoidance-features

[9] "Google Self-Driving Car Project," https://www.google.com/selfdrivingcar/, accessed: 2016-02-23.

[10] Autonomous Cars Pros and Cons. Accessed: 2016-02-23. [Online]. Available: https://sites.google.com/site/unibathautonomouscars/services

[11] G. Yan, D. B. Rawat, and B. B. Bista, "Provisioning vehicular ad hoc networks with quality of service," *Proceedings of International Journal of Space-Based and Situated Computing*, vol. 2, no. 2, pp. 104–111, 2012.

[12] D. B. Rawat, Y. Zhao, G. Yan, and M. Song, "CRAVE: Cognitive radio enabled vehicular communications in heterogeneous networks," in *Proceedings of 2013 IEEE Radio and Wireless Symposium (RWS)*, 2013, pp. 190–192.

[13] D. B. Rawat and S. Shetty, "Enhancing connectivity for spectrum-agile vehicular ad hoc networks in fading channels," in *Proceedings of 2014 IEEE Intelligent Vehicles Symposium Proceedings*, 2014, pp. 957–962.

[14] D. B. Rawat, B. B. Bista, G. Yan, and S. Olariu, "Vehicle-to-vehicle connectivity and communication framework for vehicular ad-hoc networks," in *Proceedings of 2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, 2014, pp. 44–49.

[15] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *Proceedings of IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[16] D. B. Rawat, J. J. Rodrigues, and I. Stojmenovic, *Cyber-Physical Systems: From Theory to Practice*. CRC Press, 2015.

[17] "Intro to Vehicular Networks ," http://www.cs.odu.edu/ mweigle/courses/cs795-s07/lectures/1-Intro-VANET.pdf, Accessed: 2016-02-23.

[18] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust On the Security of Wireless Vehicular Ad-hoc Networking." *Ad Hoc & Sensor Wireless Networks*, vol. 24, no. 3-4, pp. 283–305, 2015.

[19] D. B. Rawat, B. B. Bista, G. Yan, and M. C. Weigle, "Securing vehicular ad-hoc networks against malicious drivers: a probabilistic approach," in *Proceedings of 2011 International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, 2011, pp. 146–151.

[20] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[21] T. S. Rappaport, "Wireless Communications Principles and Practice, (The Book End)," *Microwave Journal*, vol. 45, no. 12, pp. 128–129, 2002.

[22] D. B. Rawat, C. Bajracharya, and G. Yan, "Towards intelligent transportation Cyber-Physical Systems: Real-time computing and communications perspectives," in *Proceedings of IEEE SoutheastCon 2015*, 2015, pp. 1–6.

[23] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015-2020 White Paper," http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html, accessed: 2016-02-23.

[24] S. Sengupta, "DSA enabled Cognitive Radio Networking for First Responders Critical Networks," *Dept. of Mathematics and Computer Science John Jay College of Criminal Justice New York, NY*, vol. 10019, 2010.

[25] J. Mitola III and G. Q. Maguire Jr, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[26] M. Song, C. Xin, Y. Zhao, and X. Cheng, "Dynamic spectrum access: from cognitive radio to network radio," *IEEE Wireless Communications*, vol. 19, no. 1, pp. 23–29, 2012.

[27] F. C. Commission *et al.*, "Second memorandum opinion and order in the matter of unlicensed operation in the tv broadcast bands and additional spectrum for unlicensed devices below 900 mhz and in the 3 ghz band," *Washington, September*, 2010.

[28] D. B. Rawat, S. Shetty, and K. Raza, "Geolocation-aware resource management in cloud computing-based cognitive radio networks," *International Journal of Cloud Computing*, vol. 3, no. 3, pp. 267–287, 2014.

[29] D. B. Rawat, M. Song, and S. Shetty, "Dynamic Spectrum Access for Wireless Networks," *SpringerBriefs*, 2015.

[30] ©[2015] IEEE. Reprinted, with permission, from [S. Reddy, I. Cushman, D. B. Rawat, M. Song, "Securing real-time opportunistic spectrum access in cognitive networks against malicious secondary users," in *Proceedings of IEEE GLOBECOM Workshop on Security, Privacy, and Forensics in Wireless Mobile Ad Hoc Networks and Wireless Sensor Networks*, pp. 1–6, Dec. 6 - 10,2015].

[31] D. B. Rawat, "ROAR: An Architecture for Real-time Opportunistic Spectrum Access in Cloud-assisted Cognitive Radio Networks," in *Proceedings of 13th Annual IEEE Consumer Communications & Networking Conference (IEEE CCNC 2016).*, 2016, pp. 943–948.

[32] R. Buyya, R. N. Calheiros, J. Son, A. V. Dastjerdi, and Y. Yoon, "Software-defined cloud computing: Architectural elements and open challenges," in *Proceedings of 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2014, pp. 1–12.

[33] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. De Rose, and R. Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Proceedings of Software: Practice and Experience*, vol. 41, no. 1, pp. 23–50, 2011.

