UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica
Más que un estado sólido
https://doi.org/10.14483/issn.2248-4728

VISIÓN ELECTRONICA
A CURRENT VISION

Primary user emulation in mobile cognitive radio network: a survey

Emulación de usuario primario en la red de radio cognitiva móvil: estudio

Ernesto Cadena-Muñoz[1], Hermes Javier Eslava-Blanco[2], Ingrid Patricia Páez-Parra[3]

INFORMACIÓN DEL ARTICULO

Historia del articulo
Envíado: 12/09/2019
Recibido: 14/09/2019
Aceptado: 22/11/2019

Palabras clave:
Emulación de usuario primario,
Red de Radio Cognitiva,
ataque PUE,
técnicas de detección,
seguridad.

Keywords:
Primary User Emulation,
Cognitive Radio Network,
PUE attack,
detection techniques,
security

RESUMEN

En el caso de las redes emergentes, como la red de radiocomunicaciones cognitivas móviles, es esencial estudiar sus posibles ataques y generar así estrategias de detección. Por lo general, los ataques se centran en una sola capa del modelo OSI, se han estudiado para cada capa desde el nivel físico hasta el nivel de aplicación y se han centrado en los usuarios secundarios fijos. En las redes de radiocomunicaciones cognitivas, la emulación de usuario primario (PUE) es el ataque más estudiado, ya que afecta a todo el ciclo cognitivo desde la capa física hasta las capas superiores. En este documento se definen los tipos de ataque PUE y las contramedidas, analizando los efectos en los usuarios secundarios fijos y móviles y en los atacantes.

ABSTRACT:

For emerging networks such as the mobile cognitive radio network, it is essential to study their possible attacks and thus generate detection strategies. Generally attacks are focused on only one layer of the OSI model, they have been studied for each layer from the physical level to the application level and have focused on fixed secondary users. In cognitive radio networks, the primary user emulation (PUE) is the most studied attack since it affects the entire cognitive cycle from the physical layer to the upper layers. This paper defines types of PUE attack and countermeasures, analyzing the effects on fixed and mobile secondary users and attackers.

1 Facultad de Ingeniería Universidad Nacional de Colombia Bogotá, Colombia E-mail: ecadenam@unal.edu.co
2 Facultad Tecnológica Universidad Distrital Francisco José de Caldas Bogotá, Colombia, E-mail: hjeslavab@udistrital.edu.co
3 Facultad de Ingeniería Universidad Nacional de Colombia Bogotá, Colombia, E-mail: ippaezp@unal.edu.co
Cite this article as: E. Cadena-Muñoz, H. Javier Eslava-Blanco and I. P. Páez-Parra, "Primary user emulation in mobile cognitive radio network: a survey", Visión electrónica, vol. 2, no. 1, Special edition, january-june 2019 https://doi.org/10.14483/issn.2248-4728

1. Introduction

Colombia uses the spectrum management system called command and control, where an operator is given a specific frequency band, whether used or not. This system underutilizes the radioelectric spectrum, which is the most important and limited resource in the area of telecommunications [1]. For this reason, technological alternatives are sought to optimize its use and that's why in the last decade, the interest of the scientific community has grown to the study of mobile cognitive radio networks [2] .

Studies carried out by entities such as the FCC (Federal Communications Commission)[3]and results of doctoral studies in Colombia[4] , have shown that a large part of the radioelectric spectrum is used inefficiently, which offers the possibility of taking advantage of the spectrum that is not being used for the transmission of data of other users, optimizing the radio spectrum management. This is the basis of cognitive radio, sending data from secondary users through frequencies that are not being used by primary users in a moment of time[4] .

In cognitive radio, security is an aspect to be evaluated with the convergence of networks and services in mind, since each type of network has its own security requirements [5] . For example, security and privacy are required against illegal interceptions, espionage techniques or Denial of Service (DoS) attacks, among others [6] . With the emergence of this technology and the current services, the question arises about what attacks can occur in these networks and how to detect them. Several authors have highlighted the importance of evaluating these attacks in cognitive radio networks, in addition to traditional attacks on any mobile network [7].

