International Journal in Management and Social Science
Volume 09 Issue 11, November 2021 ISSN: 2321-1784 Impact Factor: 7.088
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

EFFECT OF SPECTRUM ON COGNITIVE RADIO NETWORKS

NAADIR KAMAL,
Research Scholar, Dr. A.P.J Abdul Kalam University, Indore

DR. AMOL KUMBHARE
Research Supervisor, Dr. A.P.J Abdul Kalam University, Indore

ABSTRACT

One of the most promising features of cognitive radios is its potential to consistently and independently locate unoccupied frequency bands. This article provides a high-level summary of the regulatory needs and significant problems related to the actual implementation of spectrum sensing capabilities in cognitive radio systems. We also describe the tradeoffs that must be made during design to improve the system's performance in several respects. This article begins with a thorough examination of the challenges posed by cognitive radio network security before moving on to discuss the fundamental concerns surrounding this technology. The paper then examines the dynamic spectrum access security and AI in light of the distinctions between cognitive radio networks and conventional wireless networks. Finally, it provides a conclusion on cross-layer design security issues. Superior to traditional radio systems, Cognitive Radio employs a distributed network of artificial intelligence-powered nodes. As opposed to conventional radio, cognitive radio systems maximize the utilization of all available resources by making full use of the whole frequency spectrum. Cognitive radio's main benefit is that it can find free spectrum channels and adjust transmission settings such that several unused frequencies may be utilised at once.

KEYWORDS: - Spectrum Access; Cognitive Radio Network; Artificial Intelligence; Network Security; Radio Transmission

INTRODUCTION

Wireless communication systems are experiencing fast development to fulfill the changing expectations and requirements of people. The development in wireless applications and services makes it important to solve the spectrum shortage issue. U.S. telecom regulator FCC measurements suggest up to 90% underutilization of permitted bands. The findings of the measurement were released by the FCC Spectrum Policy Task Force group in the paper entitled "FCC Report of the Spectrum Efficiency Working Group". A lot of study has gone into the most efficient ways to use these unoccupied or underutilized spectrum bands in recent years. One of the significant notions in the investigations is the cognitive radio concept, developed by Mitola in 1999. CR is a software-based technology that senses the electromagnetic environment in which it runs, discovers unused frequency bands, and changes the radio operating settings to broadcast in these bands. CR is a fundamental technology that allows the restricted and inefficiently utilized frequency bands to be used more effectively using an opportunistic approach. Cognitive radio networks rely heavily on the accuracy of the spectrum sensing function to provide the best possible communication performance and uptime.

As was said before, the licensed and unlicensed frequency spectra are under increasing amounts of stress due to the fast expansion of wireless communication technology. Since the media requirements cannot be met by the predetermined spectrum allocation. Making use of the already available spectrum for holes as transmission medium seems to be a workable approach. As was previously noted, all secondary users have some kind of system in place to guess which frequency ranges are free. On the other hand, a significant obstacle arises when there are many supplementary users. Because the secondary users get varying amounts of energy from the main user, the white space they experience will also vary in frequency. Since a result, it is important to have a centralized station that can determine which frequency bandwidths are genuinely accessible for detection, as the accuracy of an individual secondary user in this scenario is doubtful at best.

The history of radio dates back over a century. The very nature of radio means that anybody using the same frequency range runs the risk of encountering interference. The frequency bands will become very congested as the number of users continues to rise. Because of the exponential expansion of wireless networks over the last several decades, the situation has only worsened. The specifics of the frequency allocation demonstrate the severe difficulty the rising demand poses due to the lack of newer frequencies. The frequency spectrum is absent from the newest wireless system designs. It's an issue for any developing new system, since the underlying infrastructure tends to freeze after a few years. It's also worth noting that redistributing the current infrastructure is out of the question. It was in response to this formidable obstacle that the idea of "cognitive radio" was originally conceived. Cognitive radio is based on the idea of using existing signal processing technology to distribute bandwidth to new consumers. The new technology had to meet strict criteria, including no quality loss, the ability to accommodate a large number of users on the same frequencies without interfering with the experience of current users, and a significantly increased data transfer rate. Utilizing already-existing frequency bands in a more efficient manner via the use of technological know-how is one such method. It will need a number of adjustments to the current spectrum in order to make room for the additional frequencies.

