ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

EFFICIENT DETECTION OF SELFISH ATTACKS IN COGNITIVE RADIO NETWORKS USING COOPON ALGORITHM

R.Sujitha
PG Scholar
Department of ECE,
Oxford Engineering College
Trichy, tamilnadu, India

N.Poornima
Assist.prof
Department of ECE.
Oxford Engineering College
Trichy, tamilnadu India

Abstract:

Cognitive radio is a solution for the spectral crowding problem by introducing opportunistic usage of frequency bands that are not occupied by licensed primary users. Cognitive radios determine vacancy portions of licensed spectrum, and utilize such portions for secondary use in order to meet regulatory constraints of limiting harmful interference to licensed Wireless systems Cognitive radio is an opportunistic communication technology designed to help unlicensed users to utilize maximum available bandwidth.Little research has been done on cognitive radio regarding security and more research has been done regarding the specrum sensing and allocation.Selfish cognitive radio attacks is considered as a serious security problem because they will significantly degrade the performance of the cognitive radio networks.In this paper we identify a new type of attack in cognitive radio networks known as the selfish attack and a technique known as COOPOON is used to overcome the selfish attack.It takes place only in multichannel resourses.

Keywords--- Cognitive Radio, COOPON, Selfish Attacks ,Channel Allocation

1. INTRODUCTION

Cognitive radios are designed in order to provide highly reliable communication for all users of the network, wherever and whenever needed and to facilitate effective utilization of the radio spectrum. Cognitive radio is a radio that can change its transmitter parameters based on interaction with environment in which it operates. Spectrum sensing aims to determine spectrum availability and the presence of the licensed users (also known as primary users)[1]. A major challenge in cognitive radio is that the secondary users need to detect the presence of primary users in a licensed spectrum and quit the frequency band as quickly as possible if the corresponding primary radio emerges in order to avoid interference to primary users. In practice, the unlicensed users, also called secondary users (SUs), need to continuously monitor the activities of the licensed users, also called Primary Users (PUs), to find the spectrum holes (SHs),which is defined as the spectrum bands that can be used by the SUs without interfering with the PUs. This procedure is called spectrum sensing. There are two types of SHs, namely temporal and spatial SHs, respectively. A temporal SH appears when there is no PU transmission during a certain time periods can use the spectrum for transmission. A spatial SH appears when the PU transmission is within an area and the SUs can use the spectrum outside that area. To determine the presence or absence of the PU transmission, different spectrum sensing techniques have been used, such as matched filtering detection, energy detection, and feature detection.

The secondary users who transmit to emulate the primary transmitter are referred to as "malicious users"whereas the secondary users who evacuate

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

the spectrum upon sensing from the primary user or the malicious user is termed as good secondary users such an attack by the malicious users on secondary users is called as primary user emulsion attack.This leads to poor usage of spectrum for authorized users.

In this paper, we identify a new type of attack known as selfish attack and it can be overcome by using COOPON technique. In selfish attack the secondary users accomdates multiple channel. Each SU will regularly broadcast the current multiple channel allocation information to all its neighbouring secondary users and they will broadcast the current multiple channel allocation information including the number of channels.

.

The selfish SU will broadcast fake information on available channels in order to pre-occupy them. The selfish SU will send the large number of hannels.The COOPON techniques are used to detect the selfish attacks that are present in cognitive radio networks,The proposed scheme combats the primary user emulsion attacksand enables more robust system operation and efficient spectrum sharing. The effectiveness of the proposed approach is demonstrated through both theoretical analysis and simulation examples. It is shown that with the AES-assisted DTV scheme, the primary user, as well as malicious user, can be detected with high accuracy and low false alarm rate under primary user emulation attacks.

