Wireless Engineering and Technology, 2016, 7, 67-74
Published Online April 2016 in SciRes. http://www.scirp.org/journal/wet
http://dx.doi.org/10.4236/wet.2016.72007

Performance of Analysis Cognitive Radio with Cooperative Sensing under Malicious Attacks over Nakagami Faded Channels

Hagar O. Shazly[1], Asmaa Saafan[2], Hesham El Badawy[2], Hadia M. El Hennawy[1]

[1]Faculty of Engineering, Ain Shams University, Cairo, Egypt
[2]National Telecommunication Institute (NTI), Cairo, Egypt
Email: hagaromar1@yahoo.com, asmaa.nti@gmail.com, heshamelbadawy@ieee.org, hadia.elhenawy@eng.asu.edu.eg

Received 4 February 2016; accepted 9 April 2016; published 12 April 2016

Abstract

The different realistic propagation channels are faced frequently the multipath fading environments. The main goal of this system design (cognitive radio network) is to improve the efficiency of spectrum access on a non-interfering basis. This system achieves high utilization for the limited spectrum in order to fulfill needs for all users' demands which are considered as a problem in wireless communications due to rapidly increasing in wireless applications and service. This system is exposed to attack due to the vulnerabilities existence in this system. So, the main outcome of this paper is to investigate the performance of the cooperative sensing in cognitive radio networks under malicious attacks over different channel impairments, and to illustrate the most suitable individual probability of detection $\left(\overline{P_{dNAK}}\right)$ in real faded channel by using Nakagami model. This paper illustrates the effectiveness of the attacks and fading on the performance of spectrum sensing process.

Keywords

Cognitive Radio, Cooperative Sensing, Malicious Attacks, Nakagami Faded Channels

1. Introduction

Cognitive Radio Networks (CRNs) are considered as promising technologies that utilize the unused spectra to enable much higher spectrum efficiency. An example of CRN is the usage of free spectrum (white spaces) in the television band where the television transmitter is considered as a primary transmitter, the television receivers

How to cite this paper: Shazly, H.O., Saafan, A., El Badawy, H. and El Hennawy, H.M. (2016) Performance of Analysis Cognitive Radio with Cooperative Sensing under Malicious Attacks over Nakagami Faded Channels. *Wireless Engineering and Technology*, **7**, 67-74. http://dx.doi.org/10.4236/wet.2016.72007

are considered as primary receivers and the secondary transmitters receivers are considered as the users who are not television subscribers but need to use the free spectrum in the television band for their own traffic. Where the secondary (unlicensed) users are utilize the licensed frequencies while the primary user (licensed) is absent. An introduction for this system is illustrated in [1]; different types of threats are discussed in [2]. To make this utilization, the spectrum sensing process is needed to recognize on the situation of the primary user. If the secondary user found that the primary user does not transmit, then the secondary user can transmit his own traffic. Otherwise, if the secondary user detects the presence of the primary user, the secondary user must stop his transmission or immigrate this band to another free band while simultaneously avoiding interference with the primary users. Some problems will be raised during this process. One of such problems is due to malicious attackers, which are presented in [3] [4], without detailed study about the cooperative spectrum sensing under malicious attack in case of the presence of channel impairments. When the primary user does not use the spectrum, a malicious user or attacker sends a signal with characteristics identical to the primary user signal therefore the secondary user may think that this signal is coming from the primary user. Thus, secondary user will be prevented from accessing the CRNs. The security of CRNs on the level of physical layer security is analyzed under malicious attacks and is presented in [3] [5] and [6]. But in the presence of channel impairments, this will affect the efficiency of cooperative spectrum sensing. In [6], different attack scenarios are proposed, a malicious user detection method to further improve the performance. It is shown that by exploiting the malicious user detection scheme, the system performance is improved significantly under various attacks. The channel impairments (Nakagami fading) are discussed in [7]. So, this paper investigates the behavior of CRNs with cooperative sensing process under malicious attacks during channel impairments which are not studied in details in [3] by using Nakagami model. A cooperative sensing is a robust method that can face the uncertainty in results. However, malicious users can attack the cooperative sensing process by reporting false information. The sensing rules are working on minimizing false alarm probabilities (Q_f) in order to reduce attacking risks and illustrate that for a fixed percentage of malicious users, the detection accuracy increases almost exponentially as the network size increases. The system of energy detection of unknown signal over different faded channels which the energy detection has been widely applied, then a closed form expression for the probability of detection (P_d) is presented in [7]-[9] not only over Rayleigh fading but also over Nakagami and Rician faded channels. Some assumptions about all users in cooperative spectrum sensing process are presented in [10]. The effect of cooperative spectrum sensing which considered as a critical issue of cognitive radio technology which it needs to detect the presence of primary users accurately and swiftly using many techniques for make a decision was discussed in [11]. New cooperative spectrum sensing process schemes were discussed in [12] [13]. Another technique about the cooperative spectrum sensing process denoted by q-out-of-n rule, where n denotes the number of users that cooperate in the network (the base station decides the presence of primaries if number of users (q) or more report "1") was illustrated in [14]. The goal of this paper is studying the performance of cooperative spectrum sensing over Nakagami faded distributions under malicious attack which is not illustrated in detailed in [3].

