Journal of Engg. Research **Vol. 5 No. (3) September 2017 pp.** *73-90*

تحسين الاستشعار الطيفي المتبادل لمحاكاة الهجمات من المستخدم الأساسي في شبكات الراديو المعرفية

إيف أوروموينز* ، أولوتايو أويريند و ستانلي منيني***

* كلية الهندسة الكهربائية والالكترونية وهندسة الحاسوب، جامعة كوازولوا نتال، ديربان، جنوب أفريقيا

** كلية الهندسة الكهربائية والهندسة المعلوماتية، جامعة ويتواترسراند، جوهانسبرغ، جنوب أفريقيا

* مراسلة المؤلف: *efe.orumwense@gmail.com*

الخلاصة

أصبحت شبكات الراديو المعرفية (CRN) على نحو متزايد تقنية هامة في شبكات الاتصالات اللاسلكية بسبب إمكاناتها وقدرتها على تحسين استخدام الطيف الترددي. هذه الشبكات تطبق تقنية الاستشعار الطيفي المكاني لتحديد النطاقات الشاغرة وتطبيق استراتيجيات لتقرر متى وكيف وأي نطاق تختار للاتصال. ولتحقيق ذلك، تتعرض الشبكة لتهديدا كبيرا والمعروف باسم محاكاة هجوم المستخدم الأساسي (PUEA). وفي هذا الهجوم يتم تقليد إشارة المستخدم الأساسي وذلك لتدمير عملية الاستشعار عن الطيف بواسطة مستخدمين مخربين وخداع المستخدمين الثانويين (SU) من نقل المعلومات في النطاقات الطيفية الشاغرة التي تم تحديدها. في هذه البحث، نهدف إلى تحسين أداء الاستشعار الطيفي من أجل التقليل من أضرار (PUEA) على الشبكة. في هذه الدارسة نقترح تقنية جديدة للكشف عن الطاقة للاستشعار الطيفي المكاني للشبكات الراديوية الإدراكية والتي سوف تساعد المستخدمين الثانويين في الكشف بدقة عن إشارات المستخدم الأساسي (PUEA) في النطاقات الطيفية الموجودة في الشبكة. دراسة مقارنة بين طريقتنا المقترحة والطرق الاخرى الحالية للاستشعار الطيفي المكاني، النتائج أظهرت أن الطريقة المقترحة يمكن أن تساعد بشكل فعال المستخدمين الثانوي في الحد من الأخطاء التي تحدث أثناء الكشف عن إشارات المستخدم الأساسي وأيضا التخفيف من أنشطة (PUEA).

Improved cooperative spectrum sensing under primary user emulation attacks in cognitive radio networks

Efe Orumwense*, Olutayo Oyerinde** and Stanley Mneney*

**School of Engineering, Electrical, Electronic and Computer Engineering, University of KwaZulu-Natal, Durban, 4041, South Africa.*

*** School of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg, 2050, South Africa.*

**Corresponding Author: efe.orumwense@gmail.com*

ABSTRACT

Cognitive Radio Networks (CRN) is increasingly becoming an important technology in wireless communication networks because of its potential and ability to improve the utilization of radio spectrum. Such networks implement co-operative spectrum sensing technique to locate vacant bands and apply strategies to decide when, how and in which band they may choose to communicate. In realizing this, the network is exposed to a major threat known as Primary User Emulation Attack (PUEA), in which malicious users may tend to destruct the spectrum sensing process by imitating the primary user signal and deceive the Secondary Users (SU) from transmitting in the identified vacant spectral bands. In this article, we aim to improve the cooperative spectrum sensing performance in order to mitigate the activities of PUEA in the network. We propose a new energy detection cooperative spectrum sensing technique in cognitive radio networks which will assist secondary users in accurately detecting primary user signals in spectral bands with (PUEA) present in the network. Comparing our proposed method to other existing cooperative spectrum sensing methods, the results show that our proposed technique can effectively assist secondary users in reducing the errors that occurs during detection of primary user signals and also mitigate the activities of (PUEA).

INTRODUCTION

In recent years, technologies and innovation in wireless networks have gained significant improvements and the struggle in accessing the electromagnetic spectrum has increased significantly. In a view to using this electromagnetic spectrum efficiently, an effective spectrum sharing technique termed as Dynamic Spectrum Access (DSA) was proposed (Akyildiz *et al*., 2006). The main objective of this technique is to dynamically allocate spectrum for efficient use by means of allowing Secondary Users (SUs) to access licensed frequency bands only when the licensed user or Primary User (PU) is not present in a Cognitive Radio (CR) environment.

In order to implement this technique, a spectrum sensing process is performed in the Cognitive Radio Network (CRN) where secondary users can sense a spectrum band for its availability. Multiple secondary users can also conduct their own local spectrum sensing independently and make a binary decision about the availability of the spectrum and then forwarded these binary decisions to a Fusion Center (FC) for fusion, a process known as cooperative spectrum sensing

(CSS). It has been shown that with the introduction of CSS in CRNs, the performance of spectrum sensing has significantly improved and there is more accurate detection of primary user signals (Ganesan & Li, 2005), (Ghasemi & Souza, 2005), (Mishra & Brodersen, 2006) (Orumwense *et al*., 2015a).

CSS however, is vulnerable to some threats and attacks which provide an opportunity for disruption of the network and degradation as regards the overall performance of the spectrum sensing process. One of the major attacks capable of ruining the CR spectrum sensing etiquette is known as the Primary User Emulation Attack (PUEA) (Chen & Park, 2006). In this kind of attack, a secondary user decides to be malicious by pretending to be a PU thereby transmitting signals similar to that of a PU. This will result in making good (non-malicious) SUs to accept that the PU is present while it is actually not (Orumwense *et al*., 2014). These good SUs, following the ideal spectrum etiquette, will vacate the spectrum band unnecessarily making the network unreliable or untrustworthy. PUEA also has a disrupting effect on the energy efficiency of the network and its obtainable overall performance (Orumwense *et al*., 2015b).