2. HYPOTHESIS TESTING

The major task of spectrum sensing is to determine whether the PU signal is present or not in the specified spectrum band. The CR detection problem can be considered as hypothesis testing. In this, CR has to distinguish between the PU signal and noise signal. The binary hypothesis testing model can be described as

$$y(t) = n(t) ; \quad \text{H0 hypothesis} \quad (1)$$

$$y(t) = x(t) + n(t) ; \quad \text{H1 hypothesis} \quad (2)$$

Hypothesis H0 indicates, the received signal consist of noise only whereas hypothesis H1 determines that the received signal contains both PU signal and noise. In binary hypothesis test, the CR user has to choose between these two hypotheses on the basis of test statistic. A test statistic is a function of the received signal, which is compared against the threshold. To achieve better performance , the selection of threshold value should depends on the noise power and the number of samples.

$$E = 1/N \sum x(n)^2 \quad (3)$$

3. PROPOSED SYSTEM

In this paper we have detected the primary user emulsion attacks using the advanced encryption standard, The receiver regenerates the encrypted reference signal, with the secret key and the third party cannot interfere with the primary user.

A correlation detector is employed, where for primary user detection, the receiver evaluates the crosscorrelation between the received signal r and the regenerated signal s for the malicious user detection the receiver evaluates the autocorrelation of the received signal r,

The cross-correlation of two random variables **x** and **y** is defined as:

(4)

Under PUEA, the received signal can be modeled as:

4. SYSTEM MODEL

There are two types of attackers: 1) a selfish SU that wants to use a channel that exclusively launches the primary user emulsion attack and to drive the secondary users out of the channel 2)the malicious user wants to cause the denial of service to the cognitive radio networks.The main common objective of this to cause the denial of service.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

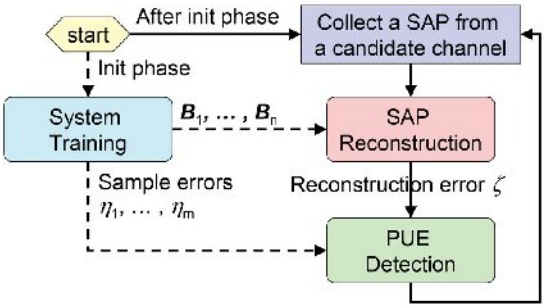

Fig. 1. SPARS Architecture

In this paper we adopt a fingerprint to track the transmitted signal and hence SPARS technique is applicable for both static and mobile primary users. The received signal extracts the finger print and it records the ON and OFF periods of the signal to be stored as the data base which includes the finger print of the signal. This ingerprint will serve as the transmitter ID independently carries out spectrum sensing on every channel. Every secondary user will record the ON and OFF periods of every primary user signal to be transmitted. Spectrum sensing techniques are carried on the basis of time domain. The ON or OFF periods are considered as a random variable. TSs is considered as as the duration of spectrum sensing cycle.

An ON or OFF period is then a discrete dom Variable to be represented as the number of time unit *Ts*. SPARS run periodically depending upon the time domain. SPARS is used to detect the transmitted signal whether the attacker is present are not.The ON and OFF periods determine the SPARS.

(6)

Comparing to the Primary user emulsion attacks, COOPON algorithm, simulation results show that the SPARS detection algorithm can make a lower collision probability between the primary user and the cognitive user, despite a little increasing of the spectrum unavailable probability. Finally by proposed Improved Double threshold Energy detector, by which reduction in the probability of detection is less reduced. In past few decades the need for high data rate wireless communication has experienced a booming growth indicating a huge commercial potential. The growing demand of wireless devices is restricted by the spectrum access policy of radio regulatory regime. Large part of the spectrum is allocated for exclusive use by the licensed users and only a small portion of the spectrum is given for open access. The commercial success of the unlicensed spectrum has encouraged FCC to frame policies towards more flexible and open spectrum access. Most of the licensed bands suffer from under-utilization and less spectral occupancy of spectrum. The exclusive usage criteria in the licensed spectrum have resulted in wastage of limited and precious spectrum. The so called „spectrum scarcity and „limited radio spectrum is a result of the way the spectrum is being regulated.

5.TYPES OF SELFISH ATTACK

5.1 Attack Type1

.