The rest of the paper is organized as follows. Section 2 illustrates the detection and false alarm probabilities of non-fading additive white Gaussian noise (AWGN). Section 3 discusses the average detection probability over faded channel. The cooperative spectrum sensing is presented in Section 4. The cooperative spectrum sensing with malicious attack is discussed in Section 5. The results and analysis are presented in Section 6. Finally, the paper is concluded in Section 7.

2. Detection and False Alarm Probabilities over AWGN Channels

Closed form expressions for both the individual probability of detection P_d and the individual probability of false alarm P_f over AWGN channels were presented in [7]-[9], as follows

$$P_d = P_r\left(Y > \lambda \middle| H_1\right) \tag{1}$$

$$P_f = P_r\left(Y > \lambda \middle| H_0\right) \tag{2}$$

where

Y = received signal strength.

H_1 = hypothesis that the primary signal successfully received.

H_0 = hypothesis that the primary signal not successfully received.

λ = is the received threshold to decide whether there is a primary user present or not.
P_d and P_f may be evaluated as follow in conjunction with [7]-[9].

$$P_f = \frac{\Gamma\left(u, \frac{\lambda}{2}\right)}{\Gamma(u)} \tag{3}$$

$$P_d = Q_u\left(\sqrt{2\gamma}, \sqrt{\lambda}\right) \tag{4}$$

where u = TW: time bandwidth product, γ is the instantaneous signal to noise ratio, Q_u is the generalized Marcum's Q_u function, Γ (,) is the incomplete gamma function [15].

3. Average Detection Probability over Faded Channel

The average detection probability is derived over Nakagami faded channels. The presented expressions are in a closed form by averaging the P_d in the AWGN over the signal to noise ratio (SNR) fading distribution following the criteria that was presented in [7]-[9]. P_f will not be affected heavily according to the different conditions. So, P_f will be approximately considered as the case of AWGN and this is in consistence with the presented work in [7]-[9].

Nakagami Channels

If the amplitude of the received signal (after the channel impairments effect and noise existence) follow a Nakagami distribution, then the PDF of γ follows a gamma PDF which was mentioned [7]-[9], will be shown as follows.

$$f(\gamma) = \frac{1}{\Gamma(m)}\left(\frac{m}{\overline{\gamma}}\right)^m \gamma^{m-1} \exp\left(-\frac{m}{\overline{\gamma}}\gamma\right), \quad \gamma \geq 0 \tag{5}$$

where m: is the Nakagami fading parameter and $\overline{\gamma}$ is the average signal to noise ratio. The average P_d in the case of Nakagami channels $\overline{P_{dNAK}}$ can now be obtained by averaging equation (4) over equation (5) as follows.

$$\overline{P_{d\,NAK}} = \int_0^\infty Q_u\left(\sqrt{2\gamma}, \sqrt{\lambda}\right) \cdot f(\gamma)\, \mathrm{d}\gamma \tag{6}$$

$$\overline{P_{d\,NAK}} = \alpha\left(G_1 + \beta\sum_{p=1}^{u-1}\left[\frac{\left(\frac{\lambda}{2}\right)^p}{2p!}\,{}_1F_1\left(m; p+1; \frac{\lambda}{2}\frac{\overline{\gamma}}{m+\overline{\gamma}}\right)\right]\right) \tag{7}$$

where ${}_1F_1$ (; ;) is the confluent hypergeometric function and where β, α are presented as follows.

