We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Chapter 5

Spectrum Sensing and Mitigation of Primary User Emulation Attack in Cognitive Radio

Avila Jayapalan and Thenmozhi Karuppasamy

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.80328

Abstract

The overwhelming growth of wireless communication has led to spectrum shortage issues. In recent days, cognitive radio (CR) has risen as a complete solution for the issue. It is an artificial intelligence-based radio which is capable of finding the free spectrum and utilises it by adapting itself to the environment. Hence, searching of the free spectrum becomes the key task of the cognitive radio termed as spectrum sensing. Some malicious users disrupt the decision-making ability of the cognitive radio. Proper selection of the spectrum scheme and decision-making capability of the cognitive reduces the chance of colliding with the primary user. This chapter discusses the suitable spectrum sensing scheme for low noise environment and a trilayered solution to mitigate the primary user emulation attack (PUEA) in the physical layer of the cognitive radio. The tag is generated in three ways. Sequences were generated using DNA and chaotic algorithm. These sequences are then used as the initial seed value for the generation of gold codes. The output of the generator is considered as the authentication tag. This tag is used to identify the malicious user, thereby PUEA is mitigated. Threat-free environment enables the cognitive radio to come up with a precise decision about the spectrum holes.

Keywords: cognitive radio, spectrum sensing, PUEA, collaborator node, authentication tag

1. Overview

The introduction of wireless technique has led to the achievement of mobility and global connectivity through its advantages in flexibility, cost and convenience. Due to its rapid growth, there arises a demand for the spectrum. But analysis shows that there are portions

IntechOpen

© 2018 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

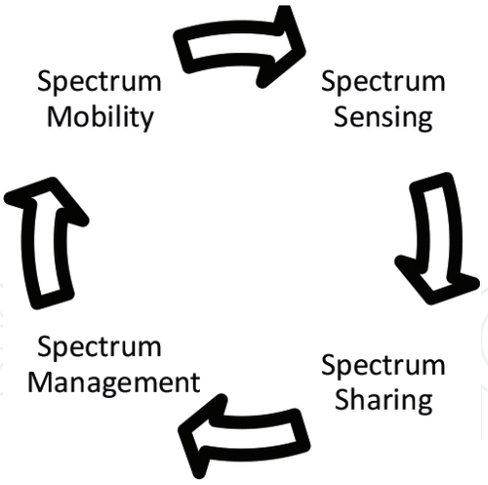


Figure 1. Cognitive cycle.

of the spectrum which are not effectively used and those portions of the spectrum could be exploited, whenever in need. For dynamic spectrum access, cognitive radio has risen as a favourable solution [1, 2]. Cognitive radio searches out for the free spectrum termed as 'spectrum holes'. The process of finding the spectrum holes is termed as spectrum sensing. Apart from spectrum sensing some of the other functions of cognitive radio are spectrum sharing, spectrum management and spectrum mobility. These four functions are put together termed as cognition cycle [3–6] and it is shown in **Figure 1**.

1.1. Spectrum sensing

The users in the wireless environment can be classified into three main groups, namely primary users, secondary users and selfish, malicious users. Primary users are those who gain ownership of the spectrum [7]. Secondary users desire to gain access in the absence of primary users [8]. Malicious users desire to own access of the spectrum by cheating the secondary users [9].

In the cognitive environment, the procedure of searching the spectrum holes by the secondary users is known as spectrum sensing. The cognitive radio not only looks for the free spectrum, but also checks for the arrival of primary users. On the homecoming of the primary users, cognitive users or the secondary users should quit the existing spectrum immediately and search for some other new spectrum hole.

1.2. Types

Various types of spectrum sensing schemes are available and they are shown in **Figure 2**. Some of them are energy detection method [10], cyclostationary method [11], matched filter method [12], etc. Feature detection and matched filter methods require prior knowledge about the licenced user for detection and they are time-consuming.

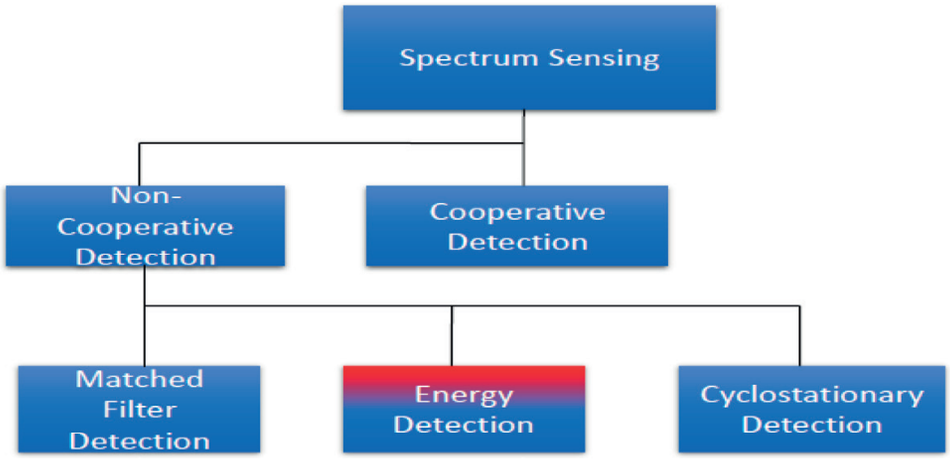


Figure 2. Types of spectrum sensing.

Energy detection method does not require any former knowledge about the primary user and it is simpler and quicker when compared to the previously mentioned methods. Energy detector can be classified into two types:

- Frequency domain-based energy detector
- Time domain-based energy detector

Energy detection method is not suited for places where the SNR is very low. Hence, it is a trade-off in choice of the proper spectrum sensing scheme.

1.2.1. Time domain

Figure 3 shows time domain-based energy detector. The energy of the signal is calculated and compared with the threshold.

The output of the detector is

$$Z = \sum_{n=0}^{N} y(n)^2 \tag{1}$$

where n = 1, 2, 3, …, N. N = number of samples

$$\begin{aligned} &\text{If } Z \prec \lambda \text{ primary user absent} \\ &\text{If } Z \geq \lambda \text{ Primary user present} \end{aligned} \tag{2}$$

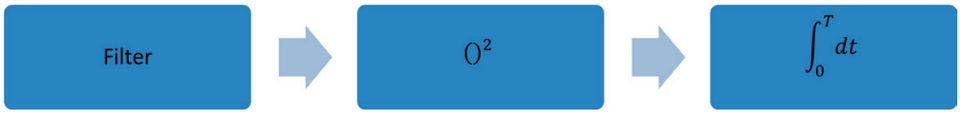


Figure 3. Time domain-based energy detector.

The decision hypothesis is as follows:

$$\begin{aligned} y(n) &= s\,H_0 = \text{only the presence of noise} \\ y(n) &= x(n) + s\,H_1 = \text{presence of both primary user signal and noise} \end{aligned} \tag{3}$$

where n is the noise, y(n) is the received signal and x(n) is the transmitted signal.

1.2.2. Threshold

Keeping the probability of false alarm fixed the threshold value is set according to the equation:

$$\lambda_f = \sigma_n^2\left(1 + \frac{Q^{-1}\left(P_f\right)}{\sqrt{\frac{N}{2}}}\right) \tag{4}$$

$$\lambda_d = \sigma_n^2(1 + SNR)\left(1 + \frac{Q^{-1}\left(P_f\right)}{\sqrt{\frac{N}{2}}}\right) \tag{5}$$

where N = number of samples and Q^{-1} = complementary error function.

