SCHOOL OF INFRASTRUCTURE, PROCESS ENGINEERING AND TECHNOLOGY
AND SCHOOL OF ELECTRICAL ENGINEERING AND TECHNOLOGY
FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

Book of Proceedings IEC 2023

4 INTERNATIONAL ENGINEERING CONFERENCE

Theme

Smart Engineering and Technology Innovation for Enhancing Economic Growth

21st - 23rd MARCH 2023

Venue: NITDA ICT-HUB Federal University of Technology, Minna, Niger State - Nigeria

Edited By: Technical Sub-Committee

MEMBERS OF THE CONFERENCE ORGANISING COMMITTEE

1.	Engr. Prof. M. Alhassan	Chairman
2.	Engr. Prof. O.M. Olaniyi	Co-Chairman
3.	Engr. Dr. Bala A. Salihu.	Member
2.	Engr. Prof. S.M. Dauda	Member
3.	Engr. Dr. A. U. Usman.	Member
4.	Engr. Dr. T. E. Adejumo.	Member
5.	Engr. Dr. M. D. Yahya	Member
6.	Engr. Dr. Alkali Babawuya.	Member
7.	Engr. Prof. R. A. Muriana.	Member
8.	Engr. Dr S. A. Mohammed	Member
9.	Engr. Dr. B. A. Orhevba.	Member
10.	Engr. Dr. Michael David	Secretary

MEMBERS OF SUB-COMMITTEES

TECHNICAL SUB-COMMITTEE

1.	Engr. Dr. Bala S. Salihu	Chairman
2.	Engr. Dr. Eyitayo Afolabi	Member
3.	Engr. Dr. M. U. Garba	Member
4.	Engr. Dr. U. S. Dauda	Members
5.	Engr. Dr. James Ambafi	Member
6.	Engr. Dr. S. A. Mohammed	Member
7.	Engr. Dr. B. A. Orhevba	Member
8.	Engr. Dr. A. M. Ibrahim	Member
9.	Engr. Balogun Temitope	Member
10.	Engr. Dr. T.A. Folorunso	Member
11.	Engr. Buhari U. Umar	Member
12.	Engr. Dr. A. Yusuf	Member
13.	Engr. Dr. Michael David	Member
14.	Engr. Dr. M. Abubakar	Secretary

ICT SUB-COMMITTEE

1.	Engr. Dr. Bala A. Salihu	Chairman
2.	Engr. Dr. Sadiq Ahmed	Member
3.	Engr. Dr. Steven Oyewobi	Member
4.	Engr. S. A. Bala	Member

WELFARE SUB-COMMITTEE

1.	Engr. Dr. M.D. Yahya	Chairman
2.	Engr. Prof. R.A. Muriana	Member
3.	Engr. Dr. A.J. Otaru	Member
4.	Engr. Dr. B. A. Orhevba	Member
5.	Engr. Dr. C. O. Alenoghenna	Member
6.	Engr. Dr. A. Yusuf	Member
7.	Mr. Usman Baro	Member
8.	Engr. Danlami	Member
9.	Engr. Dr. B.A. Orhevba	Secretary

FINANCE SUB-COMMITTEE

1.	Engr. Dr. B. A. Orhevba	Chairman
2.	Engr. Prof. O. A Olugboji	Member
3.	Eng. Bello Abdulkadir	Member
4.	Eng. Dr. T. E. Adejumo	Member
5.	Engr. Dr. M. D. Yahya	Member
6.	Engr. Gana Menegbe Esther	Member
7.	Dr. Abdulkadir Balogun	Member
8.	Dr. Alhassan Musa	Member
9.	Engr. Buhari Umar	Member
10.	Engr. Dr. Alkali Babawuya	Member

LOGISTICS SUB-COMMITTEE

1.	Engr. Prof. R. A. Muriana	Chairman
2.	Dr. T. E. Adejumo	Secretary
3.	Shaka Abdulazeez Enahoro	Member
4.	Nweke Augustine Chidiebele	Member
5.	Adeyeye Sumayyah Adedola	Member
6.	Abraham Dirisu	Member
7.	Mohammed Shehu	Member
8.	Dr. Achonu Adejo	Member