$$\alpha = \frac{1}{\Gamma(m)2^{m-1}}\left(\frac{m}{\overline{\gamma}}\right)^m, \ \beta = \Gamma(m)\left(\frac{2\overline{\gamma}}{m+\overline{\gamma}}\right)^m \exp\left(-\frac{\lambda}{2}\right)\overline{\gamma}$$

Hence,

$$G_1 = \frac{2^{m-1}(m-1)!}{\left(\frac{m}{\overline{\gamma}}\right)^m}\frac{\overline{\gamma}}{m+\overline{\gamma}}\exp\left(-\frac{\lambda}{2}\frac{m}{m+\overline{\gamma}}\right)\left[\left(1+\frac{m}{\overline{\gamma}}\right)\left(\frac{m}{m+\overline{\gamma}}\right)^{m-1} L_{m-1}\left(-\frac{\lambda}{2}\frac{\overline{\gamma}}{m+\overline{\gamma}}\right) + \sum_{\upsilon=0}^{m-2}\left[\left(\frac{m}{m+\overline{\gamma}}\right)^{\upsilon} L_{\upsilon}\left(-\frac{\lambda}{2}\frac{\overline{\gamma}}{m+\overline{\gamma}}\right)\right]\right]$$

where L_v () is the Laguerre polynomial of degree v [15].

4. Cooperative Sensing

In order to improve the performance of spectrum sensing, different secondary users cooperate by sharing their sensing information (local observation) as shown in **Figure 1**. Secondary users only share their final 1-bit decisions (H_0 or H_1) to the central base station. If a free spectrum was detected, it reports "0" (primary user not present) otherwise "1". The base station collects all the reports and makes the final decision statistics by using different techniques as was mentioned in [8] [9] and [14]. So, it will send its final decision for all users in the CRN. This paper used the technique which was denoted by q-out of-n rule.

For simplicity, assume that all users have the same independent and identically distribution (i.i.d) fading condition with the same average signal to noise ratio ($\overline{\gamma}$), such that each user has an individual probability of false alarm P_f and an individual probability of detection P_d.

5. Cooperative Sensing under Malicious Attack

In the previous section, it was assumed that all users in the system are benign. There are number of malicious users sending false reports (sensing information) to the base station. Assume that there are k malicious users in the system and the base station was used the q-out-of-n rule for make a decision. In the worst case, all malicious users report "1" when the spectrum is actually unoccupied.

In the generalized sensing strategy, assume that the network consists of n active users including k malicious users. First, assume that malicious users can detect the primary signal with no errors and always report false information. Each node in the network performs spectrum sensing and reports its one-bit hard decision result to a base station (fusion center) through a control channel. The control channel is assumed to be error free ($P_e = 0$). The sensing result is either "1" which means that the primary user is present, or "0" which means that the band is not used by the primary. The fusion center is then responsible for making the final decision based on the received sensing reports from all users. In the q-out-of-m_s scheme, the fusion center randomly polls m_s out of n users and relies on q-out-of-m_s rule for final decision making (the fusion center decides that a primary is present if q or more out of the m_s polled users report "1"), then at least there should be q users reporting the presence of the primary signal in order to be able to detect it. The number of malicious users $d = \max(0, m_s + k - n)$ indicates that when the number of users being polled, m_s, is greater than that of the benign users, then there are at least $m_s - (n - k)$ copies of malicious reports received by the fusion center. The main objective is to minimize the overall false alarm rate (Q_f) while keeping the overall miss-detection (Q_m) below a certain predefined value quality of service (β). as was mentioned in [3] as illustrated in **Figure 2**, it was derived the overall false alarm probability Q_f and the probability of detection Q_d under two cases: 1) the sensing information that was sent correctly to the base station during a channel free of error, and 2) the sensing information was sent with error due to the channel impairments.

5.1. Report without Channel Errors

The malicious users always report false information. So, the attacking scenarios may be described as follows.

