Threats Advancement in Primary User Emulation Attack and Spectrum Sensing Data Falsification (SSDF) Attack in Cognitive Radio Network (CRN) for 5G Wireless Network Environment

A.H.Fauzi and A.S.Khan
Faculty of Computer Science and Information Technology,
Universiti Malaysia Sarawak, Sarawak, Malaysia.
hadinata@unimas.my

***Abstract*—Primary User Emulation (PUE) attack and Spectrum Sensing Data Falsification (SSDF) attack on Data Fusion Centre and attack on Common Control Channel (CCC) is a serious security problems and need to be addressed in cognitive radio network environment. We are reviewing the recent advances of threats for the future 5th Generation (5G) wireless radio network from these attacks. Several existing security schemes have been proposed and discussed to overcome these attacks. We propose new security scheme that able to mitigate the attacks and provide security solutions. This scheme intended to mitigate the threats from the attacks in CRN and improve the future 5G network security.**

***Index Terms*—CRN; Data Fusion; Radio Network; Wireless 5G; Secure; PUE; SSDF.**

I. Introduction

Cognitive Radio Network (CRN) was introduced as a promising technology to solve the issues of spectrum scarcity in cellular wireless network due to the increasing number demand of wireless services [1]. Cognitive Radio Network is part of the 5G initiative towards high speed and secure wireless radio network.

The concept of the 5G network is promising to satisfy the growing needs of mobile wireless communication. Along with increasing data rate, number of users, reliability and coverage of the mobile network, security is a matter of key importance that requires careful consideration. As with the upcoming spread of the Internet of Things (IoT) that the 5G network is going to propagate to almost all aspects of our lives, security will become even more crucial than it is now [2].

Security is one of the fundamental aspects of the next generation mobile network [3]. Many new technologies are emerging to be deployed in the 5G network and improve its performance. Their security issues should be examined so that appropriate countermeasures can be taken before new technologies are deployed into live operation. Novel approaches for security enhancement also have been proposed. In particular, physical layer security seems to offer reasonable solutions for many security requirements [4]. It is important to recognize its possible risks and point out topics for further research.

The rapidly growing number of mobile devices, capacious data and higher data rate are pushing to reconsideration the existing generation of the cellular mobile communication. The next or fifth generation (5G) wireless network is expected to meet high end requirements. The 5G networks would provide novel architecture and technologies beyond state of the art architecture and technologies. The new research track will lead the elementary changes in the design of fifth generation (5G). The 5th generation mobile network signifies the next foremost phases of mobile telecommunications standards beyond the current 4G. 5G has speeds beyond what the current 4G can offer.

The Next Generation Mobile Networks Alliance realizes that 5G should be rolled out by 2020 to meet the business and consumer demands. In addition to providing simple faster speeds, they expect that 5G networks also will need to meet the needs of new use case, such as Internet of Things (IoT) as well as broadcast-like services and lifeline communication in times of natural misfortune. Cognitive Radio Network will help 5G by Device-to-device (D2D) communication [5], Moving Network (MN) [6], Ultra Dense Network(UDN) [7] and Self Organizing Network(SON) [8].

Cognitive Radio Network consist of two type of users that are licensed primary user (PU) of the cellular network and unlicensed secondary user (SU). Secondary user constantly observed the licensed spectrum band by performing spectrum sensing to check the availability of the channel for them to use. When vacant spectrum channel discovered, secondary user will transmit using the available channel. However, in a legitimate manner, if secondary user sense any PU signal which indicates that PU wants to use the channel, SU will need to back off and find another available channels [9]. There are several well-known challenges CRN. Among them are:

- Performance degradation overall Cognitive Radio Net-work Quality of Service (QoS) and underutilized channel usage in Cognitive Radio Network due to attack from malicious user.
- Protecting the Data Fusion Centre becomes target for false data input and data manipulation. Data fusion centre used to store information from legitimate user details and makes global decision
- Denial of Service attack on Data Fusion and Common Control Channel.

In this paper we will address the security issues in 5G wireless network. In particular, we study the security challenges of CRN in 5G. This paper aims to review the advances of threats in primary user emulation attack, spectrum sensing data falsification (SSDF) attack in CRN and attack against Common Control Channel which become the path for data dissemination.