The exclusive attack on the cognitive radio network called primary user emulation (PUE), is based on the mimic of a primary user's signal, causing an erroneous frequency assignment to the attacker by identifying it as a primary user. The approaches to detecting this type of attack have been designed for each layer of the OSI model, an approach inherited from the traditional fixed network, which does not apply in the same way for mobile cognitive networks [8], [9] .

The attacks to the mobile cognitive networks have evolved and the affectation can reach all or several layers of the network [10]. This implies that the detection of such attacks must also be multi-layered. Several authors have proposed the use of the cross-layer design for the detection of attacks [6], [11], [12], but it is still not validated with a real case, especially for attacks on the mobile cognitive radio network such as PUE, since it allows obtaining and sharing information between non-underlying layers of the network architecture, thus optimizing the detection of the attack [6] .

2. Mobile cognitive radio network security threats

2.1. Mobile Cognitive Radio Network

Cognitive radio is based on intelligent or cognitive radio-defined software (SDR). This concept was raised by Joseph Mitola in 1999, as part of his doctoral thesis [13], defining a cognitive radio device as a portion of the physical world, with the ability to detect a user's communication needs, analyzing the environment and the availability of the system, to use the transmission medium required for a connection [13]. The characteristics of a cognitive radio system are [14]:

- Perception of the environment in which he works, with spectrum sensing techniques.
- Consciousness of the environment, of their own capacities and of the available resources.
- Variability and intelligent adaptation of its transmission and reception configuration.
- Autonomy to act as transmitter or receiver.

After the appearance of the general concept of cognitive radio, the IEEE standard 802.22 [6] [8], is created, defined as the first worldwide standard based on cognitive radio. It seeks to be a standard for wireless regional area networks WRAN (wireless regional area network), which focuses on fixed point-multipoint networks, using the UHF / VHF bands, in a range of 54MHz-862MHz, although the application of its concept is broader .

2.2. Mobile Cognitive Radio Network

The main purpose of the mobile cognitive radio network is to provide cellular services in an independent network without the need of a license. For

this purpose, the cognitive base station senses the environment in a specific frequency range, if a primary user (PU) is not using its assigned frequency, it uses to communicate with a secondary user (SU). It can be a centralized model, but to improve the performance it can be a distributed and cooperative environment [6].

2.3. Security Threats in CRN

An approach to the attacks of cognitive radio networks [15], is described in Figure 1:

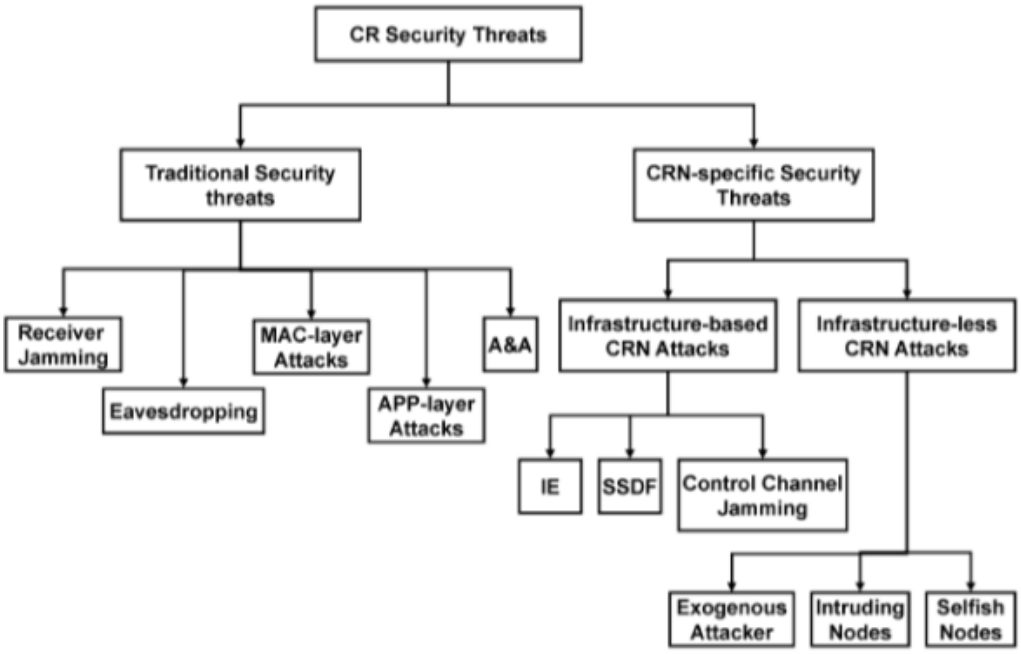

Figure 1. Cognitive Radio Network Security Threats [15]

The main threats of the cognitive radio network are classified into traditional security threats, which affect all wireless networks and the threats that appear for the cognitive radio network [7], these have different subdivisions for the different layers of the protocol in security for the cognitive radio network [8], [9].

