UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica
Más que un estado sólido

https://doi.org/10.14483/issn.2248-4728

VISIÓN ELECTRÓNICA

A RESEARCH VISION

Primary user emulation characterization in mobile cognitive radio networks

Caracterización de emulación de usuario primario en redes móviles de radio cognitiva

Ernesto Cadena-Muñoz [1], ***Luis Fernando Pedraza-Martínez*** [2], ***Enrique Rodríguez-Colina*** [3]

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:
Enviado: 23/12/2019
Recibido: 17/02/2020
Aceptado: 19/04/2020

Keywords:
Mobile cognitive radio network
Primary user emulation
Security
Software defined radio
USRP

Palabras clave:
Redes móviles de radio cognitiva
Emulación de usuario primario
Seguridad
Radio definido por software
USRP

ABSTRACT

This paper presents the results of the characterization of the attack known as the "primary user emulationïn mobile cognitive radio networks performing the implementation and testing. The tools and their configuration to carry out the attack are presented and their effects on the network are analyzed. The results show how to generate the attack with a software-defined radio equipment (SDR) using GNU-Radio and OpenBTS. The effects of the possible configurations of the attack on the network are shown, the malicious type generates constant interference on the primary or cognitive network, the selfish type allows to imitate a licensed or primary user generating interference to the primary network and inability to access the Cognitive Network while active. If the emulator's power level is fixed, the services it provides are stable. If the power is variable the services suffer intermittency. Primary user emulation is the attack that most affects the cognitive radio network so its effects are analyzed in order to propose ways of detecting or applying countermeasures.

RESUMEN

En este artículo se presentan los resultados de la caracterización del ataque conocido como la "emulación de usuario primario" en redes móviles de radio cognitiva realizando la implementación y pruebas. Se presentan las herramientas y su configuración para efectuar el ataque y se analizan sus efectos sobre la red. Los resultados muestran cómo generar el ataque con un equipo de radio definido por software (SDR) utilizando GNU-Radio y OpenBTS. Se muestran los efectos de las posibles configuraciones del ataque sobre la red, el tipo malicioso genera interferencia constante sobre la red primaria o cognitiva, el tipo egoísta permite imitar un usuario licenciado o primario generando interferencia a la red primaria e imposibilidad de acceso a la red cognitiva mientras este activo. Si el nivel de potencia del emulador es fijo los servicios que presta son estables. Si la potencia es variable los servicios sufren intermitencia. La emulación de usuario primario es el ataque que más afecta la red de radio cognitiva por lo que se analizan sus efectos para poder plantear formas de detección o aplicar contramedidas.

[1] Ph.D. (c) in Systems and Computing Engineering, MSc. in Telecommunications, Universidad Nacional de Colombia, Colombia. BSc. in Telecommunications Engineering, Universidad Distrital Francisco José de Caldas, Colombia. E-mail: ecadenam@unal.edu.co

[2] Ph.D. in Systems and Computing Engineering, Universidad Nacional de Colombia, Colombia. MSc. in teleinformatics. BSc. in Electronic Engineering. Current position: Professor at Technological Faculty, Universidad Distrital Francisco José de Caldas, Colombia. E-mail: lfpedrazam@udistrital.edu.co

[3] Ph.D. in Engineering Telecommunications Area, University of Cambridge, Reino Unido. BSc. in Electronic Communications Engineer, UAM Iztapalapa, México. Professor at Electrical Engineering Department, Autonomous Metropolitan University, Iztapalapa, Mexico City, Mexico. E-mail: erod@xanum.uam.mx

Cite this article as: E. Cadena-Muñoz, L. F. Pedraza-Martínez and E. Rodríguez-Colina, "Primary user emulation characterization in mobile cognitive radio networks", Visión electrónica, vol. 14, no. 1, pp. 26-34, january 2020.
https://doi.org/10.14483/22484728.16351

1. Introduction

Recent studies have shown the underutilization of the radio spectrum and its scarcity in countries like Colombia [1]. For this reason, it is important to analyze technological alternatives that allow its optimization, for which strategies such as the implementation of Emerging Networks such as the Mobile Cognitive Radio Network that allow an improvement in the use of this valuable means of communication are proposed [2].