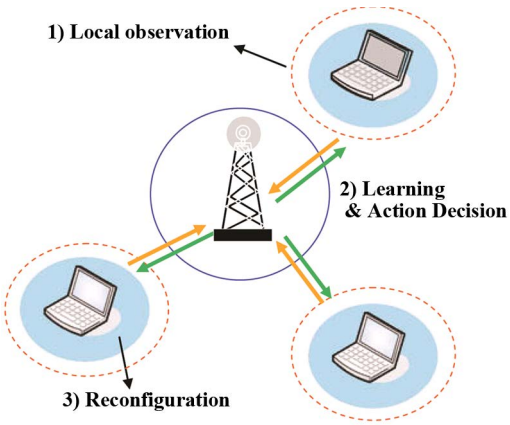

Figure 1. Cooperative spectrum sensing based-infrastructure CR networks [1].

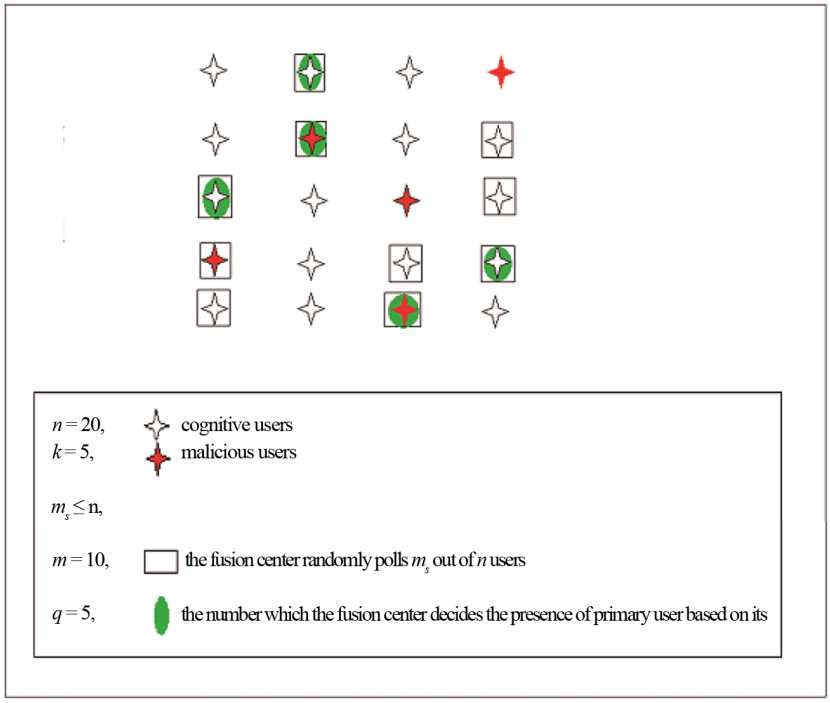

Figure 2. CRN in the existence of malicious users.

The first scenarios, part of these malicious users (*d* users) are considered as member of decision making group (*q* users). In this part the miss-detection probability ($Q_m = 1 - Q_d$) while depend only upon the malicious effect on the descion making group (*q*), by assuming that the channel is configure to be perfect one. So, any miss-detection or miss-orientation in decision making is resulting from the malicious sub-group (*d*) which deviate the decision making group (*q*). Then, the overall probability of detection Q_d under the generalized sensing strategy was mentioned in [3], and was represented as follows.

$$Q_d = \begin{cases} 0; \text{ if } (n-k) < q \\ \sum_{d=\max(0,m_s+k-n)}^{\min(k,m_s-q)} P_{k,n-k}^{d,m_s-d} \sum_{i=q}^{m_s-d} \binom{m_s-d}{i} p_d^i (1-p_d)^{m_s-d-i}; \text{ if } (n-k) \geq q \end{cases} \quad (8)$$

where

$p_{k,n-k}^{d,m_s-d} = \dfrac{\binom{k}{d}\binom{n-k}{m_s-d}}{\binom{n}{m_s}}$, as the probability of polling $m_s - d$ out of $n - k$ benign users and *d* out of *k* malicious users.