[34] D. B. Rawat and S.Reddy, "Recent Advances in Software Defined Wireless Networks," in *2016 IEEE SoutheastCon*. ©IEEE, 2016.

[35] D. B. Rawat, S. Shetty, and M. Song, *Adaptive Resource Allocation in Cognitive Radio Networks*. Springer, 2015.

[36] ©[2015] IEEE. Reprinted, with permission, from [D.B. Rawat, S. Reddy, N. Sharma, B. B. Bista, S. Shetty, "Cloud-assisted gps-driven dynamic spectrum access in cognitive radio vehicular networks for transportation cyber physical systems," in *Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (IEEE WCNC 2015)*, pp. 1942–1947, 2015].

[37] ©[2016] IEEE. Reprinted, with permission, from [S. Reddy and D.B. Rawat, "Evaluating misdetection and false alarm in securing cloud assisted cognitive radio networks," *Under Review in International Journal of Monitoring and Surveillance Technologies Research (IJMSTR)*, 2016].

[38] D. B. Rawat, S. Shetty, and C. Xin, "Stackelberg-Game-Based Dynamic Spectrum Access in Heterogeneous Wireless Systems," *IEEE Systems Journal*, 2014.

[39] D. B. Rawat and S. Shetty, "Game theoretic approach to dynamic spectrum access with multi-radio and QoS requirements," in *Proceedings of 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2013, pp. 1150–1153.

[40] R. Doost-Mohammady and K. R. Chowdhury, "Design of spectrum database assisted cognitive radio vehicular networks," in *Proceedings of 2012 7th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, 2012, pp. 1–5.

[41] D. B. Rawat, D. C. Popescu, G. Yan, and S. Olariu, "Enhancing VANET performance by joint adaptation of transmission power and contention window size," *Proceedings of*

IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 9, pp. 1528–1535, 2011.

[42] D. B. Rawat, G. Yan, D. C. Popescu, M. C. Weigle, and S. Olariu, "Dynamic adaptation of joint transmission power and contention window in VANET," in *Proceedings of 2009 IEEE 70th Vehicular Technology Conference Fall (VTC 2009-Fall)*, 2009, pp. 1–5.

[43] D. B. Rawat, B. B. Bista, and G. Yan, "CoR-VANETs: Game theoretic approach for channel and rate selection in cognitive radio VANETs," in *Proceedings of 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA)*, 2012, pp. 94–99.

[44] S. Chen, R. Vuyyuru, O. Altintas, and A. M. Wyglinski, "On optimizing vehicular dynamic spectrum access networks: automation and learning in mobile wireless environments," in *2011 IEEE Vehicular Networking Conference (VNC)*, 2011, pp. 39–46.

[45] T. Jiang, Z. Wang, L. Zhang, D. Qu, and Y.-C. Liang, "Efficient spectrum utilization on tv band for cognitive radio based high speed vehicle network," *Proceedings of IEEE Transactions on Wireless Communications*, vol. 13, no. 10, pp. 5319–5329, 2014.

[46] "Riak," http://basho.com/riak/, accessed: 2014-08-10.

[47] "Cassandra," http://cassandra.apache.org/, accessed: 2014-08-10.

[48] "Memcached," http://memcached.org/, accessed: 2014-08-10.

[49] "Storm Cassandra Integration," https://github.com/, accessed: 2014-08-10.

[50] "FCC Release 2011," http://www.fcc.gov/DailyReleases/DailyBusiness/2011/db0126/DA-11-131A1.pdf, accessed: 2014-08-10.

[51] S. Geirhofer, L. Tong, and B. M. Sadler, "Cognitive medium access: constraining interference based on experimental models," *Proceedings of IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 95–105, 2008.

[52] S. Song, K. Hamdi, and K. B. Letaief, "Spectrum sensing with active cognitive systems," *IEEE Transactions on Wireless Communications*, vol. 9, no. 6, pp. 1849–1854, 2010.

[53] D. S. De, D. S. Couto, D. Aguayo, R. Morris, and J. Bicket, "A high-throughput path metric for multi-hop wireless routing," *Proceedings of 2003 9th International Conference on Mobile Computing and Networking*, 2003.

[54] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Proceedings of International Journal of Navigation and Observation*, vol. 2012, 2012.

[55] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 75–86.

[56] G. Yan, B. B. Bista, D. B. Rawat, and E. F. Shaner, "General active position detectors protect VANET security," in *Proceedings of 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, 2011, pp. 11–17.

[57] (2016, Feb) GPS Accuracy, Errors & Precision. [Online]. Available: http://www.radio-electronics.com/info/satellite/gps/signals.php

[58] (2016, Mar) GPS Tutorial Error Correction. [Online]. Available: http://www.trimble.com/gps_tutorial/howgps-error2.aspx

[59] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *Proceedings of 2013 Proceedings IEEE INFOCOM*, 2013, pp. 2751–2759.

[60] K. Zeng, S. Kondaji Ramesh, and Y. Yang, "Location spoofing attack and its countermeasures in database-driven cognitive radio networks," in *Proceedings of 2014 IEEE Conference on Communications and Network Security (CNS)*, 2014, pp. 202–210.