In general, an area of study that has a significant impact today is the security of the networks [3, 4], both from the point of view of the information transmitted by the user, and the security of the network against vulnerabilities external In this case, it is essential to start with a study of the possible attacks on the mobile cognitive radio network, its classification, behavior, the impact on the network or on the users who make use of it and subsequently generate detection or defense strategies [5].

Within the classification of attacks on the cognitive network, there are some that are common to all wireless networks [6], but there are some specific attacks on the mobile cognitive radio network. When reviewing the classification of attacks, it is found that one of the attacks that most affects the Network is the Primary User Emulation (PUE), since it can affect all cycles of the cognitive process and disable services to secondary users even affecting somehow the primary users [2, 7].

In the literature, it is found that the studies developed have been implemented on simulation software, but have not been tested in a real environment, the theoretical aspects of the attack are raised and simulations are carried out. The first objective of this work is through programmable devices such as SDR and GNURadio, implementing a mobile cognitive radio network and obtaining real evidence of its operation by providing services to mobile secondary users [7–9]. The second objective is to achieve the generation of the primary user emulation attack, to subsequently analyze its impact on the network and to be able to characterize all types of derived attacks. Having the knowledge of how the attack is generated and its characterization, the next step is to generate defense or detection strategies.

The following work carries out the characterization of the primary user emulation in mobile cognitive radio networks through the classification, implementation and testing of radio equipment defined by NI USRP-2922 software. Section 2 shows the used methodology. In section 3 the results of the experiments are analyzed and finally the conclusions are made.

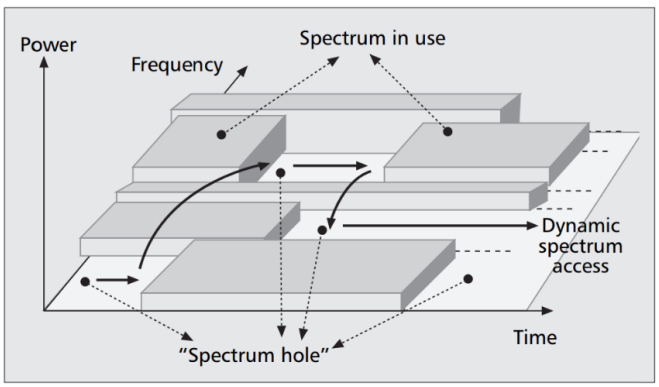
2. Methodology

In this section the fundamental theoretical concepts are presented, together with the assemblies made for the different hardware and software components of the mobile cognitive radio network and the primary user emulation attack, the tools, algorithms and the initial characterization of the attack.

2.1. *Mobile Cognitive Radio Network*

The mobile cognitive radio network is defined as a network created for the purpose of constantly monitoring, perceiving or detecting the frequencies of the primary user (PU), which pays for the license of the use of the radio spectrum and in the instants of time that it does not use it, provide its own secondary users (SU), a service that can be calls, messages or data in general [10]. In Figure **1**, the process can be observed, where the spectral holes are searched, that is, the time spaces where the frequency is not used, this is where the cognitive radio takes advantage of for its communication [11].

Figure 1: Spectral holes in Cognitive Radio. [11].



It is important to note that if a primary user is detected at some point in the communication, the cognitive network must be able to release the channel automatically so that there is no affectation to the primary user, so the system hops from frequency to frequency as soon as a frequency is released or used within the working band [10]. To achieve this goal, the cognitive radio team must have the ability to perform a spectral analysis, while carrying out its communication [11]. The 802.22 standard is defined as the first standard

that works with cognitive radio, for wireless networks, but focuses on fixed point-multipoint networks, such as television in 54MHz to 862 MHz bands [12]. In the case of the cognitive network, due to the characteristics of the SDR NI USRP-2922 equipment and according to the regulations and spectral assignment of Colombia, the experiment uses the 850MHz band of the cellular network.