In order to curtail the menace of PUEA in CRNs, several research advances have been suggested and proposed in literature towards countering the various security threats associated with this attack. For instance, a location based defense (*LocDef*) method, where a non-interactive localization scheme was used to take estimation on the location of the transmitter and then compare it with the already known location of the primary transmitter is proposed in (Chen *et al*., 2008). (Liu *et al*., 2010) analysed an authentication method of a licensed user's signal which was done with the aid of cryptographic and wireless link signatures via a "*helper node*" sited in close proximity to the licensed user. In (Clancy & Goergen 2008), an approach for mitigating attacks capable of influencing the spectral environment in a CRN is also studied.. An analytical study of the feasibility of PUEA in a wireless fading environment using a group of cooperating malicious users in order to ascertain the lower bound on the probability of a successful PUEA was discussed by (Anand & Subbalakshmi 2008). Another strategy based on Received Signal Strength (RSS)-based defense strategy is applied to combat PUEA in a CRN using the analysis of belief propagation of location information as discussed in (Yuan *et al*., 2011). In (Chen *et al*., 2011), the authors analysed a CSS scenario with the existence of a PUEA in the network using optimal weights to maximize the detection probability.

Even though there have been significant amount of research that focused on the defense strategy and detection of PUEA in CRNs lately, less attention has been given to combating and mitigating PUEA in a CSS environment of a CRN. In this paper, we propose a model of CSS considering a PUEA, which like other CR users, also perform spectrum sensing and send primary imitative signals when the PU is not active. We assume each CR user sense the spectrum in the same manner. Then we propose an achievable new technique to reduce the total error rate in the system by formulating a method of energy detection in secondary users for the OR/AND rules to the fusion center. This is done so as to maximize primary user signal detection while limiting interference between users in the system. We also determined the ideal decision fusion rule that will reduce the total error rate with PUEA acting in the network. We further consider a scenario where the PUEA constantly sends fake signals in both vacant and occupied bands in order to selfishly acquire the band thus making the secondary user to vacate the existing band.

This paper aims at mitigating PUEA attacks in CRNs by optimizing the detection performance of secondary users when PUEA is present in the network using a proposed improved energy detection based cooperative spectrum sensing technique. The results obtained are compared with the conventional energy detection based cooperative spectrum sensing approach that was considered in (Hang *et al*., 2016) and other PUEA mitigation techniques to determine its performance.

The organization of the paper is presented as follows. Section 2 presents the system model for CRNs. In section 3, a cooperative spectrum sensing technique is formulated employing the OR/ AND fusion rules with the existence of a PUEA in the network. In section 4, an analysis of the considered spectrum sensing for energy detection where a technique is proposed to be employed in the local spectrum sensing process of each SU in the network is presented. Section 5 considers the case of an 'always present' attacker in the network. Discussions and simulation results are documented in section 6 while section 7 concludes the work with future recommendations.

SYSTEM MODEL

Considering a system as in Fig. 1 consisting of a PUEA existing in a CRN with number of cognitive radio secondary users and a fusion center. A PUEA is also present in the network with the objective of deceiving the secondary users. The PUEA is not oblivious of the radio environment and therefore sends misleading fake signals when the primary user is absent. The SUs employ energy detection sensing as its local spectrum sensing to detect spectrum holes and sends its decisions about the presence or absence of a PU to the FC. The FC receives these decisions from all the secondary users and fuse them together by using logic fusion rules (OR/AND fusion rules) so as to arrive at a final or grand decision. Since the PUEA tends to send similar signals like the primary user, we can take the signals being transmitted by the primary user and the PUEA as $\sqrt{P_p}x_p^k$ and $\sqrt{P_a}x_a^k$ respectively, and the power used in the transmission of the signals at kth time instant as P_p and P_a respectively.

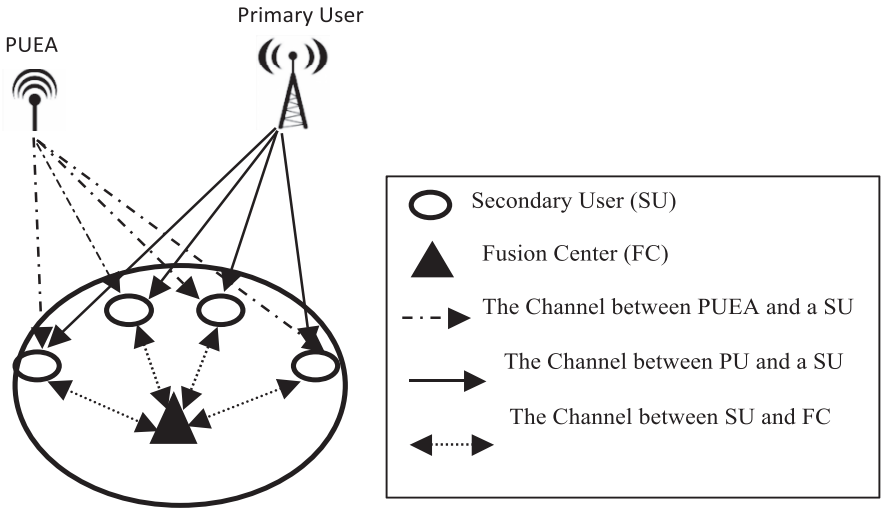

Fig. 1. A system model of a cognitive radio network with PUEA

Also, y_i^k is the received signal of an i^{th} SU in k^{th} time instant. H_1 and H_0 is respectively taken as the presence and absence of a primary user signal in our model while A_1 and A_0 is taken as the presence and absence of the PUEA signal respectively.

Since it is assumed that the PUEA does not transmit when the PU is present in the network, there will be three possible outcomes of the signal received y_i^k, at the i^{th} SU which is labelled: $z_1 = \{A_0, H_1\}$ $z_2 = \{A_1, H_0\}$ and $z_3 = \{A_0, H_0\}$.

Therefore,

$$y_i^k = \begin{cases} \sqrt{P_p} x_p^k h_{p,i}^k + n_i^k, & \text{under } z_1 \\ \sqrt{P_a} x_a^k h_{a,i}^k + n_i^k, & \text{under } z_2 \\ n_i^k & \text{under } z_3 \end{cases} \quad (1)$$

where n_i^k is taken as additive white Gaussian noise of the i^{th} SU also with a zero mean and variance $\sigma_{n,i}^2$, $h_{p,i}^k$ is regarded as the channel gain between the PU and i^{th} SU at k^{th} time instant and $h_{a,i}^k$ is the channel gain between the PUEA and i^{th} SU at k^{th} time instant. We assume block fading channels with channel coefficients that can be constant in every detection time, therefore, k can be omitted from $h_{p,i}^k$ and $h_{a,i}^k$. From (1), y_i^k will be a complex random variable under z_j for $j \in \{1, 2, 3\}$.