The objectives of this review is to identify critical security threats on Cognitive Radio Network, Data Fusion Centre and Common Control Channel in 5G wireless network environment. We will propose new security scheme to secure Cognitive Radio Network, Data Fusion and Common Control Channel against Primary User Emulation Attack, data falsification and attack such as Denial-of-service to Data Fusion Centre and Common Control Channel. The proposed security scheme will be evaluated using simulation against all the identified attacks in Cognitive Radio Network in 5G cellular network environment.

Based on the critical analysis of the literature review, we suggest future direction of the Cognitive Radio Network technology in the 5G wireless network environment with recommendation and framework based on the simulation result.

II. Background

An attack in cognitive radio network environment can happen due to Secondary User (SU) ability to sense signal and making decision, attacker can imitate Primary user signal that can caused Secondary User to back off. Attackers can emulate Primary User signal to enforce Secondary User to vacate the specific band. This is called as Primary User Emulation(PUE) attack. We categorize the attacks of Primary User Emulation into three characteristics:

- Greedy/Selfish - Secondary User (attacker) emulates Primary User signal so it can use the vacant channel for itself [10].
- Malicious - Secondary User (attacker) emulated Primary User signal to caused Denial of Service attack [11], [12]
- Mixed - Between selfish and malicious [13].

In Yu, R et al. [14] outlined in their work that security is very important by not well addressed issue in Cognitive Radio network and Primary User Emulation attack is a serious security problem in cognitive radio network. According to Sharma et al. [15], Cognitive Radio systems are vulnerable to numerous security threats that affect the overall performance. Dynamic sharing of the spectrum between multiple users poses several significant challenges in security and trust [16]. Intrinsic characteristic of Cognitive Radio opens new ways for attackers [17]. Dynamic behaviour of Cognitive Radio Network, conventional attack detection scheme unable to detect attack on Common Control Channel [18]. Primary User Emulation is the most studied attack in Cognitive Radio Network [19].

For cooperative sensing, which Cognitive Radio use to deliver the spectrum sensing report to the Data Fusion Centre using Common Control Channel (CCC). Other than centralized Data Fusion Centre, it also able to update and share with neighboring nodes the spectrum sensing report if there are any changes to the results. For spectrum sensing report, it must meet three control channel requirements which is the bandwidth, reliability and security [1]. Due to Primary Emulation attack, the available channel is use dedicatedly by greedy secondary user and possibly not being used at all. This is causing overall performance degradation in Cognitive Radio Network Quality of Service (QoS) and underutilized channel usage.

The main reason of using CRN is to fully utilizing the available vacant channel but due to attack such as Primary User Emulation, it fails to achieve the goal. Data fusion centre is used to store information of legitimate user details to overcome the malicious PUE attack. However, by protecting the Data Fusion itself also causing it to be targeted for false data input also known as SSDF attack. Apart from that, there are possibility of denial of service attack on Data Fusion Centre and Common Control Channel (CCC). User unable to check status of Primary User and Secondary User trustworthiness and makes it vulnerable to attack and making wrong decision.

As we discuss further about the Data Fusion Center as they are subjected to Spectrum Sensing Data Falsification (SSDF) Attack. Collaborative Spectrum Sensing (CSS) has been proposed to overcome the problem effect of multipath fading, shadowing, and hidden station issues [1].

Unfortunately, the CSS is vulnerable to Spectrum Sensing Data Falsification (SSDF) attacks as well [20]. In an SSDF attack, the malicious Cognitive Radio user intentionally sends a falsified local sensing result to the Data Fusion Center (DFC) in an attempt to cause it to make incorrect global decision. To mitigate the problem of SSDF attack, many approaches have been proposed as we reviewed later.

In [21], Lu et. al has proposed scheme using hard decision scheme. The spectrum sensing process divided into two. First is the identifying stage and second is the sensing stage. At the identifying stage, they propose a scheme to identify reliable secondary users in the CRN. At the sensing stage, fusion center receives decision reports from all user identified in the identifying stage and trusted nodes to make global decision. In this scheme, it only accepts report from known and trusted user.