DIASPORA COMMITTEE

1.	Engr. Dr S. A. Mohammed	Chairman
2.	Engr. Prof. A. S. Abdulkareem	Member
3.	Engr. Musa Umar	Member
4.	Engr. Dr. Olatomiwa Lanre	Member
5.	Engr. Dr. Uzodinma Okoro	Member
6.	Prof. Monika Prakash	Member
7.	Engr. Dr. Saidu Mohammed	Member
8.	Engr. Fidelis Jonah Usman	Member

Forward

International Engineering Conference is the biennial conference being organized by the Schools of Engineering of the Federal University of Technology, Minna. The conference is meant to create a forum to showcase scientific discoveries, encourage knowledge sharing and build an ecosystem for Engineering and allied disciplines. This year's edition tagged the 4th International Engineering Conference (IEC 2023) with the theme "***Smart Engineering and Technology Innovation for Enhancing Economic Growth***" is carefully planned to proffer smart solutions to economic challenges through technological innovations.

About 120 technical papers were received out of which 85 were accepted after thorough peer-review processes. The richness of this conference is the diver contribution from a wide range of Authors cut-across academia, industry, and researchers. Their technical and logical presentations give a robust knowledge base in Engineering and allied disciplines. It is not surprising that the conference has been receiving more attention from Authors and participants across the globe. The keynote address and the lead papers herein are from seasoned industry key players and top-notch researchers with international recognition. This conference is packed with research contributions and design and implementation of innovative technologies that have the potential to advance smart engineering and realize the goals set out for Industry 4.0 as the 4th industrial revolution. We should take great advantage of it to learn new ideas, network with experts, and play a part in the revolution that is already taking place.

The Federal University of Technology Minna, the Citadel of learning is known for her contributions to research and innovation, especially in Engineering. Eminent researchers and scholars from the University form part of the conference organizing committee along with the editorial and Technical Board from the United Kingdom, Saudi Arabia, South Africa, Malaysia, Australia, etc.

On behalf of the conference organizing committee, I thank you all for participating. To our dedicated reviewers, you are sincerely appreciated for finding time to do a thorough review. Thank you all and we hope to see you at the 5th International Engineering Conference.

Engr. Prof. Mohammed Alhassan
Chairman, Conference Organising Committee

Table of Contents

4th International Engineering Conference (IEC 2022)
Federal University of Technology, Minna, Nigeria

A Survey of the Primary User Emulation Attack in the Cognitive Radio Networks

*Olaleru, G[1], Ohize H.O[2], Dauda U.S[3], Mohammed A.S[4]
[1]Electrical and Electronics Engineering Department, Federal University of Technology, PMB 65 Minna Niger State, Nigeria
[2]Electrical and Electronics Engineering Department, Federal University of Technology, PMB 65 Minna Niger State, Nigeria
[3] Federal University of Technology, PMB 65 Minna Niger State, Nigeria
[4] Federal University of Technology, PMB 65 Minna Niger State, Nigeria.
Corresponding author email: graceolaleru9@gmail.com +2348164649551

ABSTRACT
Cognitive Radio Technology (CRT) helps alleviate the spectrum scarcity and spectrum underutilization problems experienced by wireless networks and wireless devices by enabling the intelligent and opportunistic use of the licensed frequency band by unlicensed users. However, due to its wireless nature, it is subject to some security threats that affect the practical implementation of the CRT. In this paper, we have discussed some of the security threats affecting the protocol stack and the five layers of the Cognitive Radio Network (CRN), with a focus on the Primary User Emulation Attack (PUEA). The PUEA is one of the most common attacks on the CRN's physical layer. In this attack, a selfish or malicious user mimics the primary user's (PU) signal features to fool the legitimate secondary users (SUs), causing the legitimate SUs to leave the available channel while the real PU is absent. Although many review papers enhanced our knowledge of the PUEA, in this paper we meld new research findings with the old ones to keep up the pace in the research community. Also, we discussed some detection and countermeasures for the PUEA in the CRN. Finally, a summary of the findings on how best to mitigate the effect of PUE attacks in the CR is presented.