The term "cognitive radio" refers to a device that may adjust transmission settings in response to data gathered from the surrounding environment. In the past, a CRN was referred to as a Next Generation (xG) network because of its ability to facilitate the dynamic use of spectrum. Mind-reading radio Cognitive radio (CR) is an upgrade to SDR that can automatically detect its RF environment, act as a catalyst, and intelligently adapt its operating parameters to the network infrastructure in order to meet user demand. If the band is already in use by a licensed user, CR will either switch to a different spectrum band or stay in the same band but adjust its transmission power and modulation scheme in order to avoid interference.

LITERATURE REVIEW

Zhang, Jianzhao et.al. (2020) Spectrum is the key ingredient for 5G wireless networks and beyond. Sharing the spectrum among various users under a dynamic spectrum management (DSM) framework is crucial to meeting the ever-increasing demand for bandwidth without compromising on its long-term sustainability. The purpose of this study is to discuss the challenge of integrating intelligence into spectrum management by analyzing the Dynamic Spectrum Management (DSM) and the potential uses of machine learning and artificial intelligence (AI) in spectrum access. Spectrum data, spectrum information, and spectrum knowledge are first overlaid with SOP-related information according to processing and abstractive level. Spectrum knowledge is the information needed to reason about and forecast the usefulness of SOPs and the consequence of SOP occupancy, and it may be used in a scalable manner. Then, we propose the smart spectrum model (SSM), wherein the spectrum understanding serves as the primary enabler and the paired SOP discovery and exploitation serves as the model's central characteristic. In order to make the most of both historical data and current sensing data, a spectrum knowledge and real-time observing (SKRO) enabled SOP exploration strategy is developed inside the SSM framework. Extensive simulations are presented to show that the SKRO-enabled SSM is capable of much higher rates of SOP use while still meeting all legacy assurance requirements. In a low signal-to-noise setting, for example, the SOP utilization ratio may be improved by at least 16.55 percent over the DSM.

Fan, Rong et.al. (2019) Spectrum occupancy prediction (also known as channel state prediction) is a technique that has been included into cognitive radio (CR) in recent years to help deal with the spectrum's limited availability and maximize its efficiency. Modeling the most common user actions in CR is the first topic covered in this study. In addition, a recurrent neural network (RNN) is selected to develop a spectrum occupancy state predictor in light of the stated behavior model. Predicting the spectrum occupancy status of main user behavior is made possible by using the learning capability of recurrent neural networks. Meanwhile, the RNN-based spectrum occupancy state predictor and another existent two spectrum occupancy state predictors are modified in the paper's simulation part to highlight the benefits of the suggested predictor. Advantages of the suggested strategy are shown by numerical simulations.

Ozturk, Metin et.al. (2019) The lack of awareness of the occupancy circumstances of the spectrum bands to be felt has rendered traditional Cognitive Radio (CR) spectrum access strategies crude and inefficient. Poor Quality of Service (QoS) and excessive latency are further consequences of the fact that existing spectrum access methods can neither detect network changes nor take into account the needs of unlicensed users. Conventional CR spectrum access should be upgraded to be more effective and flexible, since user-specific techniques will play a vital role in future wireless communication networks. To reduce sensing latency and make CR Networks (CRNs) aware of the needs of unlicensed users, this research proposes a complete and new method. Accordingly, a proactive procedure is suggested, with a unique QoS-based optimization phase that comprises two alternative choice techniques. At first, A.N.N.s are used to forecast the combined traffic loads of several Radio Access Technologies (RATs) operating in a variety of frequency bands (ANN). Two approaches are suggested based on these forecasts. First, a latency-centric method known as virtual wideband (WB) sensing is devised, in which relative traffic loads in WB are forecasted and then used to power NB sensing. The second one, built on

Q-learning, is concerned with more than just reducing sensing latency. The results show that the first technique was able to minimize sensing latency in the random selection process by 59.6 percent, while the second strategy, which was aided by Q-learning, improved full-satisfaction by as much as 95.7 percent.

Eltom, Hamid et.al. (2018) The rising demand for future wireless networks has sparked a proliferation of dynamic spectrum access solutions in response to the impending spectrum shortage caused by wasteful use. Using a dynamic spectrum access system, secondary users may access main users' spectrum bands so long as the resultant interference is below a certain limit. The ability to provide minimal interference and flawless communications is dependent on the spectrum occupancy patterns of both primary and secondary users. Consequently, an optimized dynamic spectrum access system must include spectrum occupancy prediction. The field of spectrum occupancy prediction has lately attracted a lot of interest in the wireless communications literature. However, there is not currently a central repository of information in the open literature that provides a unified view of the subject of statistical spectrum occupancy prediction. Our primary contribution here is a statistical prediction classification framework for evaluating and organizing existing spectrum occupancy models. First, a brief introduction to statistical sequential prediction is given. As a result of this statistical grounding, existing methods for predicting spectrum occupancy are critically examined. This discussion expands upon previous work to include cooperative prediction into models of spectrum occupancy. Finally, complications in theory and practice are examined.