- Cooperative spectrum sensing: Group of cognitive radios, shares the spectrum sensing information. To achieve spectrum sharing and to overcome the multipath propagation effects and hidden node problems cooperative spectrum sensing scheme is utilised. The cognitive users employ less sensitive detectors, thereby reducing the cost of hardware and complexity. It is divided into two types namely
- Centralised spectrum sensing
- Distributed spectrum sensing

Centralised spectrum sensing: In this method, the central unit collects the sensing information from the cognitive users located at various places of the radio environment, analyses the received information and transmits the final decision about the existence or nonexistence of the PU to the cognitive users. Two rules are followed in deciding PU. One is AND rule and the other is OR rule.

- AND rule: All the SU's declare that the PU is present
- OR rule: If anyone SU status is high then the PU is considered present

Distributed spectrum sensing: Each node senses the PU, and a decision is made based on the earlier scenarios. Complexity is greatly reduced as there is no need of fusion center (FC). But at the same time, it increases the burden to the CR.

1.3. PUEA

On receiving the primary users signal, the cognitive radio compares it with a predefined threshold. If the incoming signal exceeds the primary threshold, user is assumed to be present

else absent. In the absence of the primary user, the malicious user sent a fake signal almost matching with the primary user signal to the cognitive radio. The cognitive radio on receiving the fake signal compares it with the threshold. The fake signal exceeds the threshold, and hence the primary user makes a wrong interpretation that the primary user is present and does not make any attempt access the spectrum. The malicious user now utilises that free spectrum. This attack is known as primary user emulation attack (PUEA) [13], which is considered as the severe attack in the physical layer of the cognitive radio.

Various researchers have analysed the importance and impact of PUEA in cognitive radio environment, and they have come out with different solutions to overrule PUEA. Few of them are as follows. A review about primary user emulation attack has been made in [14–17]. A study about PUEA has been made in [18, 19]. To ensure end-to-end security for portable devices over cognitive radio network, two authentication protocols have been proposed in [20]. Four dimensions continuous Markov chain model to combat PUEA has been proposed in [21]. PU, secondary user, selfish misbehaviour secondary user and misbehaviour secondary user are considered to combat PUEA. In [22], a trustworthy node is taken as reference and the position of PU and emulator was found to detect PUEA. Eigenvalue-based PUEA mitigating method has been discussed in [23]. Time-synched link signature scheme to mitigate PUEA has been proposed in [24]. In [25], temporal link signature scheme to establish link between transmitter and receiver has been proposed and with the aid of signature PUEA is mitigated. Any change in the transmitter location or emulator claiming as transmitter is identified.

Integrated cryptographic and link signature-based method to mitigate PUEA has been proposed in [26]. Suspicious level and trust level calculations are carried out to mitigate PUEA in cooperative spectrum sensing environment in [27]. Mitigating PUEA and worm hold attack through sequence number generation by the helper nodes has been proposed in [28]. Multiple helper nodes-based authentication method to combat PUEA in the TV band has been discussed in [29]. Optimum voting rule and sample-based scheme in cooperative spectrum sensing to mitigate PUEA has been proposed in [30]. Advanced encryption standard (AES)-based authentication method with 256-bit key size has been suggested in [31] to overcome PUEA. Digital constellation-based authentication scheme to mitigate PUEA has been proposed in [32]. Quadrature phase shift keying was considered. Based on the tag value, the phase of QPSK modulation is rotated. Helper node-based special authentication algorithm has been suggested in [33] to mitigate PUEA in mobile networks. Location, privacy-preserving framework, has been proposed in [34]. The framework consists of two parts namely privacy-preserving sensing report aggregation protocol and distributed dummy report injection protocol.

Authentication scheme based on the transmitter called localisation based defence (LocDef) to mitigate PUEA has been discussed in [35]. In [36], neural network and database management-based scheme to mitigate PUE threat have been proposed. COOPON (called cooperative neighbouring cognitive radio nodes) technique to mitigate the selfish user attack in cooperative spectrum sensing environment has been proposed in [37, 38]. Matched filter-based spectrum sensing together with the cryptographic signature-based method has been suggested in [39]. Extensible authentication protocol and carousel rotating protocol-based authentication scheme have been proposed in [40]. Location-based authentication protocol for IEEE 802.22 wireless regional area network (WRAN) has been implemented in [41]. Double key-based

encryption scheme has been proposed in [42] to overcome the attacks. Two non-parametric algorithms namely cumulative sum and data clustering-based method have been discussed in [43] to mitigate PUEA in cognitive wireless sensor networks. A study about various types of attacks and their countermeasures in wireless sensor networks has been made in [44].

In [45], Fenton's approximation and Wald's sequential probability ratio test (WSPRT)-based scheme has been proposed to mitigate PUEA. Probability of missing was the main parameter considered to set the threshold value. Modified combinational identification algorithm has been discussed in [46] to mitigate the attacks in cooperative sensing. Cluster-based technique to overcome the rogue signal intrusion in cooperative spectrum sensing has been discussed in [47]. In [48], a novel method has been suggested to mitigate the threat in cooperative spectrum sensing. It includes two phases namely identifying phase and sensing phase. In the identifying phase, reliable SUs are found and the sensing results are collected in the second phase. In [49], a trustworthy cognitive radio network has been suggested to defend against malicious users. It is based on the trust value generated and distributed among the nodes. In [50], two algorithms are derived namely encryption algorithm and displacement algorithm from overcoming PUEA. Adaptive orthogonal matching pursuit algorithm (AOMP) has been proposed in [51] to mitigate PUEA. Energy detection, cylostationary and neural network-based scheme have been reported in [52] to cancel PUEA. AND/OR rule-based sensing method has been suggested in [53] to mitigate in PUEA in cooperative spectrum sensing. Improvements in the probability of error is obtained by the OR rule than the AND rule. Nash equilibrium-based differential game method has been suggested in [54] to mitigate PUEA. A new cooperative spectrum sensing in the presence of PUEA has been offered in [55]. Based on the channel information among PU, SU and attackers, weights are derived for optimal combining in the fusion center. A hybrid defence scheme against PUEA with motional secondary users was discussed in [56]. A new spectrum decision protocol to mitigate PUEA in dynamic access networks has been discussed in [57].

1.3.1. Other attacks

Some of the other attacks in the physical layer are denial of service (DOS) attack and replay attack. Any attack in the path between cognitive radio and primary user is known as DOS attack. The malicious user eavesdrop some primary user information and transmit to the cognitive radio at an irrelevant time. This confuses the cognitive radio in deciding the existence of the primary user. This attack is termed as replay attack.

A study about denial of service attack has been made in [58, 59]. Radio frequency fingerprint-based technique has been suggested in [60] to combat DOS attack. Dynamic and smart spectrum sensing algorithm (DS3) has been generated in [61] to minimise the DOS attack. Around 90% of improvement in spectrum utilisation was obtained with the inclusion of DS3 algorithm. Channel eviction triggering scheme in the presence of Rayleigh fading channel has been proposed in [62] to mitigate DOS attack in cooperative spectrum sensing environment. This mechanism is aimed at reducing the misreports and increasing the trustworthy score. A study about replay attack in cognitive radio has been made in [18, 63–65]. A study about the malicious activities in ZigBee network has been made in [66].

http://dx.doi.org/10.5772/intechopen.80328

1.4. Performance metrics

Performance metrics are used to analyse the system's behaviour and performance. They are used to confirm and validate the specified system performance requirements and to identify the performance issues in a given system.