Independent and collaborative SSDF attacks have been developed in [12]. Naqvi et. al. proposed a novel reputation based scheme to identify the attackers. They illustrate that in the presence of 50% independent attackers, their proposed approach cannot differentiate between the malicious and benign users. However, for collaborative attack, this ratio reduces to 35%.

In [22] a hybrid method called Weighted Sequential Probability Ratio Test (WSPRT) was proposed. The method combines the nodes reputation and uses Sequential

Probability Ratio Test (SPRT) to identify malicious users. Compared with SPRT, the WSPRT improves correct sensing probability at the cost of increasing sampling overhead. A new scheme to countermeasure against SSDF attack in CSS, called Conjugate Prior-based (CoP) was proposed in [23]. The probability function of random sensing reports and each sensing report is examined for the normality based on a confidence interval.

As a countermeasure against SSDF attacks, [24] propose a new method called Attack-Aware CSS (ACSS). The idea based on attack strength estimation, where the attack strength is defined as the probability that a given user is malicious. The proposed ACSS method obtains the attack strength and applies it in koutN rule to deriving the optimal value of parameter k to minimize the Bayes risk. Simulation results presented the effectiveness of the proposed method. A common way of evaluating a decision rule is by computing the result called Bayes risk.

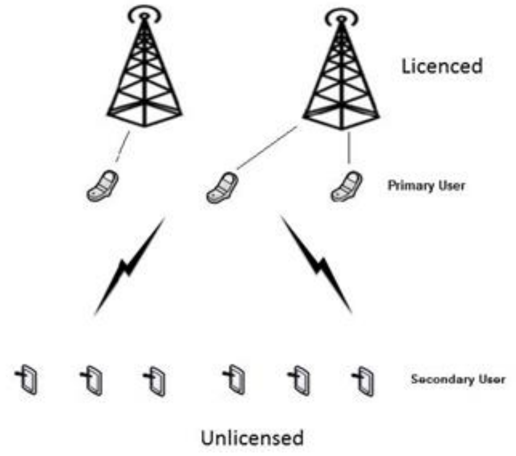

Figure 1: Overview of Cognitive Radio

Bhattacharjee et al. [25] has proposed an apriori algorithms scheme. The ability of this scheme is same in as method in detecting the spectrum sensing data falsification. The apriori scheme by attacker need to send an association in the sensing report then sent to the data fusion centre (DFC), finally the apriori take part by capture identify the association and trying to detect the SSDF attack. The SSDF attack is one of the attack that affected data fusion centre (DFC) in way give a false sensing report including modify the sensing report. There is weakness in this scheme where this scheme only able to detect the SSDF attack but unable to protect the cognitive radio network itself. However, the simulation still success and the apriori algorithms can been used as a scheme to detected the spectrum sensing data falsification (SSDF) attack.

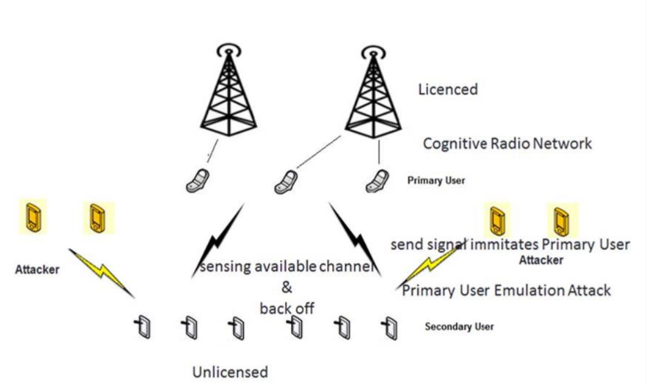

Figure 2: Primary User Emulation Attack

The ARC algorithms scheme are current work of independent and collaborative spectrum sensing data falsification attacks which is proposed by Priya and Nandhakumar [26]. They found that ARC schemes successfully reduced the error rate and capable of identifying the attacking node including overcoming the false detection rate of another original channel.