$$y_i^k \sim CN(0, \sigma_{j,i}^2) \text{under } z_j, j \in \{1, 2, 3\}, \quad (2)$$

we can clearly verify that

$$\sigma_{1,i}^2 = P_P \sigma_p^2 |h_{p,i}|^2 + \sigma_{n,i}^2 ,$$

$$\sigma_{2,i}^2 = P_a \sigma_a^2 \left|h_{a,i}\right|^2 + \sigma_{n,i}^2 ,$$

$$\sigma_{3,i}^2 = \sigma_{n,i}^2$$

COOPERATIVE SPECTRUM SENSING WITH PUEA PRESENCE

Among the pressing problems relating to spectrum sensing is channel sensing reliability (Famous *et al*., 2014), which occurs especially when SUs are shadowed or involved in deep fade. In order to improve on this problem, two or more secondary users can cohesively come together to conduct cooperative spectrum sensing. Quite a number of recent works in literature have shown that CSS significantly increases the detection probability in a cognitive radio network (Ganesan & Li, 2005), (Ghasemi & Souza, 2005), (Mishra & Brodersen, 2006). In this section, a spectrum sensing process that takes into consideration the existence of a PUEA which sends fake primary signals when the primary user is not active is introduced.

In a cooperative spectrum sensing process, every SU independently conducts its own local spectrum sensing and afterwards takes a binary decision and sends these binary decisions to a Fusion Center (FC) in order to arrive at a final or grand decision about the absence or presence of a PU user signal in a particular frequency band. There are many other fusion rules that can be employed at the FC (Kyperountas *et al*., 2013]. In this paper, the logic OR and logic AND rules are

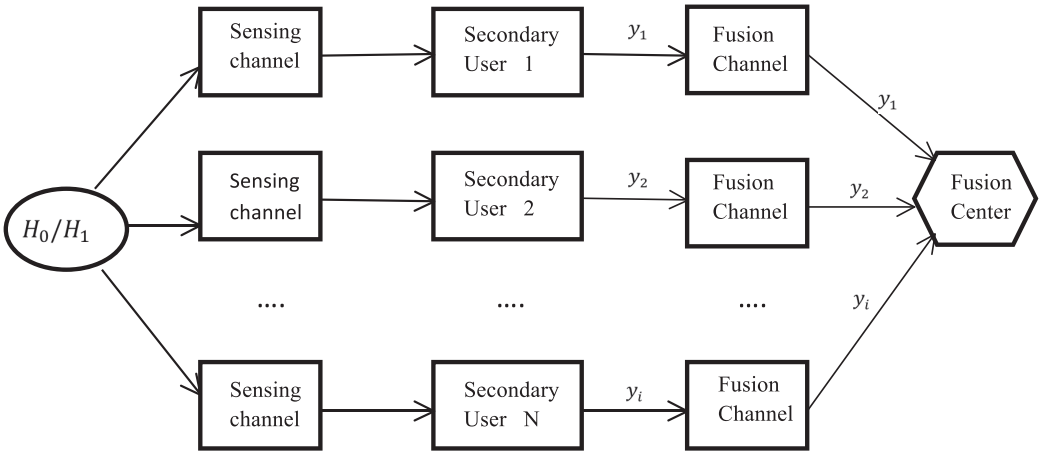

Fig. 2 : Cooperative Spectrum Sensing (CSS) in CRNs.

used because for a given a targeted probability of detection or a targeted probability of false alarm, each secondary user's threshold can easily be obtained. When using the OR fusion rule, the FC will affirm the presence of the PU when at least one of the secondary users detects the primary user signal, otherwise the spectral band is regarded as vacant. Also in the AND fusion rule, the presence of the PU is affirmed by the FC only when all the secondary users detect the primary user signal, otherwise the frequency band is regarded as vacant.

In the cooperative spectrum sensing algorithm outlined in figure 2, the detection probability (p_d) and the probability of false alarm (p_f) for the OR and AND fusion rules can easily be obtained. For the OR fusion rule, the (P_d^{OR}) and (P_f^{OR}) of the final decision taken by the fusion center using the local spectrum decisions can be written as

$$P_d^{OR} = 1 - \prod_{i=1}^{N}(1 - p_d^i)\,, \tag{3}$$

$$P_f^{OR} = 1 - \prod_{i=1}^{N}(1 - p_f^i)\,, \tag{4}$$

similarly, for AND fusion rule, the (P_d^{AND}) and (P_f^{AND}) of the final decision taken by the fusion center using the local spectrum sensing can also be given as

$$P_d^{AND} = \prod_{i=1}^{N} p_d^i\,, \tag{5}$$

$$P_f^{AND} = \prod_{i=1}^{N} p_f^i\,, \tag{6}$$

where p_d^i and p_f^i are regarded as the detection probability and the probability of false alarm respectively in the local spectrum sensing process of any of the th secondary user in the CRN. It can be expressed as,

$$p_d^i = p(D_{on}^i|H_1)\,, \tag{7}$$

and

$$p_f^i = p(D_{on}^i|H_0)\,, \tag{8}$$

where D_{on}^i indicates that an i^{th} secondary user has decided the primary user signal to be present and D_{off}^i will indicate that an i^{th} secondary user decides the primary signal is absent.

Since fake and misleading signals are sent by a PUEA when the primary user signal is not active, then that means the secondary users will receive the PUEA signals under H_0 only. When there is an attacker in the network, only the probability of false alarm $\left(p_f^i\right)$ will be affected. So when the presence or absence of an attacker A_1 and A_0 respectively is involved in equation (8), it gives

$$p_f^i = p\left(D_{\text{on}}^i\middle|A_0, H_0\right)p(A_0|H_0) + p\left(D_{\text{on}}^i\middle|A_1, H_0\right)p(A_1|\,H_0), \tag{9}$$

where $p(A_1|\,H_0)$ and $p(A_0|H_0)$ are the conditional probabilities as regards the presence and absence of fake PUEA signals respectively. If the primary signals are such that their transmission parameters are recognized by all, e.g TV towers, then it is assumed that $p(H_0)$ is known. So we can consider $p(A_0|H_0)$ and $p(A_1|\,H_0)$ as known values.