5.2. Report with Channel Errors

For more reality, the channel is not perfect all over the time due to the unstable channel characteristics of its behavior as the wireless media. In order to represent this phenomenon, the channel will be modeled as Nakagami-function which is presented in Equation (9). Then, the miss-detection probability in this case will be due to the conjunction effect between the channel imperfection as well as the malicious attackers. The presented work in this paper is focusing on this manner. So, the miss-detection probability may be represented by the collaboration or coexistence of the miss-detection due to malicious attack and the miss-detection due to the channel impairment this is represented by Equation (9), which in consistence with previously mentioned work in [3]. But the main difference between the current work and the presented work in [3], is that the current work is using a ge-

neralized channel model (Nakagmi model) whereas in [3], the channel miss-detection effect is taken as a fixed estimation of the overall detection probability. In other words, the current work will dedicate and deduce an analytical form to study and investigate the effect of practical channel impairments for different operational scenarios in case of malicious attackers are found.

Figure 3 illustrates the effect of malicious over the cooperative (collaborative) of miss-detection with channel impairments.

$$Q_d = \sum_{d=\max(0,m_s+k-n)}^{\min(k,m_s)} p_{k,n-k}^{d,m_s-d} \sum_{i=\max(0,d+q-m_s)}^{d} \binom{d}{i} p_{d,2}^{i} \left(1-p_{d,2}\right)^{d-i} \cdot \sum_{j=\max(0,q-i)}^{m_s-d} \binom{m_s-d}{j} p_{d,1}^{j} \left(1-p_{d,1}\right)^{m_s-d-j} \tag{9}$$

6. Results and Analysis

A validation of the Nakagami model had been mentioned in section 3 as illustrated in **Figure 4** which shows that the matching of the last three curves at different "*m*" value and $\overline{\gamma}$ = 20, u = 5 with the curves are mentioned in [7]. In order to use this system in [3] and applied its results. So, it is necessary to draw the Nakagami model at m = 2, $\overline{\gamma}$ = 5, u = 5 which is illustrated in the upper curve.

In this part the first objective is to define the effective region of the channel impairments on the overall detection probability. So, **Figure 5** is illustrating the probability of miss detection (due to malicious attack as well as channel impairments).

Figure 5 gives an inference about the effect of the channel impairments that may be neglected if the probability of detection is becoming more than 60%. So, the channel impairments effective reason may be discriminated into two main parts. The first part ($0 < P_d < 60\%$) the channel impairments are the dominant part. On the other hand, ($60\% < P_d < 100\%$) the malicious attacks are the dominant. So, the current work may be used to help the other researchers to use the operational parameters that P_d more than 60% and then can predict the probability of detection in spite of the channel conditions.

For further investigation, the current work is aiming to determine the most effective number of the decision making group (q_o), which is the semi optimized number of the decision making users that will bear on.

As was illustrated in paper [3], the cognitive system can efficiently utilize spectrum without causing too much interference to primary users. The interference level is determined by the QoS requirement of the primary system. By assuming that β = 0.01, it can be found that the optimal parameters are (q_{opt}, m_{opt}) = (14, 29), at which (Q_f, Q_m) = (0.00028, 0.0088). And this was proved in [4]. The optimal m_s is equal to or very close to the network size n

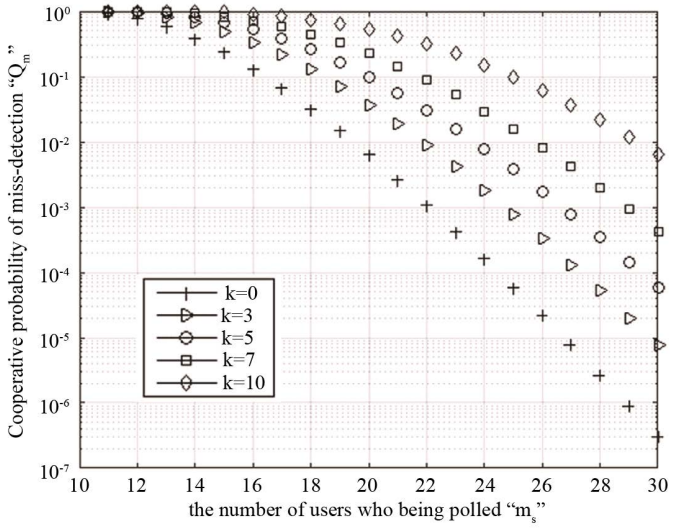

Figure 3. The effect of malicious attack over the cooperative of miss-detection with channel impairments.