The important performance metrics for cognitive radio are

- Probability of detection (P_d): Probability of detection is the time during which the primary user is detected.
- Probability of false alarm (P_f): the erroneous detection of the primary user
- Probability of missed detection: failing to detect the primary user. Probability of false alarm: A study about the performance metric has been made in [67–69].
- Receiver operating characteristics (ROC): It is the graph plotted between sensitivity and false positive rate. Here, it is plotted between probability of missed detection and probability of false alarm.

This chapter gives a brief idea about the working of frequency domain-based energy detection spectrum sensing scheme and provides a solution to mitigate PUEA through the authentication tag generated by the collaborator cognitive radio. The sample graphs are plotted between probability of detection and signal to noise ratio, P_d versus P_f.

2. Method to mitigate PUEA

2.1. Collaborator node

To ensure proper spectrum sensing, cognitive radio does not carry out spectrum sensing of its own. Instead, it depends on the third party called collaborator node. It is assumed that the collaborator node is very close to the primary user. The purpose of choosing collaborator node is due to Federal Communication Commissions (FCC) decision 'no modifications must be done to the primary user signal'.

The sample graph is shown in **Figure 4**. The collaborator node senses the availability of the primary user and in the absence of the primary user conveys the message to the cognitive

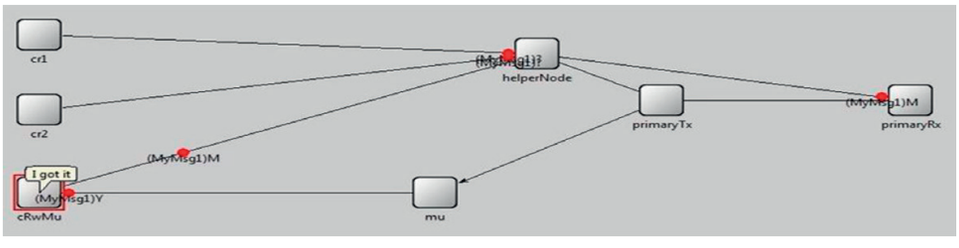


Figure 4. PUEA mitigation.

radio along with the authentication tag. To elude interference with the primary user, the collaborator node communicates with the cognitive radio only in the absence of the primary user. The key to decode the authentication tag is already known to the cognitive radio. The cognitive radio accepts the information only with authentication tag and discards other information. By this way, PUEA is mitigated.

2.2. Spectrum sensing

The collaborator node senses the availability of the primary user with the aid of energy detection method. The block diagram of frequency domain-based energy detection method is shown in **Figure 5**. The incoming signal is filtered and passed to fast Fourier transform block. The output of FFT block is fed to windowing function block. This is done so to reduce the irregularities and to reduce the side lobes. Various windows like Hanning window, Hamming window, Blackman window and Kaiser window could be utilised. Every window has its own advantage and disadvantage. By adjusting beta parameter of Kaiser window, side lobes can be reduced when compared to other windows; but at the same time, the width of main lobe is wider. By adjusting the size of the windows, better output could be obtained. Hence, proper choice of window becomes necessary. The output of windowing block is fed to magnitude square block. The average energy of the signal is then compared with the decision threshold [70–73].

If the incoming signal falls below the threshold, it is null hypothesis (H_0). Only noise is present in the channel and the primary user signal is absent. The spectrum is vacant and could be utilised by the cognitive radio. On the other hand, if the incoming signal exceeds the threshold the decision made is 'primary user present'.

Table 1 summarises the simulation parameters of the graph plotted below. **Figure 6** shows the sample result plotted between P_d versus SNR. SNR is considered as x-axis and P_d as y-axis. For the probability of detection of 0.9, the SNR is −14 dB. The negative scale indicates that the cognitive radio can pick up the primary user signal in a week SNR environment.

Figure 7 shows the output of energy detector for different values of SNR with AWGN noise present in the channel. From the figure, it is clear that as the SNR increases error reduces. Probability of missed detection is lesser for SNR of −5 dB when compared to −20 dB. Lesser the SNR, more is the noise which makes it difficult to detect the presence of the primary user.

2.3. Authentication tag generation by the collaborator node

Once the sensing process is complete, the second step is to generate the authentication tag. The authentication tag is generated in three ways. First method is logic map algorithm-based sequence generation. Second method is by means of DNA-based cryptographic algorithm

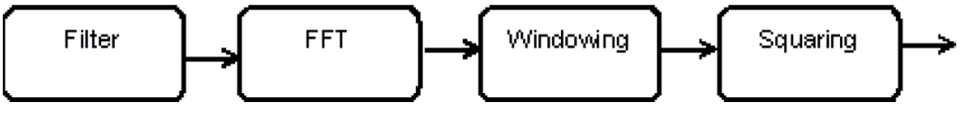


Figure 5. Energy detection method.

Number of samples	300
Probability of false alarm	0.1
Window function	Hanning
Channel	AWGN
FFT size	128

Table 1. Simulation parameters.

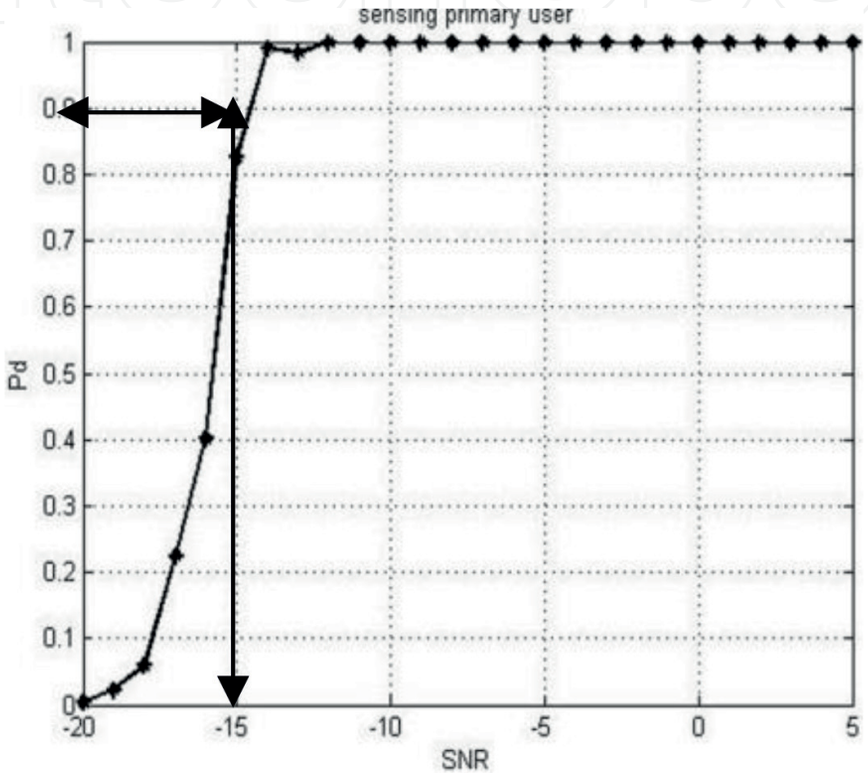


Figure 6. Spectrum sensing.

the sequence is generated. Third method is based on gold code. Utilising gold code generator gold codes are generated. In this, the initial seed value for the gold code is the sequences obtained from the first two methods. The final output from the gold code is treated as the authentication tag to mitigate PUEA.