In a non-cooperative cognitive network, an attack against a user will not affect others, since the other devices act independently and make their own decisions. In a cooperative cognitive network, attacks against a subset of users can have far-reaching effects. For example, an IEEE 802.22 implementation would have a logic in which all secondary devices are migrated to a new free frequency if a single device detected a primary user signal. Thus, an attacker can send a primary user signal to a single IEEE 802.22 device and the network will migrate all users to a new frequency, allowing access to that part of the free spectrum to the attacker [8].

In this figure, the Incumbent Emulation (IE), was the first approach to the primary user emulation attack [8].

3. Primary User Emulation

- PUE Definition

It is the first and the most investigated attack in the cognitive radio network, where the radio transmission frequency mimics the primary signal, causing the attacker user to be mistakenly identified as a primary user assigning the available frequency. The impact on the network is high because it causes: bandwidth waste, QoS degradation, denial of service, interference to the primary network and an unreliable connection [7], [16], [17], [18], [19], [20], [21], among others.

Techniques such as detection filters, energy detection and detection of cyclo-static characteristics, try to provide the ability to distinguish between the primary user and the secondary user. In such a hostile environment, the definition of the primary user can be extremely difficult. In PUE, and attacker can modify its

interface so that it emulates the signal of a primary user, in this case, the secondary user observes that the signal that is generated is from a primary user and cannot transmit on this frequency, which causes a denial of service to said user due to the attack [22].

The attacker can falsify the data collected of the use of the spectrum in the learning process of the cognitive radio to determine which frequencies to try to access in the future, causing that some frequencies cannot be used and have total control over them [22]

The PUE attack affects not only the physical layer of the OSI model, it also affects the application layer [12] and all other layers [23], [24]. In the Figure 2 you can see the relationship of the PUE attack with the cognitive radio cycles [24], which are related to the layers of the OSI model:

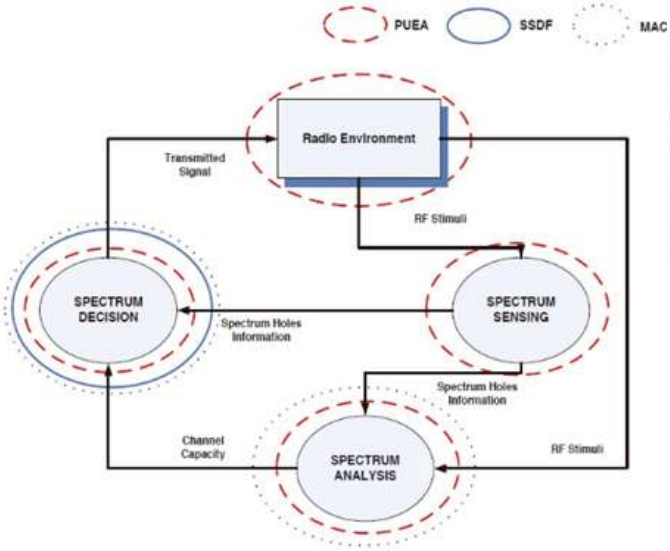

Figure 2 . Cognitive radio cycles [24]

- **PUE Example**

This figure shows the clear division between the primary mobile network, consisting of a base station and primary or licensed users connected to that station and the mobile cognitive radio network, which by definition has a cognitive base station and secondary users connected to it [21].
In the licensed band I, the network has the frequencies from f1 to f6 to distribute in its network. The frequencies f1, f3 and f4 are being used for the transmission of the primary user signals. Therefore, the frequencies f2, f5 and f6 are free. The mobile cognitive radio network detects that these frequencies are free and assigns them to SU1, SU2 and SU3. What the attacker EU2 does, by means of the primary user emulation, is to send the signal of f2, as the primary user, making communication between SU1 and SU3 impossible, disabling this frequency for its own use. For licensed band II, the attack frequencies do not impede the communication of SU4 and SU5, because they use other frequencies [21].