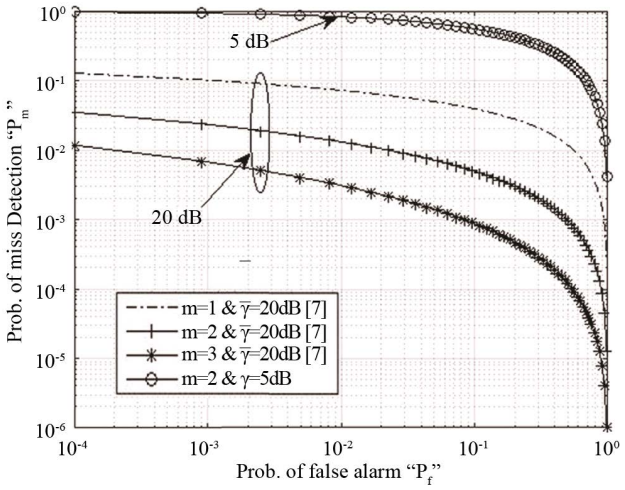

Figure 4. Complementary ROC curves for Nakagami channel at different m values (u = 5, $\bar{\gamma}$ = 5, 20 dB).

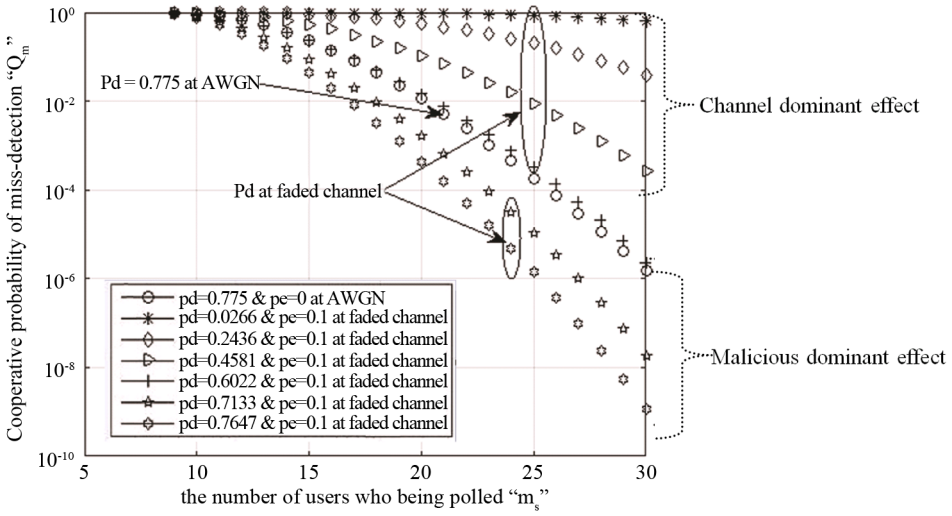

Figure 5. Cooperative probability of miss-detection under faded channel for different value of (P_{dNAK}) with P_d = 0.775 at AWGN at q = 9.

which almost independent on the percentage of malicious users, and the optimum q verses n follows an approximate linear function of n with different slopes depending on the percentage of malicious users. So, for network size n = 30 and the percentage of malicious users is 13%. Then the optimal q (*i.e.* q_o) is equal to 15, and at percentage of malicious users 20% the optimal q (*i.e.* q_o) is equal to 14, and at percentage of malicious users 27% the optimal q (*i.e.* q_o) is equal to 12. This illustrated that to improve the performance of system is not by increasing randomly q but there is a relation to be investigated in order to achieve the most probable optimal value of q. The main objective in cognitive radio is to minimize the overall false alarm rate (Q_f) while keeping the overall miss-detection (Q_m) below certain predefined value β (QoS).

7. Conclusions

This paper performs a reduction for operation parameter to get the suitable probability of detection (P_d = 0.775) against malicious attack in real faded channel using Nakagami model. The main contribution of this paper is to illustrate the suitable P_d that may be taken for malicious attack model and that give two benefits: the first benefits is making verification for proposed value of P_d mentioned in [3] without proof, and the second benefit is

making an investigation for how to use more realistic propagation model inside media which contain malicious attack and cooperative spectrum sensing.