2.3.1. Chaotic sequence

Chaotic sequences help to retrieve the data from intruder in many ways:

a. It changes the transmitted signal into unwanted noise, and therefore it will provide great confusion to the intruder.

b. Code sequences will not repeat for each and every bit of information so it causes the malicious user to take long time to find the sequences.

c. Developing chaotic sequence is simple for both transmitter and receiver who knows the data and parameters used in that transmission, the exact regeneration of data is difficult for a receiver those who wrongly estimate the value. A slight deviation in estimation leads to increasing the error. This is because of sensitivity of chaotic system on their initial condition.

2.3.1.1. Logistic chaotic sequence

1-D logistic chaotic sequence is widely used in communication because of their fast computation process, and simple nature.

Logistic chaotic sequence can be generated by using an expression

$$x(j+1) = r \times x(j) \times (1 - x(j)) \tag{6}$$

where r is called as control parameter and constant, it ranges from $3.57 < r < 4$, $x(1) = 0.99$.

One of the main properties of this sequence is extreme sensitivity to initial condition and good correlation property.

Figure 8 shows the signal to noise ratio versus primary user detection graph plotted with and without authentication tag. The overlapping of both the graphs shows that there is no significant change in the performance of the collaborator system when an authentication tag is inserted. The authentication tag and the spectrum-free information are transmitted to the cognitive radio. The probability of false alarm is fixed as 0.1 and the number of samples chosen is 300. Additive white Gaussian noise (AWGN) is considered as the channel noise.

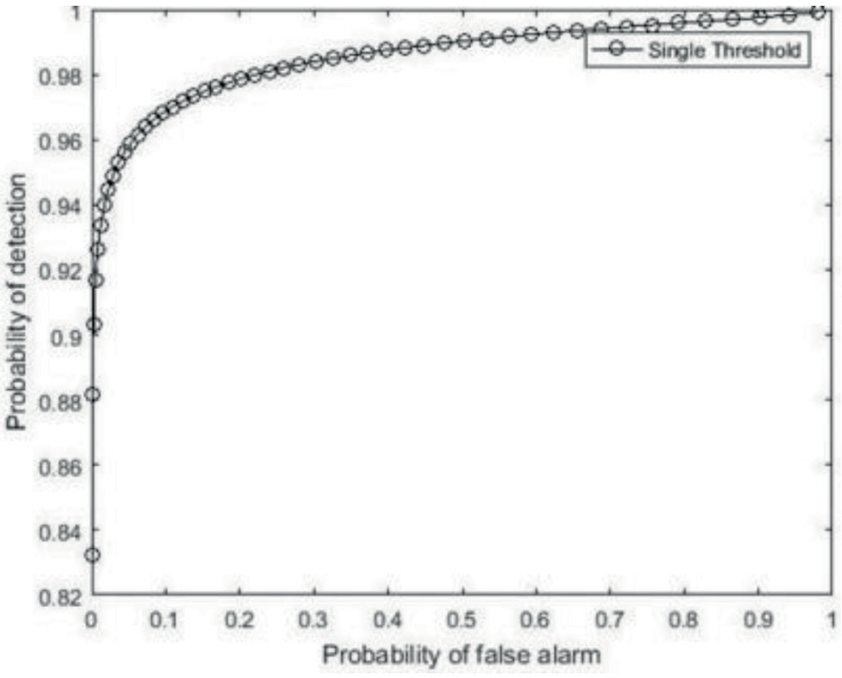


Figure 7. Comparison between various SNR.

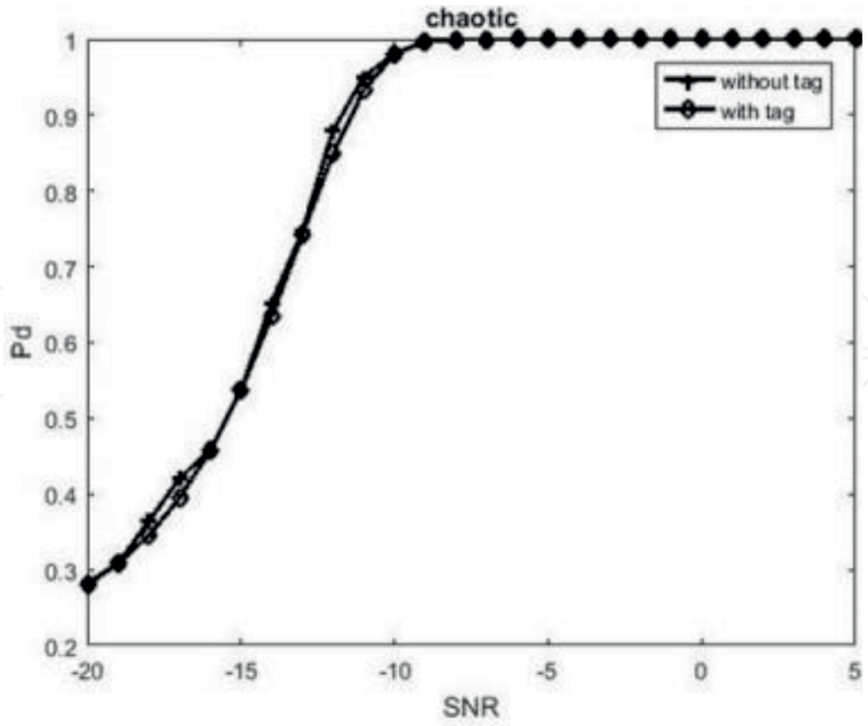


Figure 8. Chaotic-based tag generation.

2.3.2. DNA

DNA algorithm has been utilised in this work to generate the authentication tag because the storage and processing of data is very secure. One single DNA can be split into four basic units. They are Adenine (A), Thymine (T), Cytosine (C) and Guanine (G). So, it is also known as quaternary encoding. Binary values are assigned to these units for encoding purpose as follows:

A—00, T—01, C—10 and G—11.

Algorithm

Step 1: Transform message bits into binary

Step 2: Assign A, T, G and C to binary(a)

Step 3: Get key value from server(b)

Step 4: Take one's complement to step 2 and 3

Step 5: Do XOR operation between output from step 4(a′ and b′)

Step 6: Transform bits from step 5 into DNA form

Step 7: Transform DNA form into ASCII values

Step 8: Transform into binary form(encrypted)

Figure 9 shows the signal to noise ratio versus probability of detection graph plotted with and without authentication tag. The overlapping of both the graphs shows that there is no notable

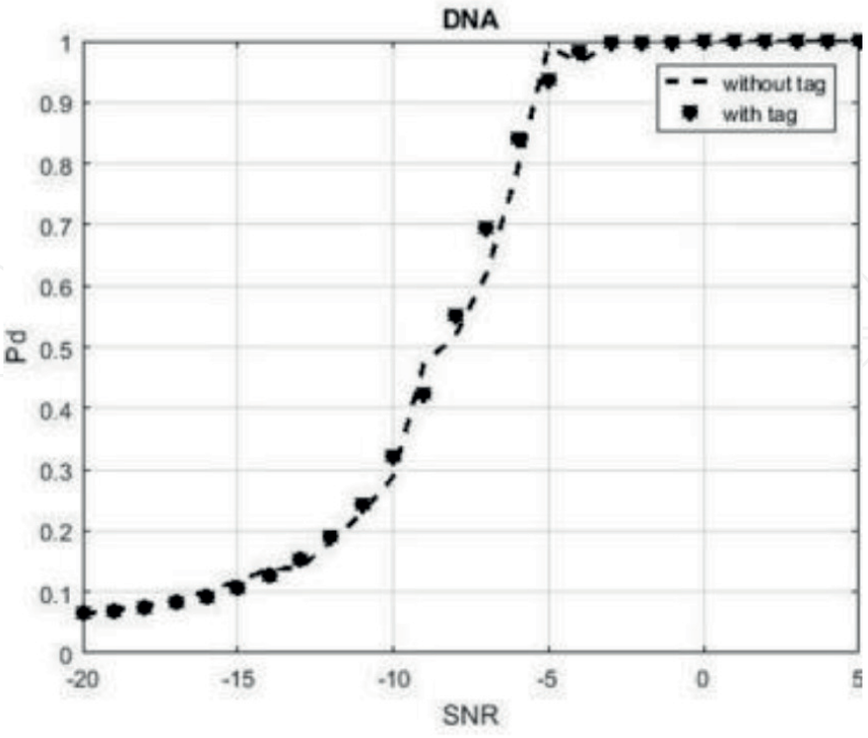


Figure 9. DNA algorithm-based tag generation.

difference in the performance of the collaborator system when an authentication tag is added along with the primary user availability information.