Selfish attacks depends on the CR spectrum resources.This type of attack is the signal fake selfish attack.This is designed to prohibit a legitimate secondary user from sensing the available spectrum bands by sending the faked primary user signals.The selfish secondary user will emulate the characteristics of the primary signals.It overhears the faked signals and it makes a decision of primary user is active so that the secondary user legiminate the sensing of the available channels.This attack is performed only on the basis of the transmission of the selfish user in regardless with the number of channels.

5.2 Attack Type 2

Type 2 attacks are also a selfish SU emulating the characteristics of signals of a primary user but it is carried in the case of dynamic multiple channel access.The secondary users directly sense the current operating band to know whether the primary user is active are not.The secondary user continuosly switch on the available channels. The attacker limit the legiminate secondary users from identifying the available spectrum channels.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

5.3 Attack Type 3

. In Type 3, called as the channel pre-occupation selfish attack,this type of attacks occur in the communication environment which is used to broadcast the current available channel information to the neighbouring nodes for transmission.The selfish secondary user will broadcast the available channel lists to its neighbouring secondary users.It will send the list of occupied channels.
attack.

6 . ATTACK MECHANISM

In a cognitive radio network, the common control channel is used to broadcast and exchange managing information and certain parameteres are used to manage the cognitive radio networks among the secondary adhoc users.The CCC is a channel that is dedicated only for exchanging managing information and parameters.It also contains the other neighbouring users channel information.Type3 attacks are used to separate the channel allocation information lists through individual CCC to the left handed side legal selfish user and the right hand side LSU.The list contains the channel information of all the neighbouring nodes.

The secondary user will use the list information distributed through CCC to access channels for transmission.A selfish secondary node will use the CCC for selfish attacks by sending fake current channel allocation information to its neighbouring secondary users.When the attackers try to preoccupy the available channels they will broadcast the available used spectrum channels.The other Legimitate secondary users are prohibited.

The available channel resources are limited in using them.In third attack the selfish secondary user sends a current fully occupied list to the right hand side of the LSU eventhough it only occupy the other three channels.The right hand side legitimate secondary user will be prohibited completely accessing the available channels.The SSU will broadcast partially the preoccupied channel list and it only uses fewer channels.This will currently use the three channels for broadcasting the left hand side LSU which uses the four channels.In this case legitimate secondary users will access one available channel out of the five maximum but they are prohibited by using one channel that is available.

7. DETECTION MECHANISM

7.1 Use Of Channel Information

In this paper we consider the COOPON algorithm which is to be designed for a cognitive radio network.It has distributed and management characteristics .This algorithm is based on the allocation information among neighbouring secondary users.Target nodes are present.The neighbouring nodes will scan any selfish attack of the target node.

T-Node 2 reports that there are two channels currently that are in use while N-Node3 reports to be currently in use.N-Node 4 receives the faked channel allocation information from the target node.The neighbouring secondary users will make use of te decision that the target secondary user is the selfish attacker.All the neighbouring secondary users sum the numbers of currently used channels sent by themselves and other neighbouring nodes.

Individual neighboring nodes will compare the summed numbers sent by all neighboring nodes to the summed numbers to be sent by the target node to check if the target SU is a selfish attacker.This detection mechanism is carried out through the cooperative behaviour of the neighbouring nodes.Once a neighbouring secondary user is chosen as a target node and the detection action is completed another neighbouring secondary user will be selected as a target node for the next detection action.

Detection of existing selfish technologies is likely to be uncertain and less reliable, because they are based on estimated characteristics of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

tochastic signals., Our proposed COOPON selfish attack technique of detection method is very reliable since it is based on deterministic information., COOPON has a drawback.When there is more than one neighboring selfish nodeCOOPON may be less reliable for detection, because twoneighboring nodes canpossibly exchange fake channel allocation of the neighbouring node to serve more information. But if there are more legitimate neighboring nodes in a neighbor, a better detection accuracy rate can be expected, because more accurate information can be gathered and more legitimate the secondary user.