Raj, Vishnu et.al. (2017) Methods to increase the spectral efficiency of wireless networks are crucial due to the introduction of 5G wireless technologies and the growing need for more throughput. If the secondary user in a cognitive radio system can make informed judgments about which channel to sense and how frequently to sense it, the system's throughput might be significantly increased. To save time on channel sensing, we offer an algorithm that does more than just choose a channel for data transmission; it also predicts how long the channel will stay vacant. To find the ideal time to forgo sensing, our method uses a Bayesian technique after first using reinforcement learning to choose channels. Extensive simulations are supplied to enable comparisons with various learning approaches. We demonstrate that the number of sensing may be lowered with just a marginal increase in primary interference, which means that the secondary user expends less energy in sensing and achieves greater throughput.

COGNITIVE RADIO NETWORK SECURITY

Due to the significant impact of the spectrum scarcity, the FCC believes it should allow illegal users access to allowed spectrum on the assumption that this would not have any negative effects on Primary users. It’s crucial item for testing spectrum hole. People proposed the technique of dynamic spectrum access to figure out how to find these open frequencies and make use of them. Through the Spectrum Sensing to free band algorithm, subprime users may make full use of spectrum resources by no influence on the premise of Primary users’ communications. Cognitive radio network as a wireless communication technology, it’s not only the classic security difficulties, but also has brought some new hidden security. Spectrum sensing, spectrum management, spectrum migration, and spectrum sharing are just a few of the numerous components that go into gaining access to the electromagnetic spectrum. There are potential security holes in every single procedure. Many studies are focusing on reasoning and optimization learning algorithms in different states so that cognitive radio may intelligently learn and adapt to its surroundings. However, as the information value continually reflects, the notion of information security in the design attracts more and more attention. The communication security has become a significant aspect of the system design, notably involving military, business secrets, etc. Since cognitive radio has become so prevalent in these settings, it is essential that more care be taken to ensure its security. The cognitive radio industry is confronting its own unique challenges in addition to the more common wireless security issues.

Threat of Dynamic Spectrum Access

In the present policy, spectrum is allocated permanently to the authorized user of a specific area by a government agency. Spectrum is a scarce commodity. Spectrum allotment is almost depleted due to the rising demand for wireless devices and connectivity. But given the finite amount of substantial spectrum, cognitive radio may make efficient use of secondary spectrum to accomplish this goal. In order to do this, the cognitive user must be able to constantly assess the state of the channel and, barring any interference, get access to the signal without disturbing the Primary users. In order to avoid harmful interference for Primary users, this kind of solution demands cutting-edge technology. Spectrum sensing, spectrum management, and spectrum migration are all parts of dynamic spectrum access, and each one has its own inherent risks. Cognitive radio has its own unique security issues, such as spectrum abuse and selfish conduct, attacks that disguise themselves as primary users, blocked public control channels, cognitive nodes that have evolved into malevolent nodes, and so on. Next, we'll take a look at the current issues with cognitive radio system security from the perspective of dynamic Spectrum Sensing.

1. Primary User Emulation Attack

One of the security issues at the physical layer is the danger posed by Primary User Emulation (PUE) attacks, which poses a serious challenge for Spectrum Sensing. The attacker sends a CR signal that mimics the original users. Under CR conditions, this approach of assault may materialize a highly adaptable, software-based air interface. In a DSA setup, the principal user has unrestricted access to the permitted frequency range at all times. When the principal user frees up the resources, the allowed frequency band enters an idle condition that the secondary users may try to access [8]. Primitive users must be able to detect a free frequency band as a required prerequisite. As a result, detecting devices need a Spectrum Sensing algorithm to provide continuous observation of the spectrum's status. In this scenario, an attacker generates a signal that is identical to that of the main user, resulting in an erroneous frequency spectrum that fools the subprime users into misjudging the spectrum's condition. As a result, the channel will be unrestrained in the system and vulnerable to assault. Primary User Emulation Attack describes this kind of attack.