2.3.3. Gold code

Pseudonoise (PN) is a signal similar to noise but generated with a definite pattern. In cryptography, PN sequences are widely to ensure data protection from intruders. The PN sequences are added with the message signal so that it appears as noise to the malicious users. Various types of PN sequences are available. Their auto- and cross-correlation properties decide the choice of PN sequences. Some PN sequences have good autocorrelation property but not cross-correlation property. Some have good cross-correlation property but not autocorrelation property. Gold code is chosen because of its good auto and cross-correlation property. Gold codes are obtained by mod-2 addition of shifted pairs of m-sequences with length m. The autocorrelation and cross-correlation function of gold code, $2^t - 1$, is

Autocorrelation function:

$$\varphi_{GC}(h)$$
$$\text{Where } \varphi_{GC}(h) = \begin{cases} \pm 2^t - 1, h = 0 \\ \pm 1, h \neq 0 \end{cases} \quad (7)$$

Cross-correlation function:

$$\psi_{GC}(h)$$
$$\text{Where } \psi_{GC}(h) = (2^t - 1, h = \lambda \quad (8)$$
$$\pm 1, h \neq \lambda$$

2.3.3.1. Trilayered authentication

The proposed work is to integrate all the three algorithms and to generate a trilayered authentication tag to mitigate PUEA. Both the LFSRs required a seed value for their functioning. Hence, the initial seed value of one LFSR is the sequence generated utilising DNA algorithm and for the second LFSR it is a chaotic sequence. The outputs from the LFSRs are XORed, and the resulting gold code sequence is considered an authentication tag. It is as shown in **Figure 10**.

Figure 11 shows the sample signal to noise ratio versus probability of detection graph plotted with and without authentication tag. From the figure, it can be depicted that there is no drastic change in the performance of the collaborator system when an authentication tag is add along with the primary user availability information.

Figure 11b shows the graph plotted by increasing the size of the window function. Here, Hamming window of size 10 has been utilised.

Figure 11c shows the plot of signal to noise ratio versus probability of detection graph plotted with and without authentication tag. Here, the FFT size of the energy detector has been raised from 64 to 128.

Figure 11d shows the graph plotted with the probability of false alarm fixed as 0.01.

2.3.3.2. Hardware implementation

Universal software-defined radio peripheral (USRP) is a universally accepted test bed for cognitive radio. The USRP software-defined radio device is a tuneable transceiver. It is used as a prototype for wireless communication systems. It offers frequency ranges up to 6 GHz with up to 56 MHz of instantaneous bandwidth. It allows advanced wireless applications to be created with LabVIEW, enabling rapid prototyping.

The prototype of energy detection-based spectrum sensing scheme is developed using LabVIEW tool. LabVIEW is a modelling, simulation and real-time implementation tool which

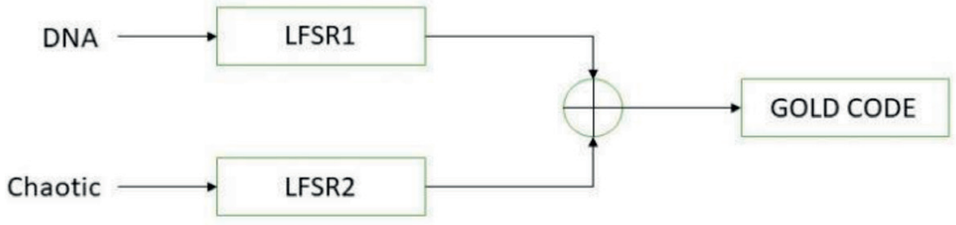


Figure 10. Trilayered authentication.

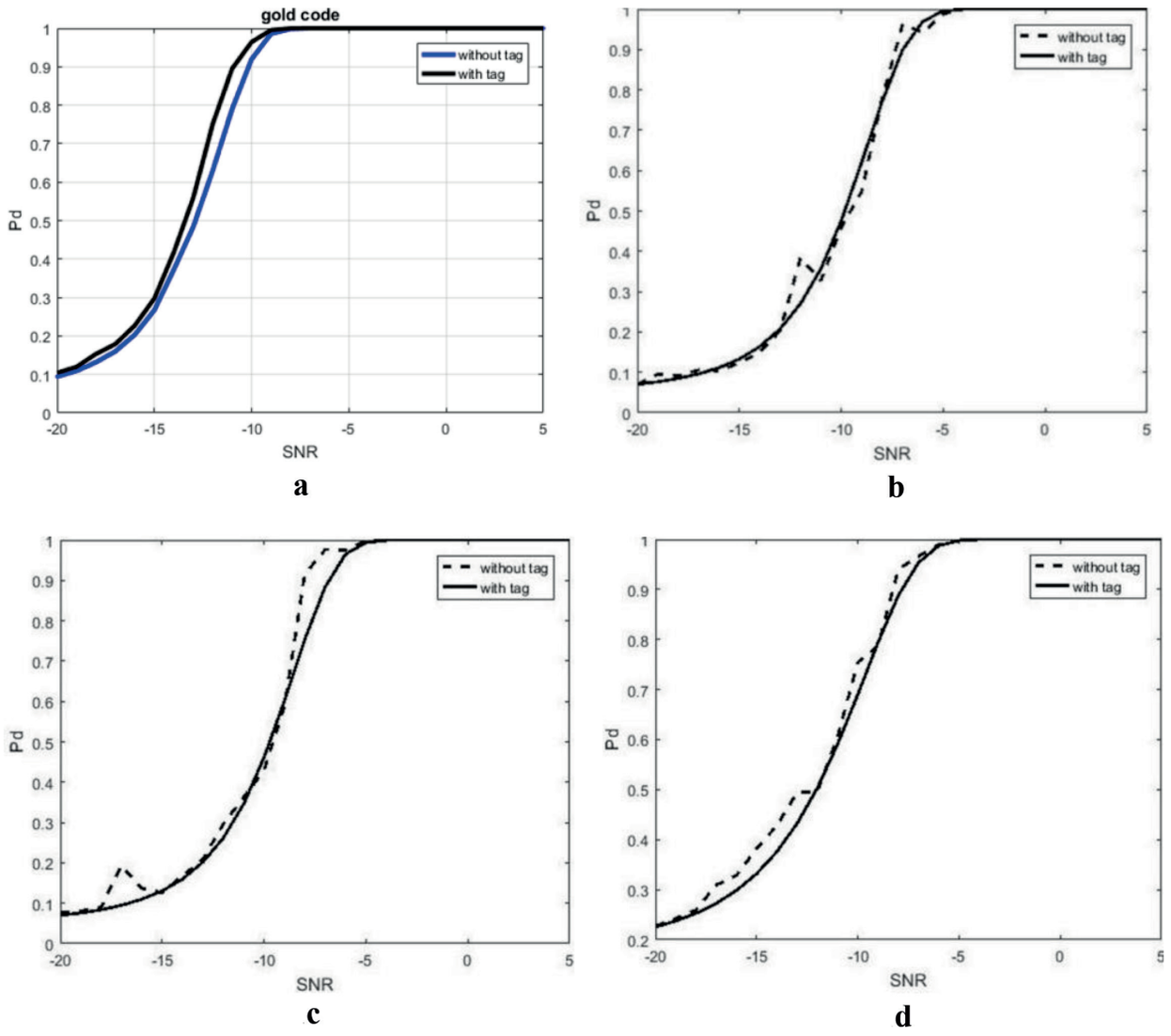


Figure 11. (a)–(d) Trilayer-based tag generation.