To understand better about Cognitive Network environment, Figure 2 shows the Primary User Emulation attack prevent SU to sense the spectrum correctly and accurately. SU must have priori known characteristic of the PU signal. With that knowledge, it can sense PU signal and vacant the channel it occupied. One of the proposed method to solve inaccurate sensing by using Data Fusion Centre (DFC) to collect all the SU sensing report and DFC will generate decision based on the SU contribution. However, using DFC introduce another problem of how reliable the collected data, what if malicious user contribute more false data is more than good secondary user which will lead to wrong decision and integrity of the DFC itself. This is called the Spectrum Sensing Data Falsification attack as illustrated in Figure 2. The new secondary user that rely fully on Data Fusion Centre will accept the DFC decision instead of sensing for vacant channel at the Primary Base station. In DFC, final decision is made based on several parameters such as OR, AND, k out of N and Majority. We assume there are three types of malicious SU in SSDF attack:

- Smart Malicious SU When it senses 0 (vacant) from the primary base station, it will send 1 (occupied) as the report to Data Fusion Centre (DFC) and visa-versa.
- Always Occupies Malicious SU It will always send 1 to the Data Fusion Centre, although it is not a smart as the first malicious SU, it caused DOS attack as it implies that the channel always not available.
- Always Vacant Malicious SU It will always send 0 to the Data Fusion Centre. SU will attempt to use the channel assuming it is vacant but unfortunately it is unavailable. It will consume energy and time.

Basically, SSDF attack need collaborative attack to make it a successful attack. We assume to have N secondary users, each of SUs sense the channel at the beginning of each slot and report their decisions to DFC by one bit, H1(=1) and H0(=0) denote the presence and absence of a primary signal respectively. The signal power received by i-th SU is given by:

$$e_i[t] = \begin{cases} \int \left| H_i(t) s_i(t) + n_i(t) \right|^2 \mathrm{d}t : H_1 \\ \int \left| n_i(t) \right|^2 \mathrm{d}t : H_0 \end{cases} \tag{1}$$

where $S_i(t)$ is a primary signal, $H_i(t)$ is a channel coefficient that is multiplied by signal and $n_i(t)$ is Additive White Gaussian Noise (AWGN). The threshold that is denoted by in Equation (2) can be defined by [27]:

$$e_i[t] \underset{H_0}{\overset{H_1}{\gtrless}} \lambda \tag{2}$$

$$\frac{\lambda}{\sigma_n^2} = 2u + 2\sqrt{u}Q^{-1}(P_f) \tag{3}$$

where P_f is the detection probability of false alarm in wireless environment, u is time-bandwidth product and n^2 is a variance of noise.

III. Proposed Scheme and Discussion

In this section, we will discuss the challenges that need to be addressed for the threats by the attacks and proposed the possible solutions. The first challenge is determining the spectrum sensing algorithm accuracy to archive the accurate spectrum value. The second challenge is how to use the collaborative spectrum sensing algorithm to make final decision with integrity and trusted value. The third challenge is how to secure the channel to deliver the individual result which is secure and tamper-proof. We propose for sensing the channel availability from the stationary nodes. Stationary which is not mobile and fixed location. This type of nodes is more predictable, traceable and able to build up good reputation over time. As for mobile nodes, they come and go all the time and it can be anywhere and their identity can be falsified easily. Their location also not fixed and easy to masquerade any other mobile nodes. Referring to Figure 3, the spectrum sensing from stationary nodes is accepted by the Data Fusion Centre. The Data Fusion Centre must have preliminary data of the identity of each contributing stationary nodes including its location. As for mobile nodes, their spectrum sensing report contribution are dropped or rejected when received by the Data Fusion Centre. In this scheme, the reliability of the report contributed by the stationary nodes are much more trusted than then random mobile nodes.