For easy and simple representation, we define

$$p(A_1|H_0) = \beta\,, \tag{10}$$

and

$$p(A_0|H_0) = 1 - p(A_1|H_0) = 1 - \beta\,, \tag{11}$$

therefore, equation (9) can be rewritten as

$$p_f^i = p\left(D_{\text{on}}^i\middle|A_0, H_0\right)(1 - \beta) + p\left(D_{\text{on}}^i\middle|A_1, H_0\right)\beta \tag{12}$$

PROPOSED ENERGY DETECTION BASED TECHNIQUE IN A COOPERATIVE SPECTRUM SENSING ENVIRONMENT WITH PUEA

In a typical cooperative spectrum sensing environment, an energy detection spectrum sensing technique is usually the most popularly used spectrum sensing technique due to the fact that it is easier to implement and does not require previous knowledge of the primary user signal (Akyildiz & Balakrishnan 2011). The secondary users conduct a local spectrum sensing technique in the presence of PUEA. It is assumed that every secondary user adopts the energy detection technique in which *M* samples of the energy of y_i^k are summed up at every detection interval,

$$Y_i = \sum_{k=1}^{M} |y_i^k|^2\,. \tag{13}$$

The value of Y_i is further compared to a threshold where every secondary user locally decides about the absence and presence of a primary user signal. The detection probability and the probability of false alarm for a *i*th secondary user in energy detection is expressed as:

$$p_d^i = p(Y_i \geq T_i|H_1)\,, \tag{14}$$

$$p_f^i = p(Y_i \geq T_i|H_0)\,, \tag{15}$$

where T_i is the threshold employed in energy detection of the i^{th} secondary user. In reference to equation (13), Y_i in energy detection is the sum of y_i^k squared denoted in equation (1). From equation (2), y_i^k is a Gaussian random variable with zero mean and a constantly known variance $\sigma_{j,i}^2$ under $z_j,\ \ j \in \{1,2,3\}$. So Y_i will be compliant with the central Chi-square (χ^2) distribution with $2M$ degrees of freedom and parameter $\sigma_{j,i}^2$.

$$Y_i = \begin{cases} \chi_{2M}^2\ (\sigma_{1,i}^2)\,, & \text{under}\ \ z_1 = \{A_0, H_1\} \\ \chi_{2M}^2\ (\sigma_{2,i}^2)\,, & \text{under}\ z_2 = \{A_1, H_0\} \\ \chi_{2M}^2\ (\sigma_{3,i}^2)\,, & \text{under}\ z_3 = \{A_0, H_0\} \end{cases} \tag{16}$$

In determining the performance of the analysed spectrum sensing method from the previous section, we apply the Neyman-Pearson criterion (Kay, 1998) in determining the detection probability using the energy detection based technique with cooperative spectrum sensing. The Neyman-Pearson technique presents a threshold for primary user signal detection contingent upon a constant probability of false alarm p_f^i. In reference to equation (9), the values of $p\left(D_{\text{on}}^i \middle| A_1, H_0\right)$ and $p\left(D_{\text{on}}^i \middle| A_0, H_0\right)$ can be obtained, which can be written in energy detection as

$$p\left(D_{\text{on}}^i \middle| A_1, H_0\right) = p(Y_i \geq T_i|A_1, H_0) \tag{17}$$

$$p\left(D_{\text{on}}^i \middle| A_0, H_0\right) = p(Y_i \geq T_i|A_0, H_0) \tag{18}$$

As in (Digham *et al*., 2007), equation (7) can be rewritten for spectrum sensing energy detection as

$$p_d^i = \frac{\Gamma(M, \frac{T_i}{\sigma_{1,i}^2})}{\Gamma(M)}\,, \tag{19}$$

where $\Gamma(.)$ is considered as the Gamma function and $\Gamma(.,.)$ as the upper incomplete Gamma function (Gradshteyn & Ryzhik, 2000). Therefore, equation (12) can also be rewritten as

$$p_f^i = \frac{\Gamma(M, \frac{T_i}{\sigma_{3,i}^2})}{\Gamma(M)}(1 - \beta) + \frac{\Gamma(M, \frac{T_i}{\sigma_{2,i}^2})}{\Gamma(M)}\beta\,. \tag{20}$$

In Neyman-Pearson criterion as seen in (Kay, 2008), in a given probability of false alarm, the ideal threshold that can maximize the detection probability can be derived if the given probability of false alarm is the actual considered probability of false alarm.

With PUEA considered in our proposed method, we can evaluate this method by comparing it to the conventional energy detection spectrum sensing method that does not consider an attacker in the system like the one proposed in (Hang *et al*., 2016). In evaluating the system performance, a metric relating to spectrum sensing called probability of error is used. The probability of error in CRNs is defined as the probability of the secondary users making wrong decisions in the spectrum sensing process. That is, when there is a declaration that the primary user is present when it is actually not present or a declaration that the primary user is absent when the primary user is sending signals. The probability of error for the OR FC rule can be expressed as

$$p_e^{OR} = p(H_0, D_{on}^{OR}) + p\left(H_1, D_{off}^{OR}\right),$$

$$= p(H_0)p_f^{OR} + \ p(H_1)p_m^{OR}\ , \tag{21}$$

while the probability of error for the AND FC rule, can be given as

$$p_e^{AND} = \ p(H_0)p_f^{AND} + \ p(H_1)p_m^{AND}\ . \tag{22}$$

THE CASE OF 'AN ALWAYS PRESENT ATTACKER' IN THE NETWORK'

There exist, an extreme case where a PUEA constantly sends fake signals in the cognitive radio environment irrespective of a band being vacant or occupied. That is, we can assume that the PUEA performs a kind of spectrum sensing to send fake signals both in vacant and occupied frequency band. The effect of the fake signals transmitted constantly by the PUEA will destroy the entire spectrum sensing process and prompting secondary users to make erroneous decisions and also cause interference in the network. In this case, there will be a possible outcome of $z_4 = \{A_1, H_1\}$ where both the primary user and PUEA are both transmitting in the cognitive radio environment. Then,

$$y_i^k = \sqrt{P_p}x_p^k h_{p,i}^k + \sqrt{P_a}x_a^k h_{a,i}^k + n_i^k, \text{ under } z_4, \tag{23}$$

where y_i^k is a complex random variable with mean of zero and a known variance of $\sigma_{4,i}^2$.

$$y_i^k \sim CN(0, \sigma_{4,i}^2) \text{ under } z_4 \tag{24}$$

and

$$\sigma_{4,i}^2 = \ P_P\sigma_p^2|h_{p,i}|^2 + P_a\sigma_a^2|h_{a,i}|^2 + \ \sigma_{n,i}^2$$