An important requirement for cognitive users is that they should access the licensed spectrum on an non-interfere basis in order to avoid interfering with PUs. Nevertheless, malicious cognitive users can cause severe. DoS attacks in primary networks through interference. The proliferation of wireless network technology has been remarkable in the last decade. The demand for Internet traffic through wireless infrastructures has increased substantially due to the widespread use of smart phones, the popularity of several online services (e.g. social networks), and the reduced subscription costs. An immediate effect of this increase is the escrowing of the ISM band. On the other hand, several portions of the licensed spectrum are under-utilized. Towards providing solutions to these shortcomings and meeting the ever increasing user demands, new technologies for future networks are investigated and proposed.

In energy detection method,detect the energy of the received signal. The received signal samples in the two-stage method are first passed through the energy detection stage. In this technique, energy of the desired transmitted signal is detected then this detected energy is compared with a threshold value. The threshold is a pre-defined value. If the detected energy is below than threshold value then it is licensed user is not present and the spectrum is free. Oppositely, if the detected energy is above the threshold value then it is assume that the spectrum is not free.

In this spectrum sensing method,determine probability of detection(Pd) and probability of false alarm(Pf).Pd is probability of correctly determining the presence of primary signals.Pf is probability of mistaking the presence of primary signals. probability of detection(Pd) and probability of false alarm(Pf) decribed as

$$Pd = Q[\text{qfuncinv}(\text{Pf}) - \text{snr}\sqrt{N}]/\sqrt{2snr+1}$$
$$Pf = (\varepsilon/\sigma X^2 - 1)\sqrt{N} \quad (7)$$

Where, ε is threshold of energy detection.snr is signal to noise ratio. Q() denotes Q-function. N represents number of samples.

Disadvantange of energy detection is the first problem is that it has poor performance under low SNR conditions. This is because the noise variance is not accurately known at the low SNR, and the noise uncertainty may render the energy detection useless. Another challenging issue is the inability to differentiate the interference from other secondary users sharing the same channel and the PU. The threshold used in energy selection depends on the noise variance, and small noise power estimation errors can result in significant performance loss.

wide sense stationary signal with no correlation among its samples. A signal is said to be cyclostationary if its autocorrelation function is periodic in time.

Cyclostationary feature detection needs high computation complexity, the best detection point is determined through simulation analysis on different detection points, and then we intend combination detection method using multiple detection points to obtain better performance. Output validate the effectiveness of the suggested method Cyclostationary feature detection can be able to have high detection probability under low SNR; actually, it requires high computation complexity. In reality, based on channel and a given location, the licensed users signal parameters are known and the SNR is changing gradually, so we assume that we can obtain the licensed users signal type and SNR before making detection. Using of the licensed users prior knowledge like properties of signal, we only makes detections in some specific frequencies and cycle frequencies, and multiple combine detection points to increase the performance further. And then given the Pd required by licensed users, the probability of false alarm (Pf) under different SNRs is implemented. Through the threshold adjustment,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

we decrease the PFA to make better use of spectrum hole when the SNR is high and increase the Pf to avoid interference to the licensed users when the SNR is low.

Cyclostationary feature detection exploits the periodicity in the received primary signal to identify the presence of Primary Users (PU). The periodicity is commonly embedded in sinusoidal carriers, pulse trains, spreading code, hopping sequences or cyclic prefixes of the primary signals. Due to the periodicity, these cyclostationary signals exhibit the features of periodic statistics and spectral correlation, which is not found in stationary noise and interference.

8. SIMULATION RESULTS

Receiver Operating Characteristics (ROC) is an important tool in analyzing performance of an energy detector. It is generally used in hypothesis testing problem. ROC curves provide graphical representation of the performance of binary classifier system. A ROC curve is generated by plotting the probability of detection (Pd) versus probability of false alarm (Pf)

Fig.2 shows the variation of probability of detection with SNR for different values of Pf. It can be observed that with increase in the Pf the detection performance increases. ROC curves are used to plots of the probability of detection vs. the probability of false alarm in energy detection. The probability of detection varies based on SNR, false alarm probability. When SNR increases, the detection probability detection method. The probability of detection varies based on SNR, false alarm probability. When SNR increases, the detection probability increases.