According to studies, a PUE assault may considerably diminish the available channel resources of legal perception users and cause severe interruption to the Spectrum Sensing process. Spectrum sensing may be accomplished via the use of filter matching and rotating feature detection technologies. Down order to differentiate between main and subprime users, nodes equipped with these identification methods may zero in on the principal users' defining traits. However, this is insufficient to repel a PUE assault. Based on their motivations and methods, PUE attacks may be classified as either selfish or malignant. An individual's motivation for engaging in selfish action is to further their own interests. The attacker would identify a band and then imitate the principal user's signal to block access to the band for any secondary users [10]. After the attackers have accomplished their goal, they will cut the channel. The time to launch an attack is minimal. When the user notices the attacker has left the channel, they may rejoin once they have gained trust in the environment again. If an attacker is acting maliciously, they may try to prevent genuine subprime users from identifying and utilizing the permitted frequency band, which would result in a denial of service. Attackers that are malevolent don't benefit from the free license and instead conduct a PUE assault over a wide spectrum of frequencies. An assault on the network, whether for selfish reasons or malevolent ones, is always an annoyance. The success of a PUE assault hinges on whether or not the signal coming from the main users can be distinguished from the signal coming from the malevolent cognitive users. The base station may utilize the user's certificate to confirm they are an authorized user, but if the certificate is lost, maintaining control becomes difficult. As a result, it has to provide a soft authentication that can verify users rapidly while using little processing resources. Furthermore, it takes appropriate action against malicious users to apply penalty as soon as harmful attack activity is detected. A loss of confidence in the network or even expulsion from the network might result from this.

2. Primary User Interference

Disruptions from malicious users to legitimate users are a typical sort of attack in DSA and happen rather often. Subprime users will create disruptions for the user, and might potentially lead to a denial-of-service assault, due to CR's adaptability and scalability. There are two ways in which subprime users may use the radio spectrum: One example is anybody may legally use the white band without paying a fee. Knowing the precise model of main users' behaviors is essential. The alternative is to share the secondary users' gray area with the principal users. The latter is crucial if we want to have an effect on the core audience. Accurate perception isn't enough; knowledge of the principal users' imminent arrival is also necessary for cognition to prevent user intervention. It is now possible for the attacker to carry out assaults. It disrupts the user's experience by blocking or altering any incoming cognitive data. Damage to the network's efficiency will result from this. As a result, the principal user could have to operate in an environment with a lot of background noise or no usable frequency range at all. It goes against the point of developing cognitive radio technology in the first place, which is to get access without disrupting the main user's routine usage. As a result, the cognitive user is at the forefront of the switch frequency spectrum. Cognitive users should quickly evacuate by switching frequency bands upon detecting the appearance of the main user's signal.

3. Data Tamper Attack of Spectrum Sensing

The attacker delivers false Spectrum Sensing data to the data collecting center during a distributed Spectrum Sensing process, leading to an incorrect judgment as seen in Figure 1. This is by far the most popular method of manipulating data to alter people's interpretation of it. The literature proposed the collaboration type Spectrum Sensing to increase the efficiency of perception, which did just that. However, this led to the emergence of additional issues, such as nodes that manipulate their partnerships to provide inaccurate outcomes. Spectrum sensing information has far-reaching consequences if tampered with, regardless of whether it is used in a centralized or decentralized network architecture. S. Arkoulis classified nodes as either misbehaving APs, selfish APs, cheat APs, or malignant APs based on their access aberrant behavior. Spectrum sensing is susceptible to manipulation by malicious nodes using tactics like as cheating, flash flooding, and gang collaboration. Through means of manipulation, deceit, flash flooding, and gang collaboration, the data fusion center was able to collect the incorrect data and orders. Spectrum data fusion center for unreliable information and guidance is a possibility. The attacker will use channel allocation to gain an advantage. Once the cognitive radio system's input data has been manipulated, it can no longer accurately control itself in response to the external world. The attacker will also have access to the finest adaptable function available. Spectrum Sensing data accuracy is, thus, crucial.