In the presence of a constant attacker sending fake signals over the licensed frequency band, the secondary users will received the PUEA signals under both H_0 and H_1 so the detection probability $\left(p_d^i\right)$ will now be affected by the presence of an attacker and $\left(p_f^i\right)$ will still be the same as analyzed in equation (9). $\left(p_d^i\right)$ is expressed as

$$p_d^i = p\left(D_{\text{on}}^i \middle| A_1, H_1\right)p(A_1|H_1) + p\left(D_{\text{on}}^i \middle| A_0, H_1\right)p(A_0|H_1) \tag{25}$$

$p(A_1|H_1)$ and $p(A_0|H_1)$ are now the new conditional probabilities as regards the presence and absence of the attacker. If we take $p(A_1|H_1)$ to be α for easy notation, then $p(A_0|H_1)$ will be $1 - \alpha$, , equation (25) can now be written as

$$p_d^i = p\left(D_{\text{on}}^i \middle| A_1, H_1\right)\alpha + p\left(D_{\text{on}}^i \middle| A_0, H_1\right)(1 - \alpha). \tag{26}$$

In the same way as in the previous section, formulating the CSS technique based on energy detection, Y_i will also be compliant with the central Chi-square (χ^2) distribution with $2M$ degrees of freedom and parameter $\sigma_{4,i}^2$ to be

$$Y_i \sim \chi_{2M}^2\ (\sigma_{4,i}^2), \text{under } z_4 = \{A_1, H_1\}, \tag{27}$$

and

$$p\left(D_{\text{on}}^i \middle| A_1, H_1\right) = p(Y_i \geq T_i | A_1, H_1) = \frac{\Gamma(M, \frac{T_i}{\sigma_{4,i}^2})}{\Gamma(M)}, \tag{28}$$

$$p\left(D_{\text{on}}^i \middle| A_o, H_1\right) = p(Y_i \geq T_i | A_0, H_1) = \frac{\Gamma(M, \frac{T_i}{\sigma_{1,i}^2})}{\Gamma(M)}, \tag{29}$$

So the probability of detection p_d^i in equation (26) can be rewritten as

$$p_d^i = \frac{\Gamma(M, \frac{T_i}{\sigma_{4,i}^2})}{\Gamma(M)}\alpha + \frac{\Gamma(M, \frac{T_i}{\sigma_{1,i}^2})}{\Gamma(M)}(1 - \alpha\ ). \tag{30}$$

SIMULATION RESULTS AND DISCUSSION

We implemented the simulations of our proposed energy based cooperative spectrum sensing algorithm with an existence of a PUEA in the network and compared the results with the cooperative spectrum sensing energy detection method used in (Hang *et al*., 2016) so as to determine its performance. We assume an identically and independently distributed (i.i.d) block Rayleigh fading channels and also the channel information is expected to be known to the cognitive radio network. At every secondary user, the average SNR is set to 0dB. The number of samples that is within a detection interval is $M = 3$, while $p(H_0)$ and $p(H_1)$ are taken as 0.8 and 0.2, respectively.

Fig. 3 illustrates the performance comparison of our proposed energy detection technique based spectrum sensing and the normal cooperative energy detection technique. Their performance is examined by setting which is the number of secondary users present in the network to 6 and using the OR fusion rule. As seen in the figure, our proposed method tends to have a lower probability of error when compared to the conventional energy detection cooperative spectrum sensing method.

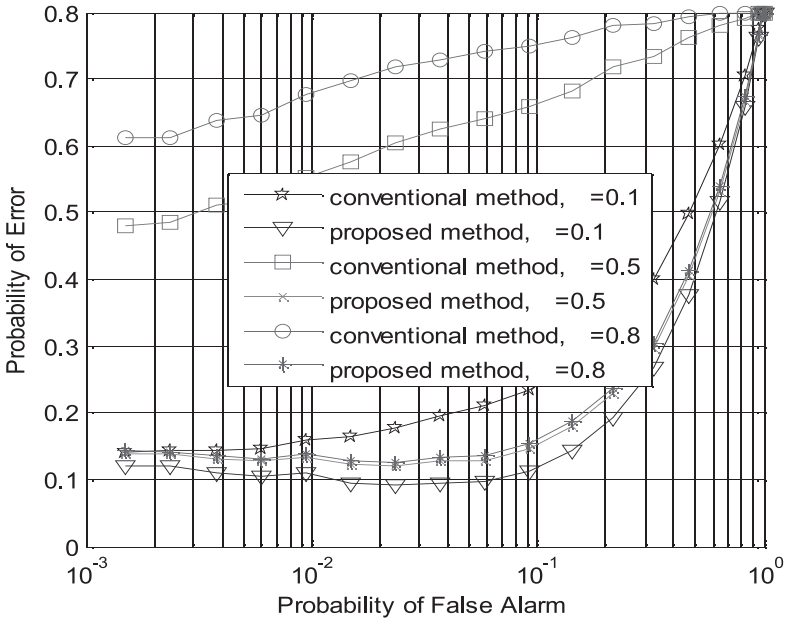

Fig. 3. Probability of error against the probability of false alarm for proposed and conventional method with N = 6 in the OR fusion rule.

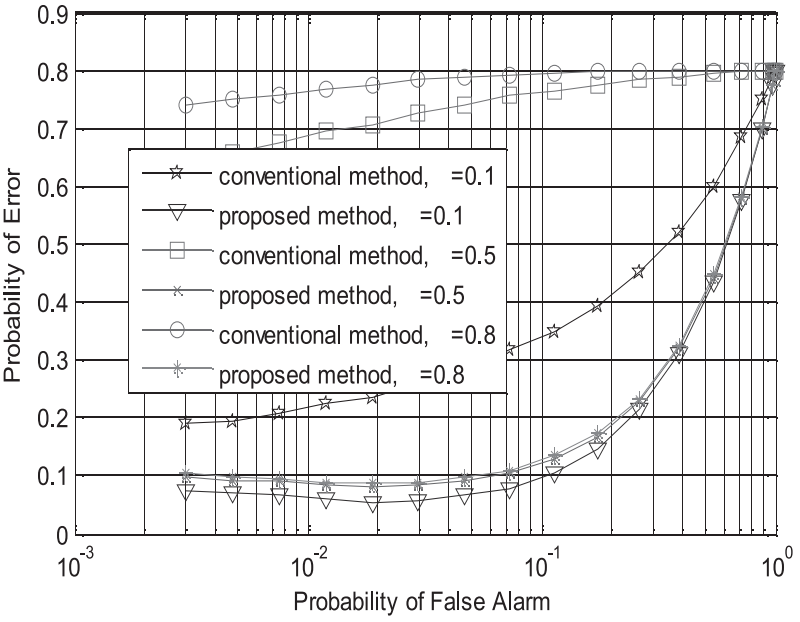

Fig. 4. Probability of error against the probability of false alarm for proposed and conventional method with N = 12 in the OR fusion rule.