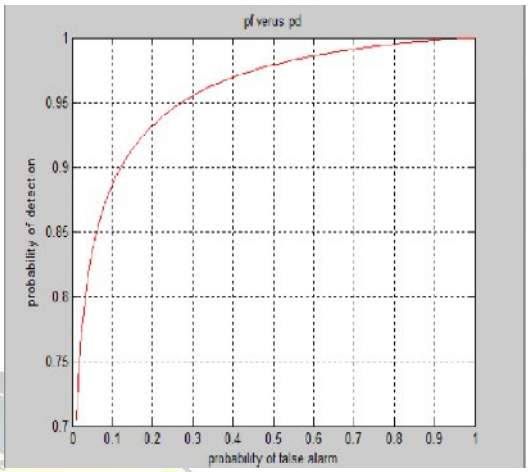

Fig.2 Pf versus Pd of energy detection

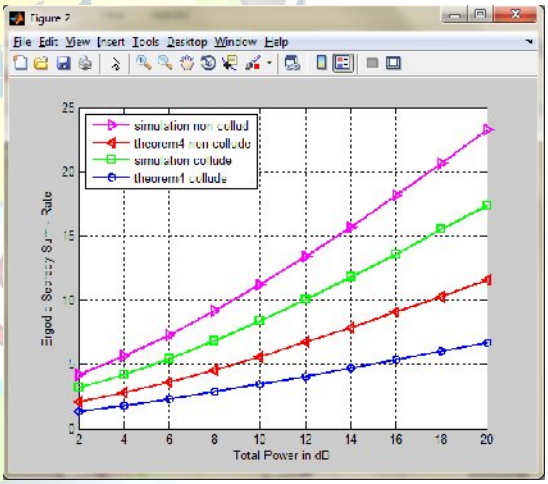

Fig .(3) CCE And Secrecy Rates Achievable With RCI Precoding

The comparison of secrecy sum rate for non colluding and colluding user, indicates the secrecy rate, and the optimal regularization parameter of the precoder, in different scenarios and under different system dimensions, network loads, SNRs, and densities. The eavesdropper compares the simulated probability of outage under non-colluding and colluding users.Total power is calculated in dB.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

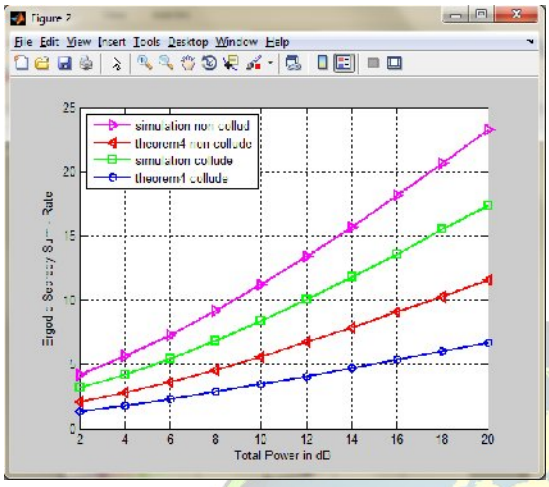

Fig .(4) CCE And Secrecy Rates Achievable With RCI Precoding

The broadcast channel with confidential messages and external eavesdroppers (BCCE), where a multi-antenna base station simultaneously communicates to multiple potentially malicious users, in the presence of randomly located external eavesdroppers. Using the proposed model, we study the secrecy rates achievable by regularized channel inversion (RCI) precoding by performing a large-system analysis that combines tools from stochastic geometry and random matrix theory The mean secrecy sum rate as well as the ergodic secrecy sum rate is calculated.Graph is plotted between total power and ergodic secrecy sum rate.