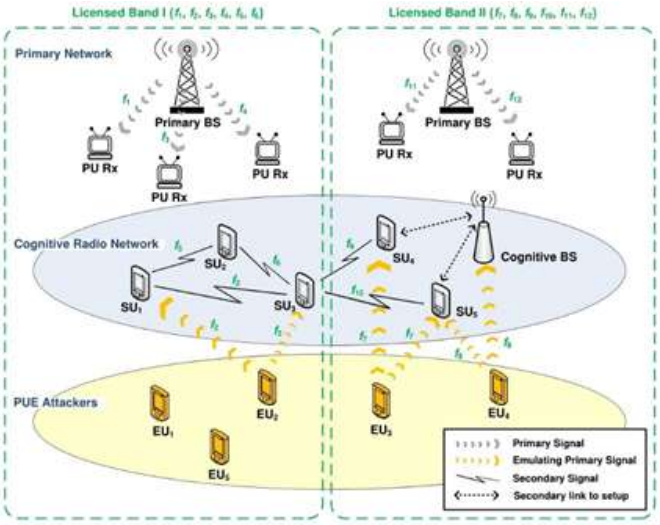

Figure 3. PUE Example [21]

- **PUE classification**

Based on the attacker's purpose, PUE attacks can be classified in [19]:

- **Malicious attack**

In PUE malicious attacks, an attacker prevents secondary users from detecting and accessing free frequency bands. The attacker does not use a band of spectrum for their own communication. The aim of the attacker is to reduce the use of the band of available spectrum [19].

- **Selfish attack**

The selfish PUE attack is performed by a selfish secondary user. In this attack, if a selfish user detects a band of free spectrum, it prevents other

secondary users from detecting the spectrum, with which the selfish user could gain full access to the spectrum. The aim of the attacker is to maximize his own use [19].

Based on the power level, an attacker can have fixed or variable power: a fixed-power attacker uses an invariable predefined power level regardless of the actual transmit power of the primary users and the surrounding radio environment. An attacker with adaptive power adjusts it's transmit power according to the estimated transmission power of the primary signal and channel parameters [22]. Based on the position, the attacker can be static or mobile: a static attacker has a fixed location that would not change during all rounds of attacks. A mobile attacker will constantly change its location, making it difficult to trace and discover [22].

In the following Table, classification is described from the point of view of purpose, power level, position [23]and general functionality.

Classification of the attacker	Category	Definition
Purpose	Selfish	The objective is to obtain bandwidth for your own transmissions.
	Malicious	Send signals in a free band or in a band occupied by a secondary user.
Power Level	Fixed	Fixed predefined power level, regardless of the actual power, the power units and the surrounding radio environment.
	Variable	It adjusts its power according to the estimated power of the primary signal and the parameters of the channel.
Position	Static	Fixed location
	Dynamic	Your position changes constantly, making it difficult to search or crawl.
General Functionality	Basic	It attacks with a fixed power level in a static position at any moment, even in the presence of a primary user.
	Smart	It attacks when there is no primary user, position can be static or dynamic and it can adapt the power level.

Table 1. PUE classification, adapted from **[23]**.

4. Primary user emulation detection

With regard to the work carried out for the detection of PUE, the author in – , classifies detection in the following categories:

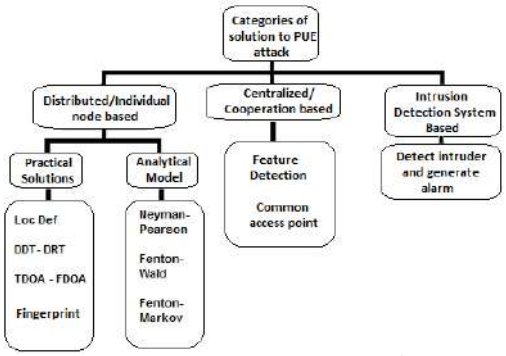

Figure 4. PUE Detection [25]

In the distributed / individual type based on nodes, the application of techniques in the individual user and how to protect a particular user from the attack is emphasized; in the centralized / cooperation based, the emphasis is on cooperation and communication with the central authority to discover unusual activities. In the distributed, the authority makes decisions with the individual user, while in the centralized scheme the decision making is with the central authority. The intrusion detection system identifies the attacking users in general and an activity may be the PUE attack [25] .