Keywords: *Cognitive Radio, Primary User, Primary User Emulation Attack, Secondary User, Security threats.*

1 INTRODUCTION

The radio spectrum used for wireless communications is a scarce resource due to the dramatic increase in the number of wireless devices and more bandwidth-demanding multi-media services [1-4]. These wireless devices use either the licensed spectrum or the unlicensed spectrum. The unlicensed bands are becoming overcrowded because all wireless users can connect. However, the licensed bands are either unused or underutilized at some geolocation and time. To address the problem of frequency scarcity and spectrum underutilization, Cognitive Radio (CR) was introduced by Joseph Mitola in 1999 [5]. The CR is a software-defined radio that enables Dynamic Spectrum Access (DSA) which enables unlicensed users to intelligently and opportunistically access and utilize the spectrum without disrupting the licensed users and therefore a better service to achieve improvement in frequency usage [2, 6]. The CR performs four basic functions that allow it to address spectrum shortages and channel underutilization [7]. These functions are (a) Spectrum Sensing which involves identifying the primary user's spectrum occupancy status, (b) Spectrum management, which captures the best available spectrum to meet users' communication needs and avoid collisions with other CRs (c) spectrum sharing: this relates to the provision of fair spectrum scheduling, and (d) spectrum mobility: defined as the process of a CR user changing its operating frequency to meet the quality of service. However, due to the wireless nature of CRT and the priority given to licensed users or primary users (PUs) over secondary users (SUs) in spectrum usage, CRN faces several security threats. One of these threats is PUEA, in which a malicious user fools the SU by mimicking the PU's signal features in relation to the PU's occupancy status. The impacts of PUEA include denial of service, wasted bandwidth, connection unreliability, and degrading the practical implementation of the CRN. Other threats that the CRN faces are classified as they affect the protocol stack and the five layers of the CR network. These include, but are not limited to: Common Control Data Attack (CCDA), Sinkhole Attack, Hello flood attack, lion attack, and jellyfish attack. These threats aim to reduce the possibility of building a real CRN, so, threat mitigation is crucial to building a real CRN.

In this paper, we have highlighted the security threats affecting the CRN with a focus on the PUEA. We also highlighted some of the detection and countermeasures used for the PUEA in the CR networks. This paper has the following research contributions:

- A detailed discussion of the security threats affecting the protocol stack and the five layers of the CRN.
- A detailed review of the PUEA in CRN stating its classification, its impacts, methods for its detection, and countermeasures.
- A summary of the findings on how best to mitigate the impact of PUE attacks in the CR.
- Meld new research findings with the old ones to keep up the pace in the research community.

The remainder of this paper is organized as follows: Section 2 discusses the various security threats faced by the CRNs, followed by a concise introduction of the PUEA in Section 3. In Section 4, we highlighted the classification of the PUEA, next; in Section 5 we listed the impact of the PUEA on the CRN. Various detection methods and countermeasures for the PUEA are presented in Section 6. Finally, in Section 7, we completed the review and proposed future work.

2 SECURITY THREATS IN CRN

In implementing any wireless technology, its security aspects need to be thoroughly looked into [8, 9]. The CRT faces some security threats due to the wireless nature of the CR and its inherent nature. These threats are classified as they affect the protocol stack and the five layers of the CRN [10, 11]. These attacks are described in this section and a summary of the attacks is presented in Table 1. They are as follows:

a) **Physical layer**: The physical layer serves as an interface to the data communication medium. The Attacks associated with this layer include:

i. Jamming Attack: In this type of attack, a jammer continuously sends a data packet into the channel, causing the SU not to recognize the channel when it is idle [12].

ii. PUEA is where a selfish or a malicious user mimics the signaling features of the PU to fool the SU and identify the attacker as the real PU [10].

iii. Common Control Data Attack (CCDA) affects the transmission process by refusing channel components to share frequency usage information [12, 13]

iv. Objective Function Attack (OFA) in which the utility resource parameters could be modified by the malicious user, resulting in the CR node not adapting correctly [4, 12, 13].

b) **Link Layer**: In this layer, data is transmitted from one node to another. The Attacks common to this layer include:

i. Spectrum Sensing Data Falsification (SSDF), where a malicious user sends false spectrum sensing (SS) results to the fusion centre or other users to fool them about channel availability [2, 10].