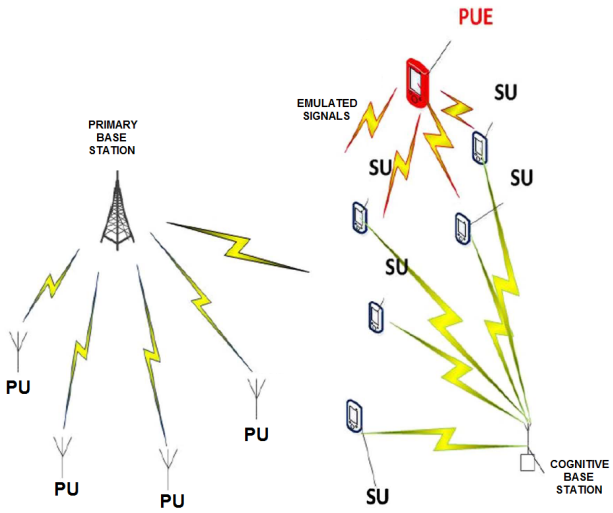
For this experiment, the SDR will be used as a cognitive base station for the mobile cognitive radio network, which is configured centrally as a mobile base station works. Two devices will be connected to this device to make a voice call. If the selected channel in the frequency band is not used by the primary user, the communication is made. However, if a PU or a PUE uses the communications channel, given the impossibility of recognizing the origin, it must make a hop to another free available frequency. In case frequencies are not available for communication, it will be suspended until the channel is released.

2.2. *Primary User Emulation Attack*

The Primary User Emulation (PUE), is defined as one of the greatest vulnerabilities of the cognitive network, since the fundamental objective is to imitate in the best way the properties and characteristics of a primary or licensed user and due to the architecture of cognitive radio, it must release the channel by recognizing the attacker as a primary user [13]. Figure **2** shows the general form of the experiment, where the frequencies of the primary base station are explored directly in the cognitive base station, from here the available frequencies are distributed or the channels are released, it can be seen that the PUE directly affects the SU through the detection made by the cognitive base station.

As can be seen for cognitive radio, the use of their frequencies must be transparent to the primary network, the objective is that the communications of their primary users are not altered. On the other hand, the PUE generates an emulation of the primary signal, with the main objective of release the channel for its own objectives [14]. These objectives can be two according to the literature; Selfish: It refers to attacking the cognitive network, so that it releases a frequency band and use it for its own benefit, that is, to meet service requests of its SUs; Malicious: It refers to the fact that it does not want to transmit data, it does not attend SU services, it only interferes the system so that the cognitive network cannot use a frequency range [5, 14].

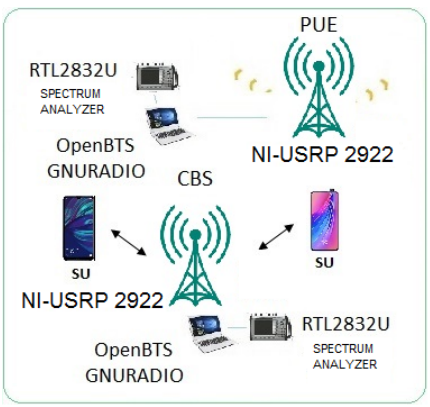
Figure 2: PUE General Structure. [14].



The primary user emulation attack for the experiments will be generated through an NI USRP-2922, which will function as a centralized PUE, due to the capabilities of the cell phones used. Two PUEs will be connected through the centralized to make calls in selfish mode, for the malicious mode radio frequency signals similar to a PU are sent, but a service is not provided, only the channel is occupied.

In Figure **3** the scheme used for the experiment can be seen, the used software is OpenBTS and GNU-Radio on Linux, together with the spectrum analyzer controllers. In hardware we use two RTL2832U, which serve as spectrum analyzer and two NI-USRP2922, for the cognitive base station and the generation of the PUE.

Figure 3: Testbed for experiments.



Source: own

The experiments are initially divided into generating and verifying the impact of the PUE attack on the mobile cognitive radio network with the selfish mode and the ambitious mode. First, OpenBTS is installed with the cognitive protocol, so that it can perform permanent spectrum detection and channel assignment to communicate to SUs. The PUE is also configured to launch the attack only in the absence of a PU and it is verified what happen if I change the signal strength over time. Measurements are also made on the channel when the SUs connected to the cognitive station are in movement.