[61] A. Badawy, T. Khattab, D. Trinchero, T. M. Elfouly, and A. Mohamed, "A Simple AoA Estimation Scheme," *CoRR*, vol. abs/1409.5744, 2014. [Online]. Available: http://arxiv.org/abs/1409.5744

[62] T. Orul and E. Afacan, "Estimation of Direction of Arrival Algorithms," *Session 3P6 SC4: Active Antennas, MIMO and Beamforming Systems*, p. 1182, 2013.

[63] R. O. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation*, vol. 34, no. 3, pp. 276–280, 1986.

[64] T. S. Dhope, "Application of MUSIC, ESPRIT and ROOT MUSIC in DOA Estimation," *Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia*, 2010.

[65] S. S. Balabadrapatruni, "Performance Evaluation Of Direction Of Arrival Estimation Using Matlab," *Proceedings of Signal & Image Processing: An International Journal (SIPIJ) Vol*, vol. 3, 2012.

[66] D. Rick, "Deriving the haversine formula," in *The Math Forum, April*, 1999.

[67] N. Sharma, D. B. Rawat, B. B. Bista, and S. Shetty, "A Testbed Using USRP (TM) and LabView (R) for Dynamic Spectrum Access in Cognitive Radio Networks," in *Proceedings of 2015 IEEE 29th International Conference on Advanced Information Networking and Applications (AINA)*, 2015, pp. 735–740.

[68] "SDN & NFV for energy-efficient clouds," http://www.all4green-project.eu/sites/default/files/workshop/workshop2/session3/E2DC_workshop_2013_Kolias_to_present_final.pdf, accessed: 2016-02-23.

[69] More Data, Less Energy: Making Network Standby More Efficient in Billions of Connected Devices. https://www.iea.org/publications/freepublications/publication/MoreData_LessEnergy.pdf. Accessed : 2016-02-23.

[70] L. Velasco, A. Asensio, A. Castro, J. L. Berral, D. Carrera, V. López, and J. P. FernaÌĄndez-Palacios, "Cross-stratum orchestration and flexgrid optical networks for data center federations," *Proceedings of IEEE Network*, vol. 27, no. 6, pp. 23–30, 2013.

[71] T. D. Nadeau and K. Gray, *SDN: software defined networks*. O'Reilly Media, Inc., 2013.

[72] N. Feamster, J. Rexford, and E. Zegura, "The road to SDN," *Queue*, vol. 11, no. 12, p. 20, 2013.

[73] S. Bhattacharjee, K. L. Calvert, and E. W. Zegura, *An architecture for active networking*. Springer, 1997.

[74] A. Bavier, N. Feamster, M. Huang, L. Peterson, and J. Rexford, "In VINI veritas: realistic and controlled network experimentation," in *Proceedings of ACM SIGCOMM Computer Communication Review*, vol. 36, no. 4, 2006, pp. 3–14.

[75] N. Feamster, H. Balakrishnan, J. Rexford, A. Shaikh, and J. Van Der Merwe, "The case for separating routing from routers," in *Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture*, 2004, pp. 5–12.

[76] H. Iqbal and T. Znati, "Distributed control plane for 4D architecture," in *Proceedings of 2007 Global Telecommunications Conference*, 2007, pp. 1901–1905.

[77] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: Taking control of the enterprise," in *Proceedings of ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, 2007, pp. 1–12.

[78] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[79] B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, T. Turletti *et al.*, "A survey of software-defined networking: Past, present, and future of programmable networks," *Proceedings of IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.

[80] B. B. Bista, M. Takanohashi, T. Takata, and D. Rawat, "A Power Saving Scheme for Open Flow Network," *Journal of Clean Energy Technologies*, vol. 1, no. 4, pp. 276–280, 2013.

[81] A. R. Curtis, W. Kim, and P. Yalagandula, "Mahout: Low-overhead datacenter traffic management using end-host-based elephant detection," in *Proceedings of 2011F IEEE INFOCOM*, 2011, pp. 1629–1637.

[82] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, and A. Vahdat, "Hedera: Dynamic Flow Scheduling for Data Center Networks." in *NSDI*, vol. 10, 2010, pp. 19–19.

[83] N. Katta, O. Alipourfard, J. Rexford, and D. Walker, "Infinite cacheflow in software-defined networks," in *Proceedings of the third workshop on Hot topics in software defined networking*, 2014, pp. 175–180.

[84] H. Huang, P. Li, S. Guo, and B. Ye, "The joint optimization of rules allocation and traffic engineering in Software Defined Network," in *Proceedings of 2014 IEEE 22nd International Symposium of Quality of Service (IWQoS)*, 2014, pp. 141–146.

[85] A. Galis, S. Clayman, L. Mamatas, J. Rubio Loyola, A. Manzalini, S. Kuklinski, J. Serrat, and T. Zahariadis, "Softwarization of future networks and services-programmable enabled networks as next generation software defined networks," in *Proceedings of 2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, 2013, pp. 1–7.