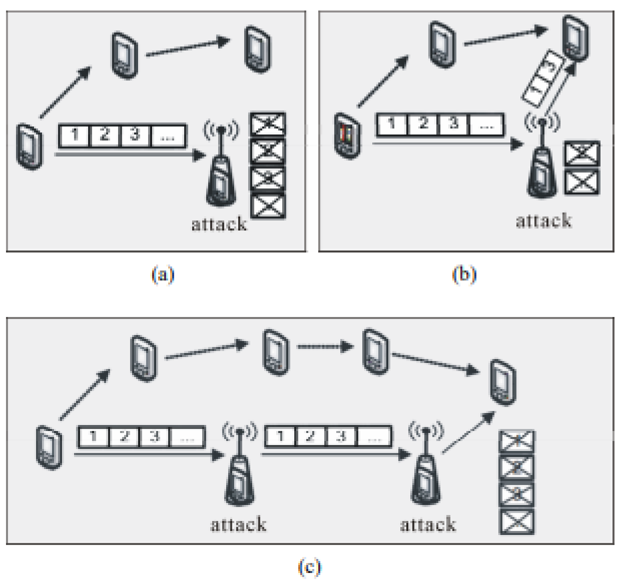

Figure 1. Data tamper attack of spectrum sensing.

SPECTRUM SENSING TECHNIQUES

In stationary Gaussian noise, a matching filter followed by a threshold test is the best detector if the original signal's structure is known. In early cognitive radio deployments, when the secondary system can only function in a few numbers of primary bands, coherence detection may be a workable solution. Since a cognitive radio will need dedicated circuitry to achieve synchrony with each type of primary licensee as required for coherent detection, the implementation cost and complexity associated with this approach will increase to the point where it is no longer practical as more primary bands are opened for opportunistic access. Using energy detection is a less complicated option for main signal recognition in noise.

	Infrastructure cost	Legacy compatibility	Transceiver complexity	Positioning	Internet connection	Continuous monitoring	Standardized channel
Database registry	High		Low	X	X		
Beacon signals	High		Low	X			X
Spectrum sensing	Low	X	High			X	

Table 1. Classification of white space identification methods.

detection. The energy received on a primary band during an observation period is monitored by an energy detector, and a white space is declared if the energy falls below a certain threshold. In cognitive radio systems, energy detection is a promising choice for spectrum sensing due to its cheap cost and ease of implementation, even if it takes more time for sensing to reach a desirable performance level than matched filtering.

The energy detector's principal shortcoming is its insensitivity to variations in the strength of background noise, particularly at low signal-to-noise ratios, due to its inability to distinguish between the core signal and noise during reception (SNR) With knowledge of the main signal's carrier frequency and modulation type, more advanced feature detectors may be used to solve this problem. Most communication signals, in contrast to stationary noise, display spectral correlation owing to inherent periodicities (features) including carrier frequency, bit rate, and cyclic prefixes, which are exploited by these detectors. A cognitive radio can pick out a principal signal from background noise and interference by using a technique called "feature detection," which takes use of the fact that various transmissions have distinctive spectral correlation qualities.

Some circumstances may need a hybrid approach, including a number of distinct strategies. To find potentially unoccupied frequency ranges, energy detection may be utilized to execute a rapid yet broad search. Through improved feature recognition, it may be possible to identify the gaps between these potential bands. Sensing performance may be enhanced by sensing (observing) the band for a longer duration, which increases signal processing gain regardless of the underlying detection technology. But as we will subsequently demonstrate, regulatory limits placed on sensing time limit such advancements.

As an alternative, system-level coordination amongst several cognitive radio networks allows them to avoid the aforementioned uncertainty at the expense of greater implementation cost. Common control channels allow tertiary systems to do things like negotiate access and handle aggregate interference. With this method, spectrum sensing begins to resemble the other options in Table 1. However, we point out that the cost advantage of the spectrum sensing method may still be maintained by raising the detection sensitivity without resorting to system-level coordination to deal with the uncertainty levels resulting from first installations.

CONCLUSION

Meeting regulatory criteria for dependable sensing has been a primary emphasis of spectrum sensing research to date. The interaction between spectrum sensing and higher-layer capabilities to improve the end-perceived user's QoS is a promising area for further study. In this regard, we describe many of the most significant cross-layer trade-offs associated with spectrum sensing. Most current studies concentrate on how people perceive spectrums. They provide a wide variety of strategies for enhancing the effectiveness of cooperative perception. However, there has not been sufficient depth in the research on security. There have been various suggested security mechanisms, but they fall short of what is required for a fully functional CRN. Cognitive radio is a cutting-edge innovation that may be used in many contexts. There has only been a little amount of study done in this area, hence surveys are of utmost relevance. This overview explains how cognitive radios operate, as well as the fundamentals of various network paradigms and sensing technologies. Essential cognitive radio components and their operations have been clearly outlined.