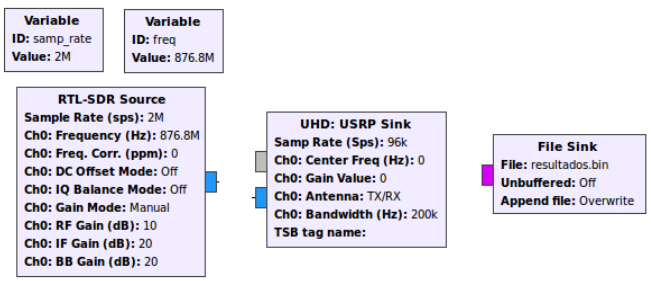
3. Results

This section will illustrate the used architecture, software, hardware, the experiments and the obtained results.

3.1. *Software*

In GNU Radio, the main components of RTL-SDR and UHD are used to configure the spectrum analyzer and cognitive radio equipment, a Python file is generated that can be modified to perform frequency reading, assignment and frequency hop of cognitive radio, as well as recording the results in a file resultados.bin". These components of GNU Radio can be seen in Figure 4.

Figure 4: Main GNURadio Components.



Source: own

In both the cognitive radio base station and the attacker, the OpenBTS software components are installed, which allow GSM communication for calls or messages between cell phones that are correctly authenticated in the network [15].

3.2. *Hardware*

For physical implementation, an NI-USRP 2922 was used to generate the PUE and another for the cognitive base station. To carry out the tests with the fixed PUE, the direct connection of the antenna is made. For the dynamic PUE, the antenna is adapted to a drone that allows its mobility, that is, the antenna is moved and not the complete equipment, because this would include moving the computer equipment and the USRP. Figure 5 shows the fixed and dynamic location hardware for PUE.

Figure 5: USRP for fixed and dynamic location PUE.

Source: own

For the experiment, the location element can be fixed or mobile and in addition the cellular equipment of both the SU and the PUE can also be fixed or moving. The objective is to observe the behavior of the calls made between the two cell phones when the PUE and the same cell phones are fixed and moving. The tests are carried out in an indoor environment with elements such as walls, desks, chairs, among others, the distance is 5 meters between the components of the cognitive base station and the PUE.

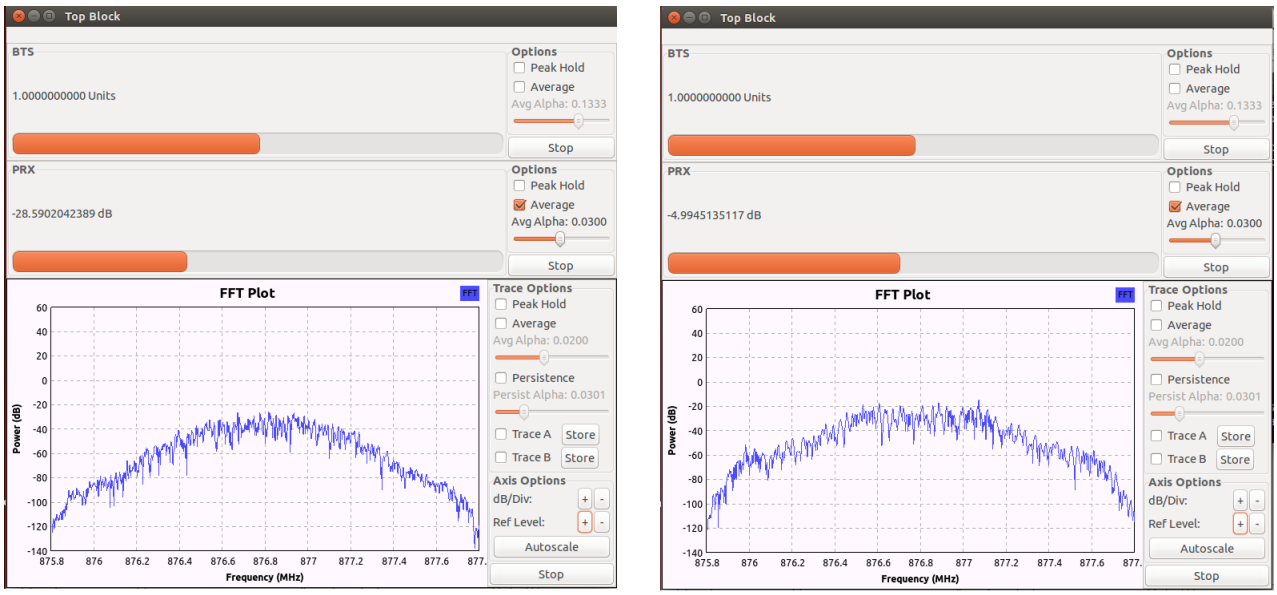
3.3. *Characterization*

The characterization of the PUE attack is then carried out based on laboratory tests.