Detecting an attacker present is the first step in mitigating the PUE attack. This topic is part of the distributed cooperative sensing scheme and the detection of anomalies [4]. It is emphasized that in the literature, the terms detection, countermeasure, defense or mitigation are used to name these detection mechanisms. [1-28]. This investigation will clarify these terms. In the work of Rong Yu (2015)[21], clarity is made in the difference between detection and counterattack or defense. Although several detection techniques have been developed, none of the existing approaches can promise accurate detection of all PUE attacks, so system-level mechanisms are needed to maintain the overall performance of the network under PUE attacks undetected. The author proposes a cross-layer design for the defense of not detected PUE [21].

The author Fragkiadakis (2013) [24], makes an evaluation of some detection techniques developed, within the most important conclusions are that if the detection technique needs to alter the information, structure or protocol of the primary user, it does not meet the criteria of the FCC, as is the case of cryptography techniques. This author emphasizes that these techniques have been tested in simulator, but not implemented in development cards. The simulations were developed for an attacker with fixed location and fixed secondary users, in addition to having a fixed power so that detection can be carried out [24].
In Table 2, some of the techniques that have been worked out for the detection of primary user emulation in cognitive radio networks [25], [26] y [27] are described in Table 2.

	Solution	Protection Mechanism Suggested	Evaluation
Practical Solutions	Loc Def	Detects PUE attack based on RSS received signal strength) value	Applicable mostly in 802.22 networks not in ad-hoc networks
	Network User Management Center (NUMC)	Employs distance difference test (DDT) and the distance ratio test (DRT).	Applicable in the case where location of PU/ SU is static
	Time Difference of arrival (TDOA) and Frequency Difference of arrival (FDOA).	Employs Time Difference of arrival (TDOA) and Frequency Difference of arrival (FDOA) for location verification	Applicable in the case where location of PU/ SU is static
	Neyman-Pearson composite hypothesis test and Wald's sequential probability	Gives improvement in results by allowing user to specify thresholds for false alarms and probability of a miss	High probability of false alarm and adding Wald's sequential probability ratio test adds complexity to the solution.
Analytical Model	Fenton's approximation and Wald's sequential probability ratio test.	Independent of sensor information and employs Fenton's approximation and Wald's sequential probability ratio	Just an Analytical approach. Complexity high to make it applicable in especially ad-hoc networks.
	Fenton's approximation and Markov inequality.	Uses received power at a SU and use Fenton's approximation to determine the mean Determine lower bound on probability of PUE using Markov inequality	Just an Analytical approach and based on received power at the SU. Received power alone is not a perfect metric to make a decision regarding occurrence of an attack.

Analytical Model	Feature detection technique	Identify modulation type of a primary signal .Distinguish whether the signal is generated by primary user or by malicious secondary user	Identifies the PUE attack only does not provide any counter measure.
Centralized/ Cooperation Based	Centralized/ access point based scheme	All the nodes send their sensing data to an access point which makes the decision about presence or absence of primary user.	Not applicable in rapidly changing networks like VANET.
	Intrusion Detection System	Detects a usual happening and generates alarm to admin.	Time consuming and need continuous monitoring. Applicable MANET.
Intrusion Detection System Based	Transmitter fingerprinting	The phase noise of the noisy career is extracted and directly applied to identify the transmitter	Noise attenuation can seriously degrade its performance.

Table 2. PUE Detection Techniques [25], [26] y [27].

According to this table, the limitation of the different types of detection exposed is that they have been developed for an attacker with a fixed position and do not apply for all scenarios of a PUE attack, since it does not analyze the scenario with dynamic location [28], [15], [25] In addition, some of these techniques do not meet the criteria of the FCC[24].

5. Conclusions

One of the most important attack in mobile cognitive radio networks is the Primary user Emulation. This attack has been analyzed in the literature for a fixed Primary user and a fixed Primary User Attacker, but in a mobile network is not often that users are fixed. It's necessary to model this attack in a mobile environment, observing not just the physical layer, but the interactions in a cross-layer design.