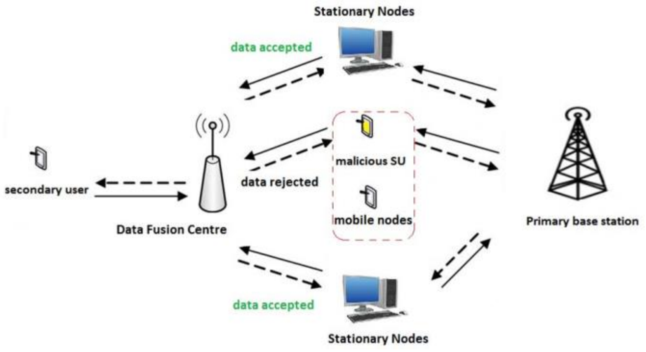

Figure 3: Stationary Nodes Sensing Available Spectrum and Reporting to Data Fusion Centre in Cognitive Radio Network

For Common Control Channel, there are several methods ensure integrity of the data that use CCC as the channel to send data to Data Fusion Centre and share data to neighboring nodes. As we assume we apply the same method of stationary nodes, we can use technique of shared key encryption which encrypt each data that used the Common Control Channel before being sent by the stationary nodes and decrypt in once received by the Data Fusion Centre. Using simple encryption technique, keys can easily be generated and distributed among the stationary nodes. Data Fusion Centre also can challenge from time to time to ensure the data received come from the authentic source of stationary nodes.

For Data Fusion Centre, the incoming data are controlled by the encryption keys. If they unable to decrypt the data, it means it does come from the usual stationary nodes and will be dropped. Only encrypted data with identity of trusted stationary nodes will be decrypted and counted towards making global decision.

Other mobile nodes rely on the Data Fusion Centre. With this proposed scheme, it able to secure the report, channel and ensure integrity of the data. Mobile nodes will need less computational power thus increasing the network performance. Less computational also able to save on energy and organize the network efficiently.

IV. CONCLUSION

As conclusion, we have reviewed the recent threats and countermeasures for attack against Cognitive Radio Network system. Cognitive Radio Network roles will able to help 5G wireless network to meet the user demand for high speed and secure wireless environment. The proposed security schemes that able to improve the security performance and network performance in term of high speed in Cognitive Radio Network and. In the future, we will proof this scheme using network simulation under various network attributes.

ACKNOWLEDGMENT

The authors would like to thank Unimas Innovation and Universiti Malaysia Sarawak for providing MyRA Special Short Term Grant (F08/SpSTG/1367/16/9).

REFERENCES

[1] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, “Cooperative spectrum sensing in cognitive radio networks: A survey,” pp. 40–62, 2011.

[2] E. Hossain and M. Hasan, “5G cellular: key enabling technologies and research challenges,” *IEEE Instrumentation & Measurement Magazine*, vol. 18, no. 3, pp. 11–21, 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7108393

[3] F. Boccardi, R. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, “Five disruptive technology directions for 5G,” *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, 2014.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, “Safeguarding 5G Wireless Communication Networks Using Physical Layer Security,” *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[5] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, “Interference Exploitation in D2D-enabled Cellular Networks: A Secrecy Perspective,” *IEEE Transactions on Communications*, vol. PP, no. 99, pp. 1–1, 2014. [Online]. Available:http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6981933

[6] H. Yasuda, A. Kishida, J. Shen, Y. Morihiro, Y. Morioka, S. Suyama, A. Yamada, Y. Okumura, and T. Asai, “A study on moving cell in 5G cellular system,” in *2015 IEEE 82nd Vehicular Technology Conference, VTC Fall 2015-Proceedings*, 2016.

[7] M.-c. Chuang, M. Chang, and Y. S. Sun, “Resource Management Issues in 5G Ultra Dense Smallcell Networks,” *International Conference on Information Networking(ICOIN),*, no. 1, pp. 159–164, 2015.

[8] S. Sun, M. Kadoch, and T. Ran, “Adaptive SON and Cognitive Smart LPN for 5G Heterogeneous Networks,” *Mobile Networks and Applications*, vol. 20, no. 6, pp. 745–755, 2015.

[9] J. Mitola, “Cognitive radio: An integrated agent architecture for software defined radio,” *Doctor of Technology, Royal Inst. Technol.(KTH)*, pp. 271–350., 2000.

[10] S. Ma, Y. Peng, T. Wang, X. Gan, F. Yang, X. Wang, and M. Guizani, “Detecting the greedy spectrum occupancy threat in cognitive radio networks,” in *2014 IEEE International Conference on Communications, ICC2014*, 2014, pp. 4939–4944.