3.3.1. *PUE with fixed location*

In the PUE with fixed location the devices are placed in a random position, a call between two cell phones is activated in the cognitive base station and the activation of the PUE is carried out in malicious mode. In this mode we are at the same frequency that the cognitive base station is using and we carry out a test communication. In Figure 6 we can see the behavior when there is only the cognitive base station and when the PUE appears. If they are at the same frequency, a higher power can be seen, but at the level of connectivity as soon as the PUE is activated, the cognitive base station changes the channel or terminates the connection if there are no channels available. In this mode, the PUE does not provide service to its equipment, it is only interfering.

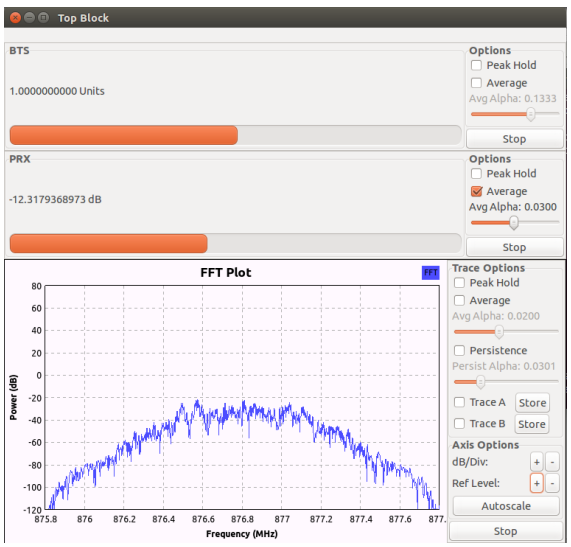
Figure 6: MCRN with and without malicious PUE.



Source: own

In selfish mode, the PUE is configured to use a specific frequency and its users are connected, a communication is made. The results show that as soon as the PUE is activated the MCRN release the channel, and if it was not occupying it, it can no longer be used. The active selfish PUE signal can be seen in Figure 7.

Figure 7: Selfish PUE.



Source: own

The theory shows that if a double potential decision threshold can be found to separate the PU from the PUE, this point could be found, but this assumes that the signal of the PU is larger than that of the PUE, this can be seen in (1), where $y(t)$ is the signal received at the cognitive base station [16].

$$y(t) = \begin{cases} n(t) & \text{SU} \\ h(t) * s(t) + n(t) & \text{PU} \\ h(t) * s'(t) + n(t) & \text{PUE} \end{cases} \quad (1)$$

Then $n(t)$ is assumed as a noise signal, $h(t)$ as the impulse response, $s(t)$ as the signal received from a PU and $s'(t)$ as the imitated PUE attack signal.

The results show that measuring this difference between the two levels even though PUE is fixed is not possible, they may have similar power levels. For this reason, the PUE in this case is established as shown in (2).

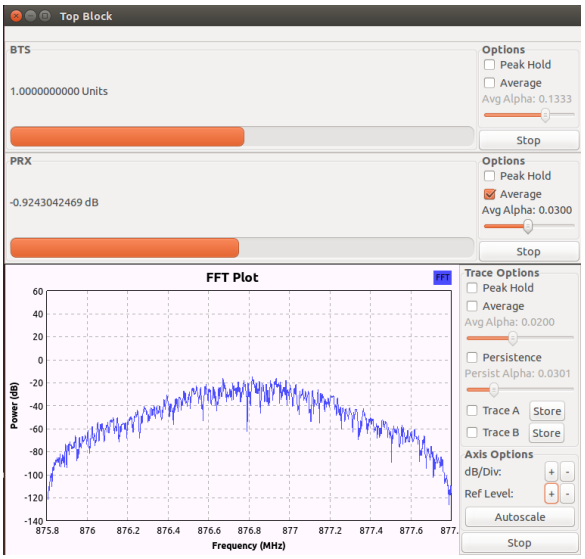
$$y(t) = \begin{cases} n(t) & \text{SU} \\ h(t) * s(t) + n(t) & \text{PU / PUE} \end{cases} \quad (2)$$