6. Future work

A solution that has been proposed for the detection of PUE in the mobile cognitive radio network is the cross-layer design [11], [6], since it allows obtaining and sharing information between non-underlying layers of the network architecture, By optimizing security and mitigating the effects of attacks on the network [6], the model can be seen in the following Figure 5.

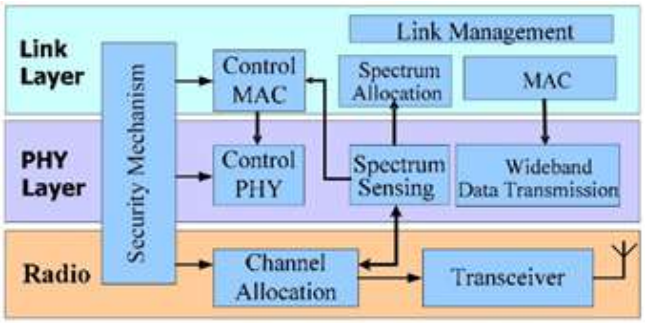

Figure 5. Cross-Layer Design for security in cognitive radio networks [6]

The authors Yu and Le [21], [12], state that the cross-layer design can be configured for the detection of PUE attacks. The behavior of the detected PUE attacks is observed in the physical layer and the upper layers are informed, such as the RRM mechanism in the MAC layer or the routing mechanism in the network layer. It is noted that even undetected PUE attacks could be estimated at the physical layer by considering the detection probability theoretically derived from the upper layer control parameters [21], [12].

The PUE detection techniques in mobile cognitive radio networks have the drawback that they have been designed with a secondary user whose location is fixed, known and a fixed attacker, therefore, the secondary user and attacker with dynamic location have not been addressed [28], [25], [15].

Acknowledgment

We express our gratitude to Colciencias and

Universidad Nacional de Colombia for the financiation of the Project.

References

[1] E. C. Muñoz, H. J. E. Blanco, and J. A. F. Calderón, "Gestión del espectro radioeléctrico en Colombia," Rev. Tecnura, vol. 19, no. 45, pp. 159–174, 2015. https://doi.org/10.14483/udistrital.jour.tecnura.2015.3.a12

[2] J. H. A. Rentería and A. N. Cadavid, "Cognitive radio–State of the Art," Sist. Telemática, vol. 9, no. 16, pp. 31–53, 2011. https://doi.org/10.18046/syt.v9i16.1028

[3] S. P. T. Force, "Spectrum policy task force report et docket no. 02-135," US Fed. Commun. Comm., 2002.

[4] L. F. Pedraza Martinez and others, "Modelo de propagación para un entorno urbano que identifica las oportunidades espectrales para redes móviles de radio cognitiva," Universidad Nacional de Colombia-Sede Bogotá.

[5] C. Hemández, L. Pedraza, I. Páez, and E. Rodriguez-Colina, "Análisis de la Movilidad Espectral en Redes de Radio Cognitiva," Inf. Tecnológica, vol. 26, no. 6, pp. 169–186, 2015. https://doi.org/10.4067/S0718-07642015000600018

[6] Y. Peng, F. Xiang, H. Long, and J. Peng, "The research of cross-layer architecture design and security for cognitive radio network," in Information Engineering and Electronic Commerce, 2009. IEEC'09. International Symposium on, 2009, pp. 603–607. https://doi.org/10.1109/IEEC.2009.133

[7] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," IEEE Commun. Surv. Tutor., vol. 14, no. 2, pp. 355–379, 2012. https://doi.org/10.1109/SURV.2011.032511.00097

[8] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on, 2008, pp. 1–8. https://doi.org/10.1109/CROWNCOM.2008.4562534

[9] J. Blesa Martínez, "Cognitive strategies for security in wireless sensor networks," Telecomunicacion, 2015.

[10] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," IEEE Commun. Surv. Tutor., vol. 17, no. 2, pp. 1023–1043, 2015. https://doi.org/10.1109/COMST.2014.2380998

[11] H. Wen, S. Li, X. Zhu, and L. Zhou, "A framework of the PHY-layer approach to defense against security threats in cognitive radio networks," IEEE Netw., vol. 27, no. 3, pp. 34–39, 2013. https://doi.org/10.1109/MNET.2013.6523806

[12] T. N. Le, W.-L. Chin, and W.-C. Kao, "Cross-layer design for primary user emulation attacks detection in mobile cognitive radio networks," IEEE Commun. Lett., vol. 19, no. 5, pp. 799–802, 2015. https://doi.org/10.1109/LCOMM.2015.2399920

[13] J. Mitola, "Software radios: Survey, critical evaluation and future directions," IEEE

. https://doi.org/10.1109/62.210638

[14] T. Le and C. Bostian, "General radio interface between cognitive algorithms and reconfigurable radio platforms," in [1] Software Defined Radio Forum Technical Conference, 2007.