ii. Selfish Channel Negotiation (SCN): Involves a malicious user feeding the channel with false information to change the node's route [10, 13].

iii. Control Channel saturation Denial of Service (DoS) attack, where the attacker reserves the control channel (CC) and eventually saturates the CC [12].

c) **Network Layer**: In this layer, packets are sent from the sender device to the receiver device which is on a different network. The attacks peculiar to this layer are;

i. Sinkhole attack in which the attacker asserts itself as the most suitable route to a given destination to fool the neighboring nodes into using this route to send their packets but end up losing them [12].

ii. Hello Flood Attack: Here, the attacker broadcasts a message to all CR nodes in the network with sufficient transmission power to convince the nodes that the attacker is the nearest neighbor in the node's network and should be used for transmitting the packets to the targeted receiver's node. However, these packets are lost before the packets reach the receiving node [10, 13].

iii. Sybil Attack: In this type of attack, the attacker creates a large number of false identities and behaves like geographically different devices. Each of the false identities requests for the frequency band, and results in the reduction of spectrum usage by legitimate SUs [13].

TABLE 1: VARIOUS ATTACKS ON THE PROTOCOL STACK

Layers in CRNs	**Attacks corresponding in the Layers**
Physical Layer	PUEA; CCDA; OFA; Jamming attack
Link Layer	SSDF; SCN; control channel saturation DoS
Network Layer	Hello flood attack; Sinkhole attack; Sybil Attack.
Transport Layer	Lion attacks; Jellyfish attack
Application Layer	All the above attacks have various damaging effects on this layer.

d) **Transport Layer**: This layer is used to transfer data between two end hosts. Attacks against this layer include:

i. Lion attack in which the attacker launches a PUEA to force the CR nodes to frequency hop between channels, thus, disrupting the Transport Control Protocol (TCP) [11].

ii. Jellyfish Attack affects the TCP, though the attack is executed at the network layer [10].

e) **Application Layer**: It can be affected by all attacks corresponding to the first four layers [11].

In this paper, the focus is on the PUEA in CRN.

3 PRIMARY USER EMULATION ATTACK

The PUEA is the most common threat affecting the CRN's physical layer. In this type of attack, a selfish or malicious user emulates the signaling features of the PU to fool the SUs that the real PU is active and therefore forces the SUs to leave the bands while the real PU is not active [4, 14, 15]. This attack occurs because the PU is given priority in spectrum usage in CRN therefore, a selfish user or malicious user tries to mimic the PU signal characteristic to gain access to the free bands by forcing the legitimate secondary user to leave the free band for it as illustrated in Figure 1.

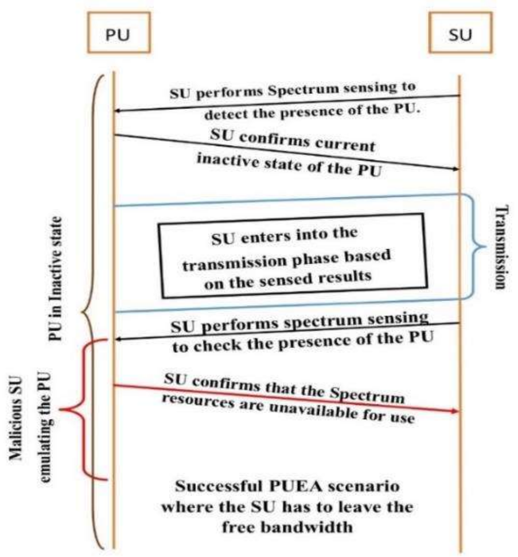

Figure 1: Illustration of a successful PUEA

The SU performs SS to capture the PU occupancy status. When the SU detects that the PU is absent, it starts to transmit, and after some time, it performs SS again, however, the PUEA has taken over the channel by mimicking the signal characteristics of the PU and transmitting the emulated signal while the PU is still absent thus, other SUs leave the free band for the PUEA.