3.3.2. *PUE with dynamic location*

In the PUE with dynamic location, the devices are placed in a position and moved randomly, a call is activated between two cell phones at the cognitive base station and the activation of the PUE is carried out in malicious mode. In this mode we are at the same frequency that the cognitive base station is using and we carry out a test communication. In Figure 8 we can see the behavior when there is only the cognitive base station

and when the PUE appears. In this case, even if it moves the behavior is the same over time, it makes a constant interference, which causes the cognitive base station to frequency hop or terminate the communication.

Figure 8: Malicious PUE with dynamic location.



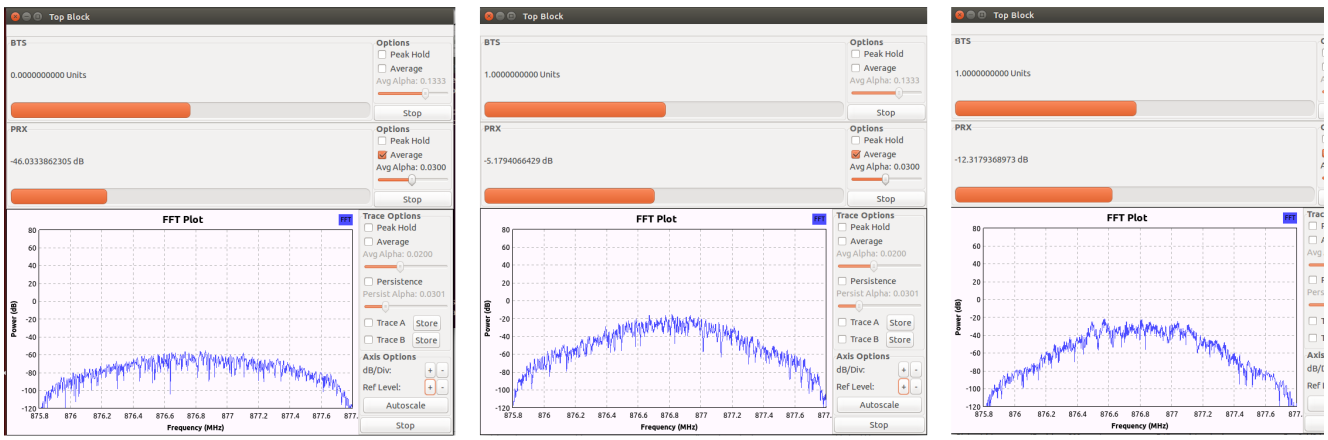
Source: own

In the selfish PUE with dynamic location, the PUE is configured to use a specific frequency and its users are connected, a communication is made. The results show a similar behavior of the fixed PUE, with the difference that the power levels vary over time, depending on the threshold chosen in the cognitive base station deactivates the communication, it cannot identify whether it is a PU or a PUE. The measured signal of selfish dynamic PUE without signal, with a position close to the cognitive base station and with a position five meters away can be seen in Figure 9.

3.3.3. *PUE with variable power*

For this experiment, selfish and malicious modes with fixed PUE are performed. For the malicious mode it is possible to generate variable powers every 5 seconds, which can confuse energy-based detection systems, their reception level varies between -80dBm and -40dBm. In the selfish mode it is not possible to carry out the experiment, since when we have a service connected, the power of the service cannot be varied, the call would have to be disconnected and restarted again, so it is concluded that the utility of the PUE with variable power is in a malicious environment, but not selfish.

Figure 9: Selfish dynamic location PUE measured signal without PUE, near cognitive network and five meters away.