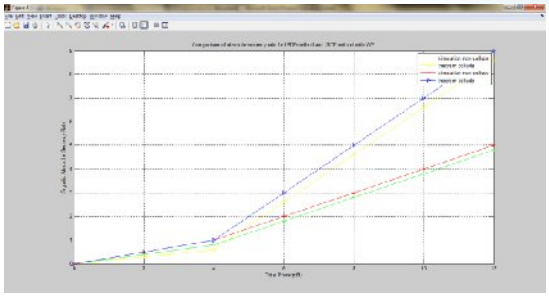

Fig.(5).Ergodic Absolute Secrecy Rate VS Total Power

As there is a secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and be used to achieve accurate identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is resent or not. The proposed approach is practically feasible in the sense that it can effectively combat PUEA with no change in hardware or system structure except of a plug-in AES chip. Potentiallyit can be applied directly to today's HDTV systems for more robustsystems.This provides security to the system. The ergodic absolute secrecy rate vs total power is calculated. The channels are assumed to be identically and independently distributed block Rayleigh fading. The number of secondary users is N = 4 and the number of samples during a detection interval is M = 3

7 CONCLUSION

Analyzed the detection of malicious user using coopon technique the spectrum sensing results are gathered in terms of probability of false alarm (Pf), probability of PU detection alarm (Pd), for a specific SNR. SPARS technique require prior information of PU and implementation Is complex, while energy detector does not require PU information, easy to implement, and speed of operation. ROC curves are used to plots of the probability of detection vs. the probability of false alarm in detection. The probability of detection varies based on SNR, false alarm probability. When SNR increases, the detection probability increases. It indicates that with the increasing of the SNR, the more users which are occupied we can detect. SPARS detection had the advantage that no prior information about the PU was required. But did not perform well at low SNR, there was a minimum SNR required. Throughput is reduced and power is also consumed.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. II, Special Issue XXIII, March 2015 in association with
FRANCIS XAVIER ENGINEERING COLLEGE, TIRUNELVELI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
INTERNATIONAL CONFERENCE ON RECENT ADVANCES IN COMMUNICATION SYSTEMS AND TECHNOLOGIES
(ICRACST'15)
25TH MARCH 2015

REFERENCES

[1] Q. Zhao and B. Sadler, "A survey of dynamic spectrum access," IEEE Signal Process. Mag., vol. 24, no. 3, pp. 79–89, May 2007.
[2] FCC, "Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band," Federal Commun. Commission, Columbia, SC, USA, Tech. Rep. ET Docket No. 04-186 and 02-380, Sep. 2010.
[3] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio etworks," in Proc. IEEE Workshop Netw. Technol. Softw.Defined Radio Netw., Sep. 2006, pp. 110–119.
[4] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in Proc. 3rd IEEE Symp. New Frontiers Dyn. Spectrum Access Netw., Oct. 2008, pp. 1–6.
[5] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE J. Sel. Areas Commun., vol. 26, no. 1, pp. 25–37, Jan. 2008.
[6] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in Proc. IEEE WCNC, Mar. 2011,pp. 599–604.
[7] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," IEEE J. Sel. Areas Commun., vol. 30, no. 10, pp. 1850–1860, Nov. 2012.

[8] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in Proc. IEEE Int. Conf. Commun., Jun. 2009, pp. 1–5.
[9] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," SIGMOBILE Mobile Comput. Commun. Rev., vol. 13, no. 2, pp. 74–85, 2009.
[10] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2135–2141,Jul. 2011.
[11] C. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in Proc. 4th IEEE CCNC, Jan. 2007, pp. 1037–1041.
[12] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in Proc. IEEE ICASSP, May 2013, pp. 2935–2939.
[13] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," IEEE Commun. Surv. Tuts., vol. 15, no. 1, pp. 428–445, Mar. 2013.
[14] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in Proc. IEEE Symp. SP, May 2010, pp. 286–301.
[15] A. Hodjat, D. D. Hwang, B. Lai, K. Tiri, and I. Verbauwhede, "A 3.84 Gbits/s AES crypto coprocessor with modes of operation in a 0.18-µm CMOS technology," in Proc. 15th ACM Great Lakes Symp. VLSI, New York, NY, USA, 2005, pp. 60–63.

.