[15] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," Proc. IEEE, vol. 100, no. 12, pp. 3172–3186, 2012. https://doi.org/10.1109/JPROC.2012.2208211

[16] S. Rizvi, J. Mitchell, and N. Showan, "Analysis of security vulnerabilities and threat assessment in Cognitive Radio (CR) networks," in Application of Information and Communication Technologies (AICT), 2014 IEEE 8th International Conference on, 2014, pp. 1–6. https://doi.org/10.1109/ICAICT.2014.7035911

[17] J. Sen, "A survey on security and privacy protocols for cognitive wireless sensor networks," ArXiv Prepr. ArXiv13080682, 2013.

[18] Ö. Cepheli and G. K. Kurt, "Physical layer security in cognitive radio networks: A beamforming approach," in Communications and Networking (BlackSeaCom), 2013 First International Black Sea Conference on, 2013, pp. 233–237. https://doi.org/10.1109/BlackSeaCom.2013.6623415

[19] K. K. Chauhan and A. K. S. Sanger, "Survey of Security threats and attacks in cognitive radio networks," in Electronics and Communication Systems (ICECS), 2014 International Conference on, 2014, pp. 1–5. https://doi.org/10.1109/ECS.2014.6892537

[20] L. Jianwu, F. Zebing, F. Zhiyong, and Z. Ping, "A survey of security issues in cognitive radio networks," China Commun., vol. 12, no. 3, pp. 132–150, 2015. https://doi.org/10.1109/CC.2015.7084371

[21] R. Yu, Y. Zhang, Y. Liu, S. Gjessing, and M. Guizani, "Securing Cognitive Radio Networks against Primary User Emulation Attacks," IEEE Netw., vol. 30, no. 6, pp. 62–69, 2016. https://doi.org/10.1109/MNET.2016.1200149NM

[22] M. Khasawneh and A. Agarwal, "A survey on security in Cognitive Radio networks," in Computer Science and Information Technology (CSIT), 2014 6th International Conference on, 2014, pp. 64–70. https://doi.org/10.1109/CSIT.2014.6805980

[23] P. K. Niranjane, V. M. Wadhai, S. H. Rajput, and J. B. Helonde, "Performance analysis of PUE attacker on Dynamic Spectrum access in cognitive radio," in Pervasive Computing (ICPC), 2015 International Conference on, 2015, pp. 1–6. https://doi.org/10.1109/PERVASIVE.2015.7086985

[24] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," IEEE Commun. Surv. Tutor., vol. 15, no. 1, pp. 428–445, 2013. https://doi.org/10.1109/SURV.2011.122211.00162

[25] B. Naqvi, I. Rashid, F. Riaz, and B. Aslam, "Primary user emulation attack and their

.mitigation strategies: A survey," in Information Assurance (NCIA), 2013 2nd National Conference on, 2013, pp. 95–100. https://doi.org/10.1109/NCIA.2013.6725331

[26] Y. Yu, L. Hu, H. Li, Y. Zhang, F. Wu, and J. Chu, "The Security of Physical Layer in Cognitive Radio Networks," J. Commun., vol. 9, no. 12, pp. 916–922, 2014. https://doi.org/10.12720/jcm.9.12.916-922

[27] J. Soto, S. Queiroz, and M. Nogueira, "Taxonomy, flexibility, and open issues on pue attack defenses in cognitive radio networks," IEEE Wirel. Commun., vol. 20, no. 6, pp. 59–65, 2013. https://doi.org/10.1109/MWC.2013.6704475

[28] M. Ghaznavi and A. Jamshidi, "Defence against Primary User Emulation Attack Using Statistical Properties of the Cognitive Radio Received Power," IET Commun., 2017. https://doi.org/10.1049/iet-com.2016.1248