4 CLASSIFICATIONS OF THE PUEA

The PUEA can be classified as follows [9, 10]:

i. Selfish SU or Malicious SU Attacker

The selfish SU attacker reserves a specific band for its transmission while a malicious attacker aims to occupy the whole free band, causing legitimate SUs to move from one free band to another [9, 10]. A malicious user does more damage to the CRN as it causes a DoS and a reduction in the available bandwidth for SUs [8, 16].

ii. Power-Fixed or Power-Adaptive Attackers

Attackers can have an adaptive power level or a fixed power level. The power-adaptive attacker can acclimatize its transmit power depending on the PU signal, while the power-fixed attacker uses a predetermined, unchanging power, independent of the actual power of the incumbent signal [13].

iii. Mobile or Static Attacker: A mobile attacker constantly changes its position in the CRN, while a static attacker maintains a fixed position in the CRN.

5 IMPACTS OF PUEA ON CRN

The impacts of PUEA on CRN include: an increase in call drop rate, delay in networks, degradation of the QoS, causes DoS, bandwidth wastage, connection unreliability, disruption of the primary network, degradation in the practical implementation of the CRNs and the possible collapse of the CRNs.[8, 9, 16].

6 EXISTING DETECTION AND COUNTERMEASURES FOR THE PUEA IN CRNs.

Several detection methods for the PUEA have been developed. Methods include [9, 11, 14, 17, 18] energy detection, signature-based detection, authentication methods, user profile detection, and location-based detection methods.

- Energy Detection (ED): This method is widely used due to its simplicity and easy implementation [18-21]. In ED, a SU will be able to see the signal features of the other SUs, but not those of the PU. Thus, when a SU sees a signal that it can easily identify, it assumes that the signal is that of the SU. Consequently, any signal that the SU cannot detect is the PU signal. However, this technique is not robust for PUEA detection [9] when the attacker is an adaptive power PUEA [22].

- Signature-based detection: This approach integrated cryptographic signatures with wireless link signatures to distinguish a PU signal from the PUEA signal. It also uses an auxiliary node to authenticate signals from its associated PU [17, 23].

- Analytical model-based detection: This method is based on the analytical models of the CRNs. These include [24-27] the Wald's Sequential Probability Ratio Test and Neyman-Pearson Composite Hypothesis Test (NPCHT) to detect the PUEA in evanescent wireless channels considering multiple malicious users. Also, in [28] the dog-fight approach was proposed in which the defenders randomly select channels to detect and avoid the PUEA.

- Feature Detection: In this technique, the SUs try to find a specific feature of a detected signal, for example, a pilot or correlation device [6] which can use this detection technique can recognize the intrinsic features of the PU signals and thus; enable them to distinguish these signals from the SU signal.
- Location-based detection: This technique is widely used by researchers. These include [9, 11, 18, 29-31] Transmitter Verification Scheme (Loc-Def), Received Signal Strength (RSS), Time of Arrival (TOA), Angle of Arrival (AOA), Time Difference of Arrival (TDOA), Distance Ratio Test (DRT), and Distance Difference Test (DDT). They are often used to detect a static attacker.
- Other detection and mitigation techniques include mitigation based on a surveillance process [32], detection with Kalman filter [33], AES-assisted DTV scheme [34], detection based on Hash Message Authentication Code [35], Hybrid of TDOA localization technique, and Modified Particle Swarm Optimization (MPSO) [4]. Table 2 presents the detection/mitigation techniques for PUEA in the CRN.

TABLE 2: DETECTION/MITIGATION TECHNIQUE FOR DIFFERENT KINDS OF PUEA

Types of PUE Attackers	Detection/Mitigation technique
Selfish or malicious attack	Any of the detection/mitigation techniques for PUEA can be used.
Power-fixed or Power adaptive attacker	The localization techniques can be used.
Static attacker	A hybrid of location techniques and an optimization algorithm can be used.
Mobile attacker	An energy detection technique can be employed.

7 CONCLUSION AND FUTURE WORK

CRT is an excellent solution to the spectrum underutilization and spectrum scarcity problems faced by wireless networks as it enables DSA. However, due to the wireless nature of CR, it encounters some security challenges that pose a threat to the practical implementation of this technology. In this paper, we discuss the security threats affecting the cognitive protocol stack and the five layers of the CRN. We have focused more on the PUEA, and given their impact on the CRN, their classification, detection, and countermeasures for the PUEA. Most researchers have worked to detect the PUEA but little attention has been paid to how to eliminate the PUEA from the CRNs. Therefore, future work lies in the development of robust systems to eliminate the PUEA in the CRNs.