With an increase in β , which is the probability of availability of PUEA signal in the network has a negative outcome on the performance of the considered spectrum sensing method. Fig. 4 also shows the probability of error versus the probability of false alarm between both spectrum sensing methods

in the OR fusion rule with the number of secondary users N increased to 12. As already known, a steady increase in the number of cooperative secondary users in the network is supposed to bring

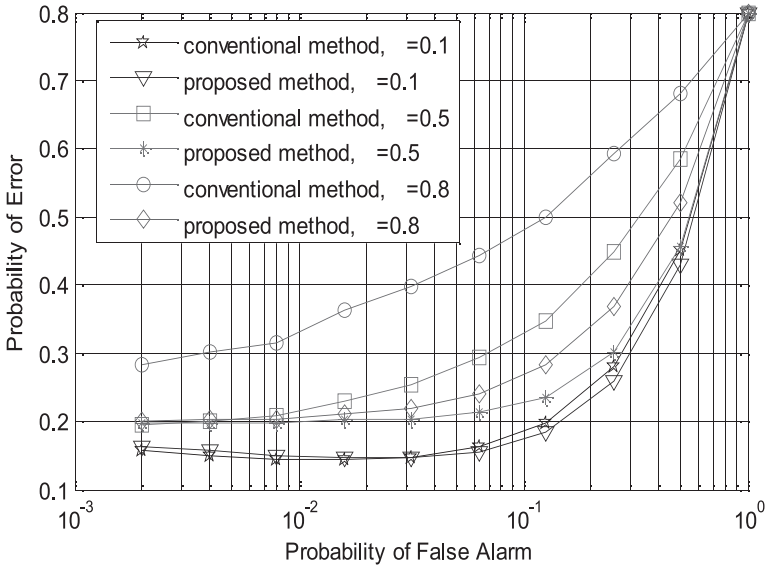

Fig. 5. Probability of error against the probability of false alarm for proposed and conventional method with N = 6 in the AND fusion rule.

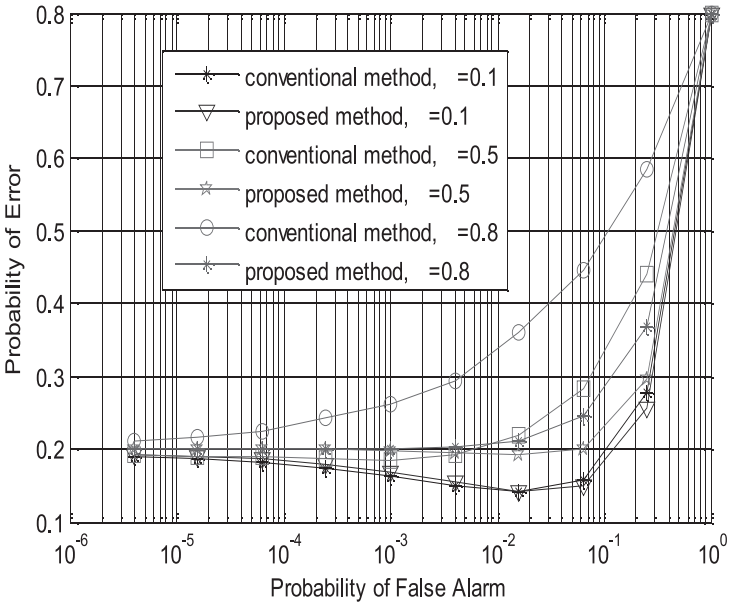

Fig. 6. Probability of error against the probability of false alarm for proposed and conventional method with N = 12 in the AND fusion rule.

about a steady increase in the detection probability or a decrease in the probability of error. But as seen in the figure, increasing the number of SUs in the network has an opposite effect on the

conventional method while our proposed method still maintains a very low probability of error.

In Fig. 5, our proposed energy detection technique based spectrum sensing method is also compared with the conventional energy detection spectrum sensing method considered for the AND fusion rule with number of SUs set at 6. We can see that our proposed technique performs better owing to the fact that the secondary users are aware of the fake signals in the network hence it has a very low probability of error even when there is an increase in β. Fig. 6 also shows the probability of false alarm and the probability of error in the AND fusion rule with the number of SUs N set at 12. Due to the increase in the number of cooperating SUs, it is seen that there is an improved performance in our proposed method with an existence of PUEA and the conventional energy detection cooperative spectrum sensing method is severely compromised by the presence of PUEA in the CRN. Also increasing β leads to an increased probability of error in the conventional cooperative energy detection spectrum sensing method.

Fig. 7 and fig. 8 shows the performance of our proposed method for the case of an attacker constantly sending fake signals to the cognitive radio network in the OR and AND fusion rule respectively. Our proposed spectrum sensing method is also compared with the conventional cooperative energy detection spectrum sensing method and also with the case of no attacker present in the network. From both figures, as expected, it is observed that there is a superior performance from our proposed method with the existence of a constant attacker present in the network.

From all the results, we can deduce that the conventional cooperative energy detection spectrum sensing method using the AND fusion rule often bring about a low probability of error in the network. This is so because in the AND fusion rule, all the SUs present in the network will have to declare the presence of a primary user signal before a final decision is made about the presence of a primary user. So if the conventional cooperative energy detection spectrum sensing method must be used, it should be used under the AND fusion rule. But again, our proposed spectrum sensing method has a better performance over the conventional cooperative energy detection spectrum