is being used around the world for implementation development through software. It uses runtime engine to simulate the designs. Front panel and block panel support the graphical user interface (GUI) structure of LabVIEW. Front panel comprises of controls and indicators, whereas block panel has functions, structures, Sub-Vis and terminals to execute the required design.

The transmitter and the receiver blocks are developed using LabVIEW software. **Figure 12** shows the block diagram of energy detector. Once the blocks are developed using LabVIEW software then the physical connections are made. Ethernet cable is used to connect USRP with the computer in which the blocks are developed.

Then, the signal is transmitted using USRP. **Figure 13** shows the USRP front panel.

Figure 14 shows the experimental setup using USPR. Out of two USRPs, one USRP is treated as transmitter and the other USRP is treated as receiver. Additive white Gaussian noise (AWGN) is considered as the noise in the channel.

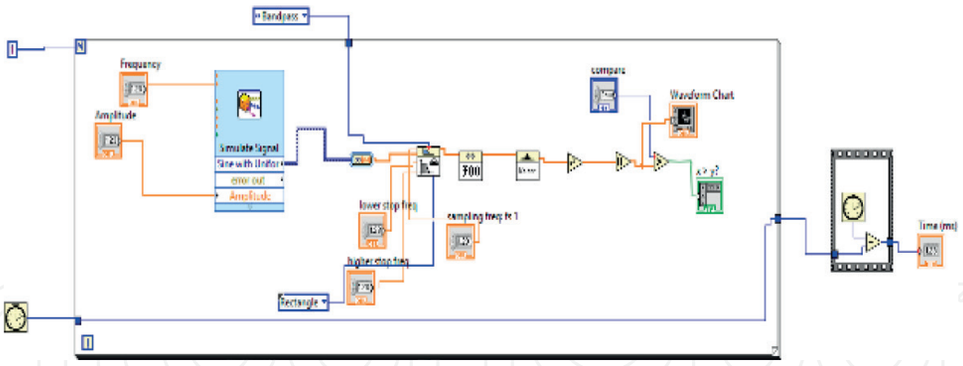


Figure 12. LabVIEW-based energy detector.



Figure 13. Front panel of USRP.



Figure 14. USRP experimental setup.

Table 2 shows the specification of USRP. For transmission, the IP address is 192.168.10.1 and for reception the IP address is set as 192.168.10.2. The USRPs are connected to the computer via Ethernet cable. The distance between the two USRPs is set as 100 cm.

Figure 15a shows the transmission of primary user signal at the transiting end and **Figure 15b** shows the detection of primary user signal at the receiving end. The received signal is now compared with the threshold value. The incoming signal exceeds the threshold value. The presence of primary user is detected and plotted. For an SNR of −5 dB, the probability of detection is 0.9.

Frequency range	50 MHz–2.2 GHz
Gain range	0–31 dB
Frequency accuracy	2.5 ppm
DAC	2 channels, 16 bit
Noise figure	5–7 dB
Maximum I/Q sampling rate	16-bit sample width at 20 MHz, 8-bit sample width at 40 MHz

Table 2. USRP specifications.

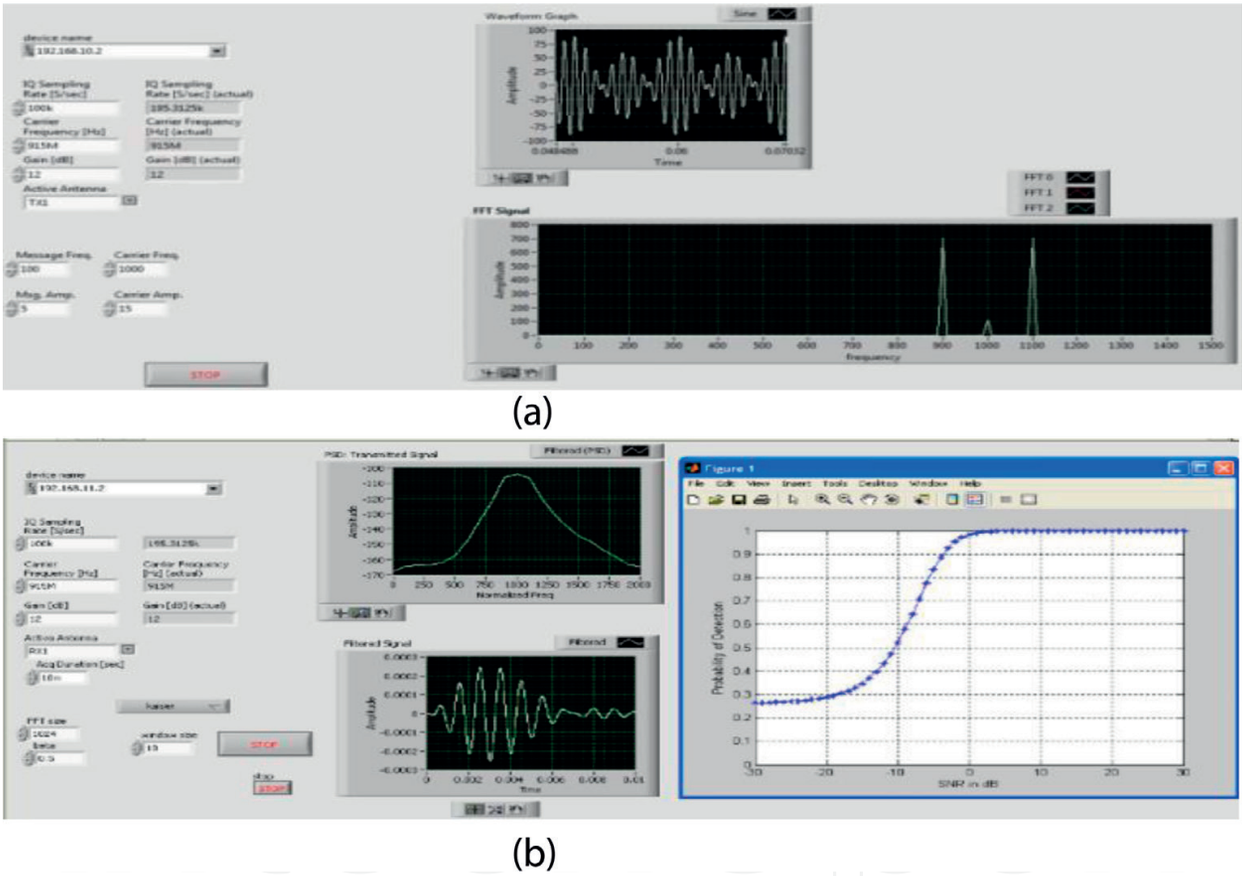


Figure 15. (a) Transmission using USRP. (b) Reception using USRP.