REFERENCES

1 Ohize, H.O.: 'Adaptive and autonomous protocol for spectrum identification and coordination in ad hoc cognitive radio network', University of Cape Town, 2017
2 Arjoune, Y., and Kaabouch, N.: 'A Comprehensive Survey on Spectrum Sensing in Cognitive Radio Networks: Recent Advances, New Challenges, and Future Research Directions', Sensors (Basel), 2019, 19, (1), pp. 126
3 Ul Hassan, M., Rehmani, M.H., Rehan, M., and Chen, J.: 'Differential privacy in cognitive radio networks: A comprehensive survey', Cognitive Computation, 2022, pp. 1-36
4 Olaleru, G., Ohize, H., Mohammed, A.S., and Dauda, U.S.: 'Optimal Detection Technique for Primary User Emulator in Cognitive Radio Network', in Editor (Ed.)^(Eds.): 'Book Optimal Detection Technique for Primary User Emulator in Cognitive Radio Network' (IEEE, 2021, edn.), pp. 1-6
5 Mitola, J., and Maguire, G.Q.: 'Cognitive radio: making software radios more personal', IEEE personal communications, 1999, 6, (4), pp. 13-18
6 Jayapalan, A., Savarinathan, P., Reddy, J.C., and Baskar, J.D.: 'Detection and Defense of PUEA in Cognitive Radio Network', Arabian Journal for Science and Engineering, 2021, 46, (4), pp. 4039-4048
7 Omer, I., Hamid, K., and Mohamed, M.: 'Overview on Cognitive Radio Network Review', International Journal of Engineering Sciences Paradigms and Researches, 2016, 33, (20), pp. 7-13
8 Sharma, R.K., and Rawat, D.B.: 'Advances on security threats and countermeasures for cognitive radio networks: A survey', IEEE Communications Surveys & Tutorials, 2014, 17, (2), pp. 1023-1043
9 Gupta, I., and Sahu, O.: 'An Overview of primary user emulation attack in cognitive radio networks', in Editor (Ed.)^(Eds.): 'Book An Overview of primary user

emulation attack in cognitive radio networks' (IEEE, 2018, edn.), pp. 27-31
10 Singh, A., and Sharma, A.: 'A survey of various defense techniques to detect primary user emulation attacks', International Journal of Current Engineering and Technology, 2014, 4, (2), pp. 900-908
11 Das, D., and Das, S.: 'Primary User Emulation Attack in Cognitive Radio Networks: A Survey', IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC)