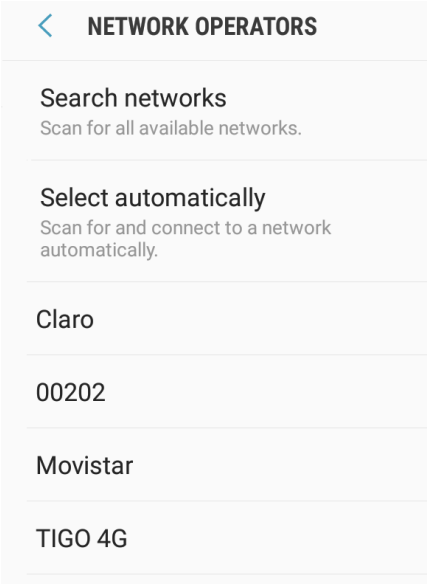
Source: own

3.3.4. *SU Affectation*

The first thing we notice when performing the experiments, whether fixed or dynamic, selfish or malicious, is that the SU will search for the mobile cognitive radio network, so a list of possible networks will appear, as can be seen in Figure 10.

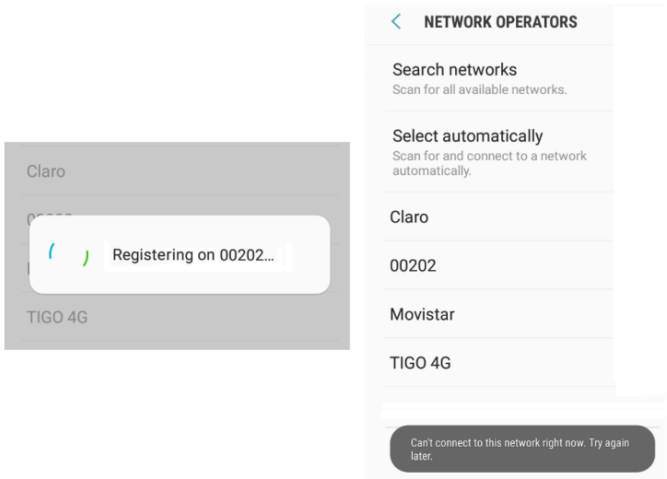
Several options appear, that the PUE has the same name and characteristics as the main network, in our case 02002 or that has different names and that are in the same frequency of use. The results show that if they have the same name even if it goes on different frequencies cause that the user does not know which one to connect to, it can even try to authenticate, but the process will result in error, as can be seen in Figure 11.

Figure 10: Malicious PUE with dynamic location.



Source: own

Figure 11: Malicious PUE with dynamic location.



Source: own

In conclusion, if the name of the network is the same, it will not let the SU connect to the network, even if it is registered for authentication. On the other hand, if there is a call from the SU, it will be disconnected when the PUE is activated.

The fixed or dynamic PUE has the same changes for the SU, since it starts in the network name, the connection frequency and the results within the coverage range of the cognitive base station are the same, even if the SUs are mobilized in the same range the results are the same, for these experiments the mobility of the SU or the same PUE have the same impact on the network. However, in the detection systems the impact of this behavior is high, since it modifies the estimation parameters of the detection systems and even with the movement, leaving some systems unusable. As the objective is the mobile cognitive radio network, the dynamic PUE is more viable.

3.3.5. Types of PUE

According to the results of the experiments, we can conclude the types of PUE, as can be seen in Table 1.

4. Conclusions

Through the use of software-defined radio devices it is possible to generate attacks on the mobile cognitive radio network that include the alteration of the detection data and the emulation of the signals coming from a primary network.

The PUE can have characteristics and information similar to the primary network, if the target is a malicious attack, it can affect the SU and also the PU. If the objective is a selfish attack, it will only affect the SU of the mobile cognitive radio network.

If the PUE imitates the name of the real primary network or even that of the cognitive network, it causes authentication and connection problems to the SUs and the PUs

The power of the PUE must be fixed if the objective is selfish, provide services to its own users. In the case of variable power, it can be used in malicious attack making it difficult to detect.

When using an energy detector, the mobile cognitive radio network is able to make the frequency hopping to not affect the PU, detection systems must be improved to be able to separate the signal from the PU and the PUE.

Acknowledgments

The authors are grateful to Colciencias for the financing of the project through conv. 757 of 2016. Thanks are given to the Universidad Nacional de Colombia, Universidad Distrital Francisco José de Caldas and to the Universidad Autónoma Metropolitana Unidad Iztapalapa, México.

Table 1: Types of PUE.