3. Conclusion

To avoid wastage of bandwidth and to achieve dynamic spectrum access cognitive radio is the best solution. To achieve dynamic spectrum access, the most important function of cognitive radio is spectrum sensing.

In this chapter,

- Energy detection-based spectrum sensing scheme has been discussed to detect the existence of the primary user by the collaborator node. This method has been chosen because of its simple nature.
- To combat PUEA, a collaborator node-based approach has been suggested. The cognitive radio requests the collaborator node to sense the free spectrum. The collaborator node senses the availability of the primary user.
- Once the availability of the free spectrum is confirmed, the message has been conveyed to the cognitive radio in a secure manner. Hence, a trilayered method has been suggested to generate the authentication tag. The message along with the tag is accepted by the CR and others are rejected. By this way, the PUEA attack has been overruled. Threat-free environment makes the cognitive radio to arrive at a proper conclusion about the presence of spectrum holes and utilise it.

Acknowledgements

The Authors would like to express their sincere thanks to SASTRA Deemed University, for the grant received under R&M fund (R&M/0027/SEEE – 010/2012–13) to carry out this book chapter.

Author details

Avila Jayapalan* and Thenmozhi Karuppasamy

*Address all correspondence to: avila@ece.sastra.edu

SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

References

[1] Mitola J, Maguire GQ. Cognitive radio: Making software radios more personal. IEEE Personal Communications. 1999;**64**:13-18

[2] Haykin S. Cognitive radio: Brain empowered wireless communications. IEEE Journal on Selected Areas in Communications. 2005;**232**:201-220

[3] Igbinosa IE, Oyerinde OO, Srivastava VM, Mneney S. Spectrum sensing methodologies for cognitive radio systems: A review. International Journal of Advanced Computer Science and Applications. 2015;**6**(12):13-22

[4] Akyildiz IF, Lee WY, Vuran MC, Mohanty S. A survey on spectrum management in cognitive radio networks. IEEE Communications Magazine. 2008;**46**(4):40-48

[5] Kaur M, Kaur A. Cognitive radio spectrum sharing techniques: A review. International Journal of Computer Science and Information Technologies. 2015;**6**(3):3089-3091

[6] Asokan A, Ayyappadas R. Survey on cognitive radio and cognitive radio sensor networks. In: International Conference on Electronics and Communication Systems; 2014. pp. 1-7

[7] Furtado A, Irio L, Oliveira R, Bernardo L, Dinis R. Spectrum sensing performance in cognitive radio networks with multiple primary users. IEEE Transactions on Vehicular Technology. 2015;**PP**(99):1-11

[8] Jia J, Zhang Q, Shen XS. HC-MAC: A hardware-constrained cognitive MAC for efficient spectrum management. IEEE Journal on Selected Areas in Communications. 2008; **26**(1):106-117

[9] Sabuj SR, Hamamura M, Kuwamura S. Detection of intelligent malicious user in cognitive radio network by using Friend or Foe (FoF) detection technique. In: International Telecommunication Networks and Conference; 2015. pp. 155-160

[10] Muchandi N, Khanai R. Cognitive radio spectrum sensing: A survey. In: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT); 2016. pp. 3233-3237

[11] Anyim IG, Chiverton J, Filip M, Tawfik A. The optimization of wideband cyclostationary feature detector with receiver constraints. In: IET 3rd International Conference on Intelligent Signal Processing (ISP 2017); 2017. pp. 1-6

[12] Kakalou I, Papadopoulou D, Xifilidis T, Psannis KE, Siakavara K, Ishibashi Y. A survey on spectrum sensing algorithms for cognitive radio networks. In: 7th International Conference on Modern Circuits and Systems Technologies (MOCAST); 2018. pp. 1-4

[13] Orumwense E, Oyerinde O, Mneney S. Improving trustworthiness amongst nodes in cognitive radio networks. In: Southern Africa Telecommunication Networks and Applications Conference; 2014. pp. 401-406

[14] Jin Z, Anand S, Subbalakshmi KP. Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks. In: IEEE Global Telecommunications Conference; 2010. pp. 1-5

[15] Jain S, Dhawan A, Jha CK. Emulation attack in cognitive radio networks: A study. International Journal of Computer Networks and Wireless Communications (IJCNWC). 2014;**4**(2):169-172

[16] Lakshmibai T, Chandrasekaran B, Parthasarathy C. Primary user authentication in cognitive radio networks: A survey. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 2014;**3**(1):6935-6942

[17] Tang L, Wu J. Research and analysis on cognitive radio network security. Wireless Sensor Network. 2012;**4**:120-126

[18] Alhakami W, Mansour A, Safdar GA. Spectrum sharing security and attacks in CRNs: A review. International Journal of Advanced Computer Science and Applications. 2014;**5**(1):76-87

[19] Tabatabaee S, Bagheri A, Shahini A, Shahzadi A. An analytical model for primary user emulation attacks in IEEE 802.22 networks. In: International Conference on Connected Vehicles and Expo; 2013. pp. 693-698

[20] Kim H. End-to-end authentication protocols for personal/portable devices over cognitive radio networks. International Journal of Security and Its Applications. 2014;**8**(4): 123-138

[21] Shan-shan W, Xing-guo L, Bai-nan L. Primary user emulation attacks analysis for cognitive radio networks communication. TELKOMNIKA. 2013;**11**(7):3905-3914

[22] Xiea X, Wang W. Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding. Journal of Ubiquitous Systems & Pervasive Networks. 2014;**5**(1):1-8

[23] Das D, Das S. Eigenvalue detection based method to mitigate PUEA in cognitive radio networks. IEEE International Conference on Advanced Networks and Telecommunication Systems; 2013. pp. 1-6

[24] Liu Y, Ning P. Enhanced wireless channel authentication using time-synched link signature. In: Proceedings IEEE INFOCOM; 2012. pp. 2636-2640

[25] Patwari N, Kasera SK. Robust location distinction using temporal link signatures. IEEE Transactions on Mobile Computing. 2010;**10**(3):449-462

[26] Liu Y, Ning P, Dai H. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In: IEEE Symposium on Security and Privacy; 2010. pp. 286-301

[27] Wang W, Li H, Sun Y, Han Z, Attack-proof collaborative spectrum sensing in cognitive radio networks. In: 43rd Annual Conference on Information Sciences and Systems; 2009. pp. 130-134

[28] Salem F, Ibrahim MH, El-Wahab Ali IA. Secure authentication scheme preventing wormhole attacks in cognitive radio networks. Asian Journal of Computer Science and Technology. 2013;**2**(4):52-55

[29] Salem FM, Ibrahim MH, Ibrahim II. A primary user authentication scheme for secure cognitive TV spectrum sharing. International Journal of Computer Science Issues. 2012;**9**(4): 157-166

[30] Saber MJ, Sadough SMS. Optimal energy detection in cognitive radio networks in the presence of malicious users, In: Third International Conference on Computer and Knowledge Engineering; 2013. pp. 173-177

[31] Alahmadi A, Abdelhakim M, Ren J, Li T. Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard. In: IEEE Global Communications Conference; 2013. pp. 3329-3334

[32] Borle KM, Chen B, Du W. A physical layer authentication scheme for countering primary user emulation attack. In: IEEE International Conference on Acoustics, Speech and Signal processing; 2013. pp. 2935-2939