REFERENCES

1. Zhang, Jianzhao& Chen, Yong & Liu, Yongxiang& Wu, Hao. (2020). Spectrum Knowledge and Real-Time Observing Enabled Smart Spectrum Management. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2978005.

2. Fan, Rong&Guo, Hesong& Di, Lujie& Ling, Xing. (2019). Spectrum Occupancy State Predictor Based on Recurrent Neural Network. Journal of Physics: Conference Series. 1345. 042020. 10.1088/1742-6596/1345/4/042020.

3. Ozturk, Metin&Akram, Muhammad & Hussain, Sajjad & Imran, Muhammad. (2019). Novel QoS-Aware Proactive Spectrum Access Techniques for Cognitive Radio Using Machine Learning. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2918380.

4. Eltom, Hamid &Sithamparanathan, Kandeepan& Evans, Rob & Liang, Ying &Risti, Branko. (2018). Statistical spectrum occupancy prediction for dynamic spectrum access: a classification. EURASIP Journal on Wireless Communications and Networking. 2018. 29. 10.1186/s13638-017-1019-8.

5. Raj, Vishnu & Dias, Irene &Tholeti, Thulasi&Kalyani, S.. (2017). Spectrum Access In Cognitive Radio Using A Two Stage Reinforcement Learning Approach. IEEE Journal of Selected Topics in Signal Processing. PP. 10.1109/JSTSP.2018.2798920.

6. Bhowmick, Abhijit& Prasad, Binod & Dhar Roy, Sanjay &Kundu, Sumit. (2016). Performance of Cognitive Radio Network with Novel Hybrid Spectrum Access Schemes. Wireless Personal Communications. 91. 10.1007/s11277-016-3476-5.

7. Masonta, Moshe &Mzyece, Mjumo&Ntlatlapa, Ntsibane. (2013). Spectrum Decision in Cognitive Radio Networks: A Survey. IEEE Communications Surveys &amp Tutorials. 15. 1088-1107. 10.1109/SURV.2012.111412.00160.

8. Sun, Can & Ding, Hua & Liu, Xin. (2020). Multichannel Spectrum Access Based on Reinforcement Learning in Cognitive Internet of Things. Ad Hoc Networks. 106. 102200. 10.1016/j.adhoc.2020.102200.

9. Shawel, Bethelhem&Woldegebreal, Dereje&Pollin, S.. (2019). Convolutional LSTM-based Long-Term Spectrum Prediction for Dynamic Spectrum Access. 1-5. 10.23919/EUSIPCO.2019.8902956.

10. Eltom, Hamid &Kandeepan, Sithamparanathan& Liang, Ying-Chang & Evans, Robin. (2018). Cooperative Soft Fusion for HMM-Based Spectrum Occupancy Prediction. IEEE Communications Letters. 22. 10.1109/LCOMM.2018.2861008.

11. Ghane, Amir Hossein&Harsini, Jalil. (2018). A network steganographic approach to overlay cognitive radio systems utilizing systematic coding. Physical Communication. 27. 10.1016/j.phycom.2018.01.008.

12. Thakur, Prabhat & Kumar, Alok & Pandit, Shweta & Singh, Ghanshyam&Satashia, S.N. (2017). Performance analysis of cognitive radio networks using channel-prediction-probabilities and improved frame structure. Digital Communications and Networks. 4. 10.1016/j.dcan.2017.09.012.

13. Nguyen, Van-Dinh& Shin, Oh-Soon. (2017). Cooperative Prediction-and-Sensing Based Spectrum Sharing in Cognitive Radio Networks. IEEE Transactions on Cognitive Communications and Networking. PP. 10.1109/TCCN.2017.2776138.

14. Gmira, Sara &Kobbane, Abdellatif&Sabir, Essaid. (2015). A new optimal hybrid spectrum access in cognitive radio: Overlay-underlay mode. 1-7. 10.1109/WINCOM.2015.7381314.

15. Chatterjee, Subhankar&Maity, Santi&Tamaghna, Acharya. (2014). Energy Efficient Cognitive Radio System for Joint Spectrum Sensing and Data Transmission. Emerging and Selected Topics in Circuits and Systems, IEEE Journal on. 4. 292-300. 10.1109/JETCAS.2014.2337191.