2013
12 El-Hajj, W., Safa, H., and Guizani, M.: 'Survey of security issues in cognitive radio networks', Journal of Internet Technology, 2011, 12, (2), pp. 181-198
13 Rehman, A., and Prakash, D.: 'Detection of PUE attack in CRN with reduced error in location estimation using novel bat algorithm', International Journal of Wireless Networks and Broadband Technologies (IJWNBT), 2017, 6, (2), pp. 1-25
14 Ghanem, W.R., Essam, R., and Dessouky, M.: 'Proposed particle swarm optimization approaches for detection and localization of the primary user emulation attack in cognitive radio networks', in Editor (Ed.)^(Eds.): 'Book Proposed particle swarm optimization approaches for detection and localization of the primary user emulation attack in cognitive radio networks' (IEEE, 2018, edn.), pp. 309-318
15 Patil, P.: 'Position Verification and Identification of Primary User Emulation (PUE) Attack in Cognitive Radio Network', International Journal for Research in Applied Science and Engineering Technology, 2018, 6, pp. 348-362
16 Jin, Z., Anand, S., and Subbalakshmi, K.P.: 'Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks', IEEE Transactions on Communications, 2012, 60, (9), pp. 2635-2643
17 Pu, D.: 'Primary user emulation detection in cognitive radio networks', Worcester Polytechnic Institute, 2013
18 Chen, R., Park, J.-M., and Reed, J.H.: 'Defense against primary user emulation attacks in cognitive radio networks', IEEE Journal on selected areas in communications, 2008, 26, (1), pp. 25-37
19 Yu, R., Zhang, Y., Liu, Y., Gjessing, S., and Guizani, M.: 'Securing cognitive radio networks against primary user emulation attacks', IEEE Network, 2015, 29, (4), pp. 68-74
20 Fragkiadakis, A.G., Tragos, E.Z., and Askoxylakis, I.G.: 'A survey on security threats and detection techniques in cognitive radio networks', IEEE Communications Surveys & Tutorials, 2012, 15, (1), pp. 428-445
21 Ghanem, W.R., Shokair, M., and Dessouky, M.: 'Investigation of PUEA in cognitive radio networks using energy detection in different channel model', Circuits and Systems: An International Journal (CSIJ), 2015, 2, (2/3)
22 Ghanem, W.R., Mohamed, R.E., Shokair, M., and Dessouky, M.I.: 'Particle swarm optimization approaches for primary user emulation attack detection and localization in cognitive radio networks', arXiv preprint arXiv:1902.01944, 2019
23 Liu, Y., Ning, P., and Dai, H.: 'Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures', in Editor (Ed.)^(Eds.): 'Book Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures' (IEEE, 2010, edn.), pp. 286-301
24 Tabatabaee, S., Bagheri, A., Shahini, A., and Shahzadi, A.: 'An analytical model for primary user emulation attacks in IEEE 802.22 networks', in Editor (Ed.)^(Eds.): 'Book An analytical model for primary user emulation attacks in IEEE 802.22 networks' (IEEE, 2013, edn.), pp. 693-698
25 Tan, Y., Sengupta, S., and Subbalakshmi, K.P.: 'Primary user emulation attack in dynamic spectrum access networks: a game-theoretic approach', IET communications, 2012, 6, (8), pp. 964-973
26 Jin, Z.: 'Primary user emulation attack in dynamic spectrum access networks: threats, mitigation and impact', Stevens Institute of Technology, 2012
27 Jin, Z., Anand, S., and Subbalakshmi, K.: 'Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks', in Editor (Ed.)^(Eds.): 'Book Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks' (IEEE, 2010, edn.), pp. 1-5
28 Li, H., and Han, Z.: 'Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems—Part II: Unknown channel statistics', IEEE Transactions on Wireless Communications, 2010, 10, (1), pp. 274-283
29 Fassi Fihri, W., El Ghazi, H., Abou El Majd, B., and El Bouanani, F.: 'A decision-making approach for detecting the primary user emulation attack in cognitive radio networks', International Journal of Communication Systems, 2019, 32, (15), pp. e4026
30 Adebo, S., Onwuka, E., Usman, A., and Onumanyi, A.: 'A hybrid localization scheme for detection of primary user emulator in cognitive radio networks', International Journal of Computing and Digital Systems, 2019, 8, (03), pp. 217-227
31 Adebo, S., Onwuka, E., Usman, A., and Onumanyi, A.: 'Cooperative-hybrid detection of primary user emulators in cognitive radio networks', International Journal of Electrical and Computer Engineering, 2020, 10, (3), pp. 3116
32 Ta, D.-T., Nguyen-Thanh, N., Maillé, P., and Nguyen, V.-T.: 'Strategic surveillance against primary user emulation attacks in cognitive radio networks', IEEE Transactions on Cognitive Communications and Networking, 2018, 4, (3), pp. 582-596

33 El Mrabet, Z., Arjoune, Y., El Ghazi, H., Abou Al Majd, B., and Kaabouch, N.: 'Primary user emulation attacks: A detection technique based on Kalman filter', Journal of Sensor and Actuator Networks, 2018, 7, (3), pp. 26

34 Alahmadi, A., Abdelhakim, M., Ren, J., and Li, T.: 'Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard', IEEE transactions on information forensics and security, 2014, 9, (5), pp. 772-781

35 Ghanem, W.R., Shokair, M., and Desouky, M.: 'Defense against selfish PUEA in cognitive radio networks based on hash message authentication code', International Journal of Electronics and Information Engineering, 2016, 4, (1), pp. 12-21