So, as illustrated in Section 6, this paper proposed that P_d must be taken as (P_d = 0.775) and this in consistent with the previous published work in [3]. In addition, the current paper is investigating different operational parameters with faded channel. It is found that by increasing the P_d more than 60% the system will behave most likely as AWGN (case of high P_d) and more immunity for malicious attacks.

Further investigations are required to investigate the traffic characteristics with the effect of the malicious attacks on the obtained performance.

References

[1] Akyildiz, I.F., Lee, W.-Y. and Chowdhury, K.R. (2009) Ad Hoc Networks. Elsevier B.V., Atlanta, 810-836.

[2] Saxena, M., Thakur, R.S., Chourasia, K. and Bonder, V. (2013) Implementation of Cognitive Radio Network on the Platform of 4G Communication. *IRAJ International Conference*, Delhi Chapter, 26 May 2013, 37-41.

[3] Wang, H., Lightfoot, L. and Li, T. (2010) Onphy-Layer Security of Cognitive Radio: Cooperative Sensing under Malicious Attacks. 44*th Annual Conference on Information Sciences and Systems* (CISS), Princeton, 17-19 March 2010, 1-6.

[4] Ammar, M., Riley, N., Mehdawi, M., Fanan, A. and Zolfaghari, M. (2015) Physical Layer Security in Cognitive Radio Networks. *International Conference on Artificial Intelligence, Energy and Manufacturing Engineering* (*ICAEME*' 2015), Dubai, 7-8 January 2015, 7-8.

[5] Abdelhakim, M., Zhang, L., Ren, J. and Li, T.T. (2011) Cooperative Sensing in Cognitive Networks under Malicious Attack. *IEEE International Conference Acoustics, Speech and Signal Processing* (*ICASSP*), Prague, 22-27 May 2011, 3004-3007.

[6] Abdelhakim, M., Ren, J. and Li, T.T. (2012) Reliable Cooperative Sensing in Cognitive Networks. In: Wang, X., *et al*., Eds., *WASA* 2012, *LNCS* 7405, Yellow Mountains, 206-217.

[7] Digham, F.F., Alouini, M.-S. and Simon, M.K. (2003) On the Energy Detection of Unknown Signals over Fading Channels. *Proc. of IEEE International Conference on Conference on Communications* (*ICC*'03), **5**, 3575-3579. http://dx.doi.org/10.1109/icc.2003.1204119

[8] Hossain, M.A., Hossain, S. and Abdullah, M.I. (2012) Cooperative Spectrum Sensing over Fading Channel in Cognitive Radio. *International Journal of Innovation and Applied Studies*, **1**, 84-93.

[9] Hossain, M.A., Ahmed, S., Hossain, S. and Abdullah, I. (2012) Performance of Cooperative Spectrum Sensing for Different Number of CR Users in Cognitive Radio. *International Journal of Science and Research* (*IJSR*), **1**, 145-149.

[10] Ghasemi, A. and Sousa, E.S. (2005) Cooperative Spectrum Sensing for Opportunistic Access in Fading Environments. *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Baltimore, 8-11 November 2005, 131-136.

[11] Tabatabaee, S. and Vakili, V.T. (2013) A New Method for Sensing Cognitive Radio Network under Malicious Attacker. *Int. J. Communications, Network and System Sciences*, **6**, 60-65. http://dx.doi.org/10.4236/ijcns.2013.61007

[12] Bansal, T., Chen, B. and Sinha, P. (2014) FastProbe: Malicious Use Detection in Cognitive Radio Networks through Active Transmissions. 2014 *Proceedings IEEE INFOCOM*, Toronto, 27 April-2 May 2014, 2517-2525. http://dx.doi.org/10.1109/INFOCOM.2014.6848198

[13] Kalamkar, S.S., Banerjee, A. and Roychowdhury, A. (2012) Malicious User Suppression for Cooperative Spectrum Sensing in Cognitive Radio Networks Using Dixon's Outlier Detection Method. *IEEE National Conference Communicatios* (*NCC*), Kharagpur, 3-5 Febuary 2012, 1-5. http://dx.doi.org/10.1109/ncc.2012.6176787

[14] Varshney, P.K. (1997) Distributed Detection and Data Fusion. Springer-Verlag, New York.

[15] Gradshteyn, I.S. and Ryzhik, I.M. (2007) Table of Integrals, Series, and Products. 7th Edition, Academic Press, 1-1221.