[33] Chandrashekar S, Lazos L. A primary user authentication system for mobile cognitive radio networks. In: 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies; 2010. pp. 1-5

[34] Gao Z, Zhu H, Li S, Suguo D, Xu L. Security and privacy of collaborative spectrum sensing in cognitive radio networks. IEEE Wireless Communications. 2012;**19**(6):1536-1584

[35] Chen R, Park J-M, Reed JH. Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications. 2008;**26**(1):25-37

[36] Di P, Alexander M. Wyglinski, primary-user emulation detection using database-assisted frequency-domain action recognition. IEEE Transactions on Vehicular Technology. 2014;**63**(9):4372-4382

[37] Jo M, Han L, Kim D, In HP. Selfish attacks and detection in cognitive radio ad-hoc networks. IEEE Network. 2013;**27**(3):46-50

[38] Sujitha R, Poornima. Efficient detection of selfish attacks in cognitive radio networks using COOPON algorithm. International Journal of Advanced Research Trends in Engineering and Technology. 2015;**2**(23):84-91

[39] Saletm FM, Ibrahim MH, Ali IA, Ibrahim II. Matched-filter-based spectrum sensing for secure cognitive radio network communications. International Journal of Computer Applications. 2014;**87**(18):41-44

[40] Nomura R, Masahiro K, Mizuno T. Radio-free mutual authentication for cognitive radio network. Information and Media Technologies. 2011;**6**(2):580-594

[41] Kim HS. Location-based authentication protocol for first cognitive radio networking standard. Journal of Network and Computer Applications. 2011;**3**(4):1161-1167

[42] Taheri S, Sharifi A, Berangi R. Deal with attacks over cognitive radio networks authentication. International Journal of Computer Technology & Applications; 2012;**2013**(6): 2027-2032

[43] Blesa J, Romero E, Rozas A, Araujo A. PUE attack detection in CWSNs using anomaly detection techniques. EURASIP Journal on Wireless Communications and Networking. 2013:1-13

[44] Araujo A, Blesa J, Romero E, Villanueva D. Security in cognitive wireless sensor networks. Challenges and open problems. EURASIP Journal on Wireless Communications and Networking. 2012;**2012**:1-8

[45] Jin Z, Anand S, Subbalakshmi KP. Detecting primary user emulation attacks in dynamic spectrum access networks. In: IEEE International Conference on Communications; 2009. pp. 1-5

[46] Qi Z, Li Q, Hsieh G. Against cooperative attacks in cooperative spectrum sensing. IEEE Transactions on Wireless Communications. 2013;**12**(6):2680-2687

[47] Jackson DS, Zang W, Gu Q, Cheng W, Yu M. Exploiting and defending trust models in cooperative spectrum sensing. EURASIP Journal on Wireless Communications and Networking. 2015;**2015**:1-18

[48] Lu J, Ping Wei A. Scheme to counter SSDF attacks based on hard decision in cognitive radio networks. WSEAS Transactions on Communications. 2014;**13**:242-248

[49] Orumwense E, Oyerinde O, Mneney S. Improving trustworthiness amongst nodes in cognitive radio networks. In: Conference on South Africa Telecommunication Networks and Applications; 2014. pp. 401-406

[50] Zhou X, Xiao Y, Li Y. Encryption and displacement based scheme of defense against primary user emulation attack. In: 4th IET International Conference on Wireless, Mobile & Multimedia Networks; 2011. pp. 44-49

[51] Dang M, Zhao Z, Zhang H. Detection of primary user emulation attacks based on compressive sensing in cognitive radio networks. In: International Conference on Wireless Communications & Signal Processing; 2013. pp. 1-5

[52] Pu D, Shi Y, Ilyashenko AV, Wyglinski AM. Detecting primary user emulation attack in cognitive radio networks. In: IEEE Global Telecommunications Conference; 2011. pp. 1-5

[53] Haghighat M, Sadough SM, Cooperative spectrum sensing in cognitive radio networks under primary user emulation attacks. In: 6th International Symposium on Tele communications; 2012. pp. 148-151

[54] Hao D, Sakurai K. A differential game approach to mitigating primary user emulation attacks in cognitive radio network. In: 26th IEEE International Conference on Advanced Information Networking and Applications; 2012. pp. 495-502

[55] Chen C, Cheng H, Yao Y-D. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack. IEEE Transactions on Wireless Communications. 2011;**10**(7):2135-2141

[56] Bao F, Chen H, Xie L. Analysis of primary user emulation attack with motional secondary users in cognitive radio networks. In: IEEE 23rd International Symposium Personal Indoor and Mobile Radio Communications; 2012. pp. 956-961

[57] Jin Z, Anand S, Subbalakshmi KP. Impact of primary user emulation attacks on dynamic spectrum access networks. IEEE Transactions on Communications. 2012;**60**(9):2635-2643

[58] Brown TX, Sethi A. Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment, mobile network applications. In: 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications; 2008. pp. 456-464

[59] Wang W. Denial of service attacks in cognitive radio networks. In: 2nd Conference on Environmental Science and Information Application Technology; 2010. pp. 530-533

[60] Soderi S, Dainelli G, Hämäläinen M, Iinatti J. Signal fingerprinting in cognitive wireless networks. In: International Conference on Cognitive Radio Oriented Wireless Networks; 2014. pp. 267-270

[61] Amjad MF, Aslam B, Zou CC. DS3: A dynamic and smart spectrum sensing technique for cognitive radio networks under denial of service attack. In: IEEE Global Communications Conference; 2013. pp. 1149-1154

[62] Sodagari S, Attar A, Leung VCM, Bilen SG. Denial of service attacks in cognitive radio networks through channel eviction triggering. In: IEEE Global Telecommunications Conference; 2010. pp. 1-5

[63] Butt MA, Zaman M. Cognitive radio network: Security enhancements. Journal of Global Research in Computer Science. 2013;**2**(4):36-41

[64] Idoudi H, Daimi K, Saed M. Security challenges in cognitive radio networks. In: Proceedings of the World Congress on Engineering; 2014. pp. 498-504

[65] Sen J. A survey on security and privacy protocols for cognitive wireless sensor networks. Journal of Network and Information Security. 2013;**1**(1):1-31

[66] Mangir T, Sarakbi L, Younan H. Detecting malicious activities in ZigBee networks using cognitive radio. International Journal of Distributed and Parallel Systems. 2011;**2**(6):51-62

[67] Sood V, Singh M. On the performance of detection based spectrum sensing for cognitive radio. International Journal of Electronics & Communication Technology. 2011;**2**(3): 140-143

[68] Pal RU, Indurkar PR, Lakhe PR. Review of performance of energy detection, matched filter detection and cyclostationary detection based spectrum sensing under different wireless channels. International Journal of Engine Research. 2015;**3**(2):6-9

[69] Buttar S. Comparison of energy detection in cognitive radio over different fading channels. International Journal of Advancements in Research and Technology. 2012;**1**(2):99-105

[70] Kim YM, Zheng G, Sohn SH, Kim JM. An alternative energy detection using sliding window for cognitive radio system. In: Tenth International Conference on Advanced Communication Technology; 2008. pp. 481-485

[71] http://www.ni.com/white-paper/4844/en/

[72] Khatun M. Implement a new window function and design FIR filters by using this new window. International Journal of Engineering and Computer Science. 2014;**3**(3):4087-4090

[73] Wang H, Noh G, Kim D, Kim S, Hong D. Advanced sensing techniques of energy detection in cognitive radios. Journal of Communications and Networks. 2010;**12**(1):19-29