[11] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, “Malicious user detection in a cognitive radio cooperative sensing system,” IEEE Transactions on Wireless Communications, vol. 9, no. 8, pp. 2488–2497, 2010.

[12] B. Naqvi, S. Murtaza, and B. Aslam, “A mitigation strategy against malicious Primary User Emulation Attack in Cognitive Radio networks,” Proceedings-2014 International Conference on Emerging Technologies, ICET2014, pp. 112–117, 2014.

[13] N. Nguyen Thanh, P. Ciblat, A. T. Pham, and V. T. Nguyen, “Surveillance Strategies Against Primary User Emulation Attack in Cognitive Radio Networks,” IEEE Transactions on Wireless Communications, vol. 14, no. 9, pp. 4981–4993, 2015.

[14] R. Yu, Y. Zhang, Y. Liu, S. Gjessing, and M. Guizani, “Securing cognitive radio networks against primary user emulation attacks,” IEEE Network, vol. 29, no. 4, pp. 68–74, 2015.

[15] R. K. Sharma and D. B. Rawat, “Advances on security threats and countermeasures for cognitive radio networks: A survey,” IEEE Communications Surveys and Tutorials, vol. 17, no. 2, pp. 1023–1043, 2015. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0 84930508485&partnerID=40&md5=3ab0bb1c2a41172f887c90a02f1c9c45

[16] Z. Jin, S. Anand, and K. P. Subbalakshmi, “Detecting primary user emulation attacks in dynamic spectrum access networks,” in IEEE International Conference on Communications, 2009.

[17] J. Marinho, J. Granjal, and E. Monteiro, “A survey on security attacks

and countermeasures with primary user detection in cognitive radio networks," EURASIP Journal on Information Security, vol. 2015, no. 1, p. 4, 2015. [Online]. Available: http://www.scopus.com/inward/record.url?eid=2s2.0-84928387229&partnerID=tZOtx3y1

[18] Y. Zou and S. J. Yoo, "A cooperative attack detection scheme for common control channel security in cognitive radio networks," in International Conference on Ubiquitous and Future Networks, ICUFN, vol. 2015-Augus, 2015, pp. 606–611.

[19] A. Araujo, J. Blesa, E. Romero, and D. Villanueva, "Security in cognitive wireless sensor networks. Challenges and open problems," EURASIP Journal on Wireless Communications and Networking, vol. 2012, no. 1, p. 48, 2012. [Online]. Available: http://jwcn.eurasipjournals.springeropen.com/articles/10.1186/16871499-2012-48

[20] Y. Hou and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," IEEE Communications Magazine, vol. 46, no. 4, pp. 50–55, 2008. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4481340

[21] J. Lu, P. Wei, and Z. Chen, "A scheme to counter SSDF attacks based on hard decision in cognitive radio networks," WSEAS Transactions on Communications, vol. 13, pp. 242–248, 2014.

[22] R. Chen, J.-M. J. Park, and K. Bian, "Robustness against byzantine failures in distributed spectrum sensing," Computer Communications, vol. 35, no. 17, pp. 2115–2124, 2012.

[23] C. Chen, M. Song, and C. Xin, "Copd: a conjugate prior based detection scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks," Wireless networks, vol. 20, no. 8, pp. 2521–2528, 2014.

[24] A. A. Sharifi and M. J. M. Niya, "Defense against SSDF attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach," IEEE Communications Letters, vol. 20, no. 1, pp. 93–96, 2016.

[25] S. Bhattacharjee, R. Keitangnao, and N. Marchang, "Association rule mining for detection of colluding SSDF attack in Cognitive Radio Networks," in 2016 International Conference on Computer Communication and Informatics, ICCCI 2016, 2016.

[26] R. Amutha Priya, M. S. Nandhakumar, and M. Tech, "Attack prevention for spectrum sensing data falsification attacks in cognitive radio networks using arc."

[27] S. Ciftci and M. Torlak, "A comparison of energy for cognitive radios in fading environments," Wireless Communications, vol. 68, no. 3, pp. 553–574, 2013.