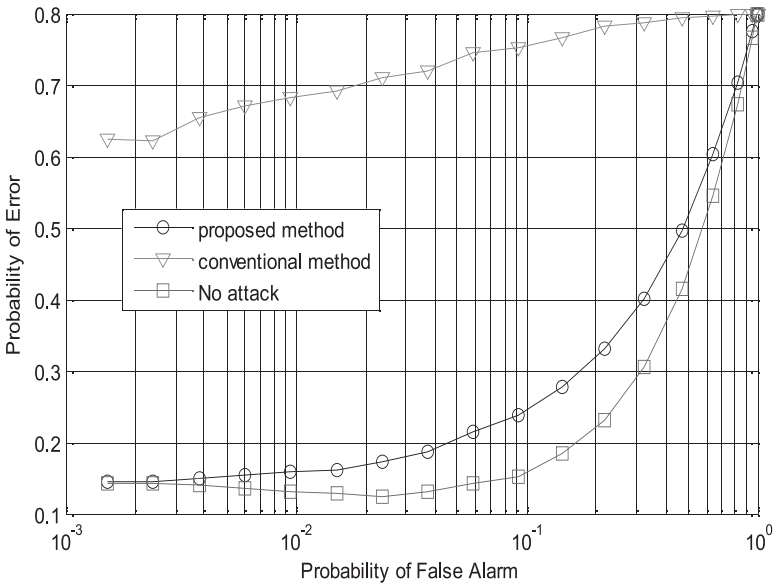

Fig. 7. Probability of error against the probability of false alarm for proposed and conventional method for an always present attacker in the OR fusion rule.

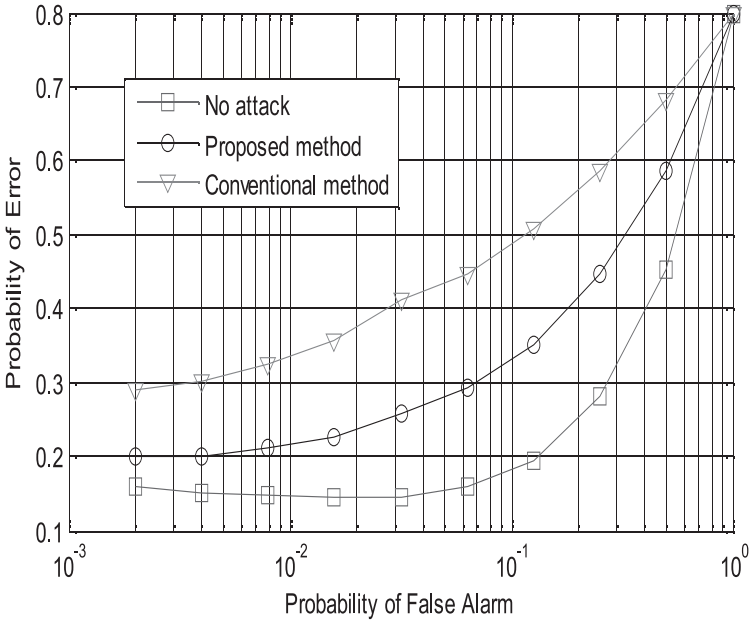

Fig. 8. Probability of error against the probability of false alarm for proposed and conventional method for an always present attacker in the AND fusion rule.

sensing method in both the OR and AND fusion rules but a much higher improvement in the OR fusion rule. So we can say that the best possible technique in improving CSS performance and mitigate PUEA in CRNs is achieved using our proposed spectrum sensing method in the OR fusion rule.

In a view to also evaluate and determine the performance of our proposed energy detection cooperative spectrum sensing technique, a table of comparison is provided in Table 1 to compare our proposed method with other techniques that includes PUEA mitigation available in literature (Hang *et al*., 2016), (Alahmadi *et al*., 2013), (Jin *et al*., 2012), (Zhao *et al*., 2009), (Huang *et al*., 2010). The comparison is carried out putting major factors that is important in achieving a successful CSS and PUEA mitigation in cognitive radio networks into consideration.

Table 1: Comparison with other Techniques

PUEA Mitigation Solutions	Category of Solution	Protection Mechanism Suggested	Energy Efficiency	Detection Probability	Interference	Evaluation
Our Proposed Technique	Centralized/ Cooperation based	Energy detection based mechanism capable of identify PUEA, decrease errors made by secondary users and mitigate an always present attacker	Solution is energy efficient as multiple secondary users are involved in cooperative spectrum sensing.	Detection probability is high as probability of secondary users making wrong decisions is low.	Interference with primary user is very low	It brings about a very low probability of error in the network and efficient spectrum usage.
Proposed Technique in [23]	Distributed or individual node based practical solution	An AES DTV scheme is developed where a reference signal is produced at the transmitter and used as the sync bytes of each DTV data frame to recognize authorized primary users.	Energy efficiency is not taken into consideration	Detection probability is relatively high as primary users can be detected easily	Interference is relatively low.	Only applicable in cognitive radio networks operation in the white spaces of digital TV bands.
Proposed Technique in [24]	Distributed or individual based analytical solution	An investigative technique employing Neyman-Pearson composite hypothesis test and Wald's sequential probability ratio test to combat PUEA.	Energy efficiency is low because of the existing distance from the primary to the secondary users and also the effects of multipath are ignored.	There is a low Probability of detection due to the high probability of false alarm.	Interference is high because of the high probability of alarm.	It is just an analytical approach. Including Wald's sequential probability ratio test adds complexity to the solution.
Proposed Technique in [25]	Distributed or individual node based practical solution	The carrier phase noise is extracted and directly put to use so as to detect the transmitter.	Energy efficiency is relatively high as phase noise is applied directly to identify transmitter	Probability of detection is relatively very low since only the phase noise parameter is used to differentiate users.	Interference is not taken into consideration	The performance can be seriously degraded by noise attenuation
Proposed Technique in [26]	Distributed or individual node based practical solution	Time Difference of Arrival (TDOA) is employed and also the Frequency Difference of Arrival (FDOA) for location verification.	Energy efficiency is high since the mechanism involves low working complexity	Probability of detection is low due to estimation of location	Interference is relatively low	Only relevant in the scenario where location of Primary User and Secondary User is static.
Proposed Technique in [14]	Centralized/Cooperation based	A cooperating spectrum sensing approach in deriving the optimal weights for a combining scheme to increase detection probability.	It is energy efficient since multiple cognitive radio users are involved in sensing	Detection probability is optimized under the probability of false alarm constraint.	Interference level is not certain as it is assumed that PUEA has already been detected.	Only one fusion center rule was used and does not consider other fusion rules.