Types of PUE	Definition	Impact on MCRN
MALICIOUS	This attack does not seek to provide its own services, it only seeks to make interference in the selected frequency bands.	It causes constant interference in the working bands for the SU or even the PU.
SELFISH	This attack seeks to appropriate the selected frequency band to transmit its own information.	By mimicking the signal of the PU, it makes the cognitive network release the work frequency and provides communication to its own users, this does not affect the PU.
FIXED	It is located in a specific position, in a range where you can provide your services.	The location does not influence the result of the PUE, but it does affect the detection system.
DYNAMIC	Its location is variable by necessity or for trying to skip the detection systems.	On the move, the characteristics of the mobile PUE are equal to the fixed PUE, since the detection systems are cheated by dynamic.
FIXED POWER	Signal strength does not vary over time.	It is used in the selfish or malicious PUE, it causes disconnection.
VARIABLE POWER	Signal strength varies over time.	It is used in malicious PUE, it causes disconnection. In the selfish does not allow continuous connection to users.

Source: own

References

[1] L. F. Pedraza, F. Forero, and I. P. Paez, "Evaluación de ocupación del espectro radioeléctrico en Bogotá-Colombia", *Ing. Cienc.*, vol. 10, no. 19, pp. 127–143, 2014. https://doi.org/10.17230/ingciencia.10.19.6

[2] M. Karimi and S. M. S. Sadough, "Efficient Transmission Strategy for Cognitive Radio Systems Under Primary User Emulation Attack", *IEEE Syst. J.*, 2017. https://doi.org/10.1109/JSYST.2017.2747594

[3] 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

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

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

[6] 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

[7] M. Ghaznavi and A. Jamshidi, "Defence against Primary User Emulation Attack Using Statistical Properties of the Cognitive Radio Received Power", *IET Commun.*, vol. 11, no. 9, 2017. https://doi.org/10.1049/iet-com.2016.1248

[8] J. Avila, S. Prem, S. Rajapradeepa, and K. Thenmozhi, "Authentication Based Primary User Emulation Attack Mitigation in Cognitive Radio", in International Conference on Computer Communication and Informatics (ICCCI), 2018. https://doi.org/10.1109/ICCCI.2018.8441397

[9] W. F. Fihri, H. El Ghazi, N. Kaabouch, and B. A. El Majd, "Bayesian decision model with trilateration for primary user emulation attack localization in cognitive radio networks", in International Symposium on Networks, Computers and Communications (ISNCC), 2017. https://doi.org/10.1109/ISNCC.2017.8071979

[10] Y. Li, C. Han, M. Wang, H. Chen, and L. Xie, "A primary user emulation attack detection scheme in cognitive radio network with mobile secondary user", in 2nd IEEE International Conference on Computer and Communications (ICCC), 2016. https://doi.org/10.1109/CompComm.2016.7924870

[11] C. A. H. Suárez, L. F. P. Martínez, and F. H. M. Sarmiento, "Algoritmos para asignación de espectro en redes de radio cognitiva", *Tecnura*, vol. 20, no. 48, pp. 69–88, 2016. https://doi.org/10.14483/udistrital.jour.tecnura.2016.2.a05

[12] C. R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard", *IEEE Commun. Mag.,* vol. 47, no. 1, pp. 130–138, 2009. https://doi.org/10.1109/MCOM.2009.4752688

[13] S. M. Elghamrawy, "Security in cognitive radio network: defense against primary user emulation attacks using genetic artificial bee colony (GABC) algorithm", *Future Gener. Comput. Syst.*, 2018. https://doi.org/10.1016/j.future.2018.08.022

[14] S. Shrivastava, A. Rajesh, and P. Bora, "Defense against primary user emulation attacks from the secondary user throughput perspective," *AEU-Int. J. Electron. Commun.*, vol. 84, pp. 131–143, 2018. https://doi.org/10.1016/j.aeue.2017.11.012

[15] M. Iedema, "Getting Started with OpenBTS: Build Open Source Mobile Networks", O'Reilly Media, Inc., 2014.

[16] F. Jin, V. Varadharajan, and U. Tupakula, "Improved detection of primary user emulation attacks in cognitive radio networks", in International Telecommunication Networks and Applications Conference (ITNAC), 2015. https://doi.org/10.1109/ATNAC.2015.7366825