CONCLUSION AND FUTURE RECOMMENDATION

This paper focuses on improving CCS in CRNs and mitigating one of the common and perilous attacks associated with the network which is Primary User Emulation Attack (PUEA). CRNs come under attack when primary licensed users are not present in the network and an attacker sends primary-like signals disrupting the network. In this article, we introduced an energy detection spectrum sensing method under PUEA which can enable secondary users make correct and right decisions about the absence or presence of a primary user signal in a spectral band with spectrum sensing rules (OR and AND fusion rules) employed in the FC to give final decisions in the network. The proposed spectrum sensing method is also applied to the case of an attacker that constantly sends fake signals in the CRN.

In evaluating the performance of the method proposed, it is compared with a method that does not acknowledge the existence of PUEA in the CRN. Simulation results show that a significant reduction in the error probability for both OR and AND fusion rules can be achieved using the proposed method. To also achieve an optimal performance in mitigating PUEA in CRNs, our proposed spectrum sensing method in the OR fusion rule can be employed.

This work primarily focuses on security challenges facing cognitive radio networks especially PUEA. However, the concept of PUEA is relatively new and there is still much work to do in this regard. The other possible areas of research that can be explored are examining a case of different channel estimation errors and also considering a case of multiple attackers in a cooperative spectrum sensing environment and investigating the corresponding impacts on the detection and mitigation performance.

REFERENCES

Akyildiz, I. Lee, W. Vuran, M. & Mohanty, S. 2006. NeXt generation/ dynamic spectrum access/cognitive radio wireless networks: A survey, Computer Networks: The International Journal of Computer and Telecommunication Networking, **50**(13): 2127–2159.

Akyildiz, I. Lo, B. & Balakrishnan, R. 2011. Cooperative spectrum sensing in cognitive radio networks: a survey. Journal on Physical Communications. **11**(1): 40-62.

Alahmadi, A. Abdelhakim, M. Ren J. & Li, T. 2013. Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard. Proceedings of the IEEE Global Communications Conference, Atlanta, USA.

Anand, S. Jin, Z. & Subbalakshmi, K. P. 2008. An analytical model for primary user emulation attacks in cognitive radio networks. Proceedings of the IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN). Chicago, USA.

Chen, C. Cheng, H. & Yao, Y. 2011. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack, IEEE Transactions on Wireless Communications. **10**(7): 21352141-.

Chen, R. Park, J. M. 2006. Ensuring trustworthy spectrum sensing in cognitive radio networks, IEEE workshop on networking technologies for software defined radio networks. Vancouver, USA.

Chen, R. Park, M. J & Reed J. H. 2008. Defense against Primary User Emulation Attacks in Cognitive Radio Networks, IEEE Journal on Selected Areas in Communications, **26**(1): 25-37.

Chen, Z. Cooklev, T. Chen, C. & Pomalaza-Raez, C. 2009. Modeling primary user emulation attacks and defenses in cognitive radio networks, Proceedings of the IEEE International Performance Computing and Communications Conference (IPCCC'2009), Arizona, USA.

Clancy T. & Goergen, N. 2008. Security in cognitive radio networks: Threats and Mitigation, Proceedings of the International Conference on Cognitive Radio Oriented Wireless Networks and communications, (CrownCom) Singapore.

Digham, F. Alouini, M. & Simon, M. 2007. On the energy detection of unknown signals over fading channels, IEEE Transactions on Communications. **55**(1): 21-24.

Famous, A. Sagduyu, Y. & Ephremides, A. 2014. Reliable spectrum sensing and opportunistic access in network-coded communications. IEEE Journal on Selected Areas in Communications. **32**(3): 400410-.

Ganesan, G. and Li, Y. G. 2005. Cooperative spectrum sensing in cognitive radio networks, Proceedings of the IEEE Symposium New Frontiers in Dynamic Spectrum Access Networks (DySPAN'05), Baltimore, USA.

Ghasemi, A & Sousa, E.S 2005. Collaborative spectrum sensing for opportunistic access in fading environments, Proceedings of the IEEE Symposium New Frontiers in Dynamic Spectrum Access Networks (DySPAN'05), Baltimore, USA.

Gradshteyn I. & Ryzhik, I. 2000. Table of integrals, series and products, 6th edition. New York. Academic Press.

Hang, G. Wang, J. Luo, J. Wen, C. Li, H. Li, Q & Li, S. 2016. Cooperative Spectrum Sensing in Heterogenous Cognitive Radio Networks Based on Normalized Energy Detection. IEEE Transactions on Vehicular Technology. **65**(3): 1452- 1463.

Huang, L et al. 2010. Anti-PUE attack based on joint position verification in cognitive radio networks. Proceedings of the International Conference on Communications and Mobile Computing (CMC). Shenzhen, China.

Jin, Z Anand, S & Subbalakshmi, K. P. 2012. Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. IEEE Transactions on Mobile Computing and Communications, **60**(4): 74 -85.

Kay, S. 1998. Fundamentals of statistical signal processing: detection theory. 2. Englewood Cliffs, NJ; Prentice-Hall.

Kyperountas, S. Correal, N. & Shi, Q. 2013. A Comparison of Fusion Rules for Cooperative Spectrum Sensing in Fading Channels. EMS Research, Motorola.

Liu, Y. Ning, P. & Dai, H. 2010. Authenticating Primary Users Signals in Cognitive Radio networks via integrated cryptographic and wireless link signatures, Proceedings of the IEEE Symposium on Security and Privacy, California, USA.

Mishra, M. Sahai, A. & Brodersen, R. 2006. Cooperative sensing among cognitive radios, Proceedings of the IEEE International Conference Communications, Istanbul, Turkey.

Orumwense, E. F. Oyerinde, O. Mneney, S. 2014. Impact of primary user emulation attacks on cognitive radio networks, International Journal on Communications Antenna and Propagation, **4**(1): 19-26.

Orumwense, E. F. Afullo T. & Srivastava, V. 2015a. Secondary user energy consumption in cognitive radio networks Proceedings of the IEEE AFRICON conference. Addis Ababa, Ethiopia.

Orumwense, E. F. Afullo, T and Srivastava, V. 2015b. Effects of malicious users on the energy efficiency of cognitive radio networks. Proceedings of the Southern African Telecommunications Networks and Applications Conference (SATNAC), Hermanus, South Africa.

Yuan, Z. Niyato, D. Li, H. & Han, Z. 2011. Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks, Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC). Quintana, Mexico.

Zhao, C. Wang, W. Huang L. & Yao, Y. 2009. Anti-PUEA attack based on the transmitter fingerprint identification in cognitive radio. Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM). Bejing, China.

Submitted: 17/05/2016
Revised : 09/11/2016
Accepted : 29/11/2016