Cadena Muñoz *et al. EURASIP Journal on Wireless Communications and Networking* (2020) 2020:53
https://doi.org/10.1186/s13638-020-1657-0

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Detection of dynamic location primary user emulation on mobile cognitive radio networks using USRP

Ernesto Cadena Muñoz[1*], Enrique Rodriguez-Colina[2], Luis Fernando Pedraza[3] and Ingrid Patricia Paez[4]

Abstract

The study and the detection of possible network attacks are essential for wireless networks, in particular for mobile cognitive radio networks due to its characteristics such as the dynamic spectrum allocation and constant frequency hopping. The primary user emulation attack is one of the most significant attacks in cognitive radio, because it hazards the complete cognitive cycle. The techniques used for the detection of primary user emulation found in the literature are based on a fixed attacker location. However, in a mobile environment, the attacker usually has dynamic locations and this compromises the current applied security techniques and generates inefficient attack detection. Therefore, our work proposes a novel technique using cross-layer design for the detection of primary user emulation with mobility. This attack detection technique was tested with experiments using software-defined radio equipment and mobile phones at indoor scenarios with dynamic locations and with a mobile phone base station built up also with software-defined radio. The obtained results show that the combination of the three utilized techniques, energy detection, motion estimation, and application information analysis, are able to optimize the detection with around 100% of effectiveness for the primary user emulation attack with dynamic location. The proposed technique shows that the energy detection time is around 100 ms and for the processing time of the information analysis in the mobile phone is about 30 s. This result shows a practical and effective approach to detect primary emulation attacks. The proposed technique, to the best of the authors' knowledge, has not been presented before in the literature with experiments neither with mobility conditions of the attacker as presented in our proposed work.

Keywords: Primary user emulation, Cognitive radio network, PUE attack, Cross-layer design, Wireless networks security

1 Introduction

The cognitive radio networks (CRN) use software-defined radio (SDR) as a tool to find free spaces in the frequency spectrum assigned to a licensed primary user (PU) and also to transmit as an unlicensed secondary user (SU) [1]. Research found in the literature have shown that primary frequencies are not efficiently used especially in mobile networks [2–4], showing the relevance of CRN implementation to optimize spectrum utilization thinking on Internet of Things (IoT) applications. The CRN transmission equipment must have the ability to sense the frequency spectrum in real time to detect the presence of primary users using specific frequencies and move to another one, in order to avoid interference with the licensed primary user [5].

The CRN security has been studied and there are new specific attacks to the network, but still there are open issues to be solved in this field [6]. The exclusive attack called primary user emulation (PUE) is one of the most relevant attacks to analyze because it can completely disable the network; it is produced when an attacker mimics the PU signal. As the CR senses the spectrum all the time, the PUE signal is fraudulently detected as a primary user, and the secondary user must release the channel [7].

Several authors have studied how to detect PUE attack in CRN, but just a few have made it specifically in a mobile cognitive radio network (MCRN) [8, 9]. In general,

* Correspondence: ecadenam@unal.edu.co
[1]Systems and Industrial Department, College of Engineering, Universidad Nacional de Colombia, Bogota, Colombia
Full list of author information is available at the end of the article

the detection to hop to another frequency as soon as possible to avoid interference is made by methods such as energy detection [10], localization [11], and among others as shown in Section 3; however, with dynamic location scenario, these traditional methods will increase the false alarm results.

Research found in the literature, for example, in [8, 12, 13], shows the use of the cross-layer design for detection optimization of the PUE attack, but this is not validated with a practical implementation, especially in a MCRN.

The present work is organized as follows: Section 2 presents the methods used for experiments. The related work is presented in Section 3. In Section 4, the proposed detection system is described. In Section 5, results and discussions are shown. The contributions are presented in Section 6 and the conclusions in Section 7.

2 Methods

2.1 Primary user emulation attack

The PUEA in this work is generated by a software-defined radio (SDR): universal software radio peripheral (USRP-N210), and there are two proposed scenarios. The first scenario is quite basic, there is no need to measure the spectrum, because it always transmits the signals without any purpose, its location is static and its power is fixed. The other scenario is the smart attack; it transmits when there is no PU present. Its location is dynamic and its power can be fixed or variable. We used a fixed power in the experiments because the connection present fails when the power is variable and the location is dynamic. The experiments focus on selfish attack, because the malicious can be seen as a jammer [14, 15]. A USRP is used for the PUE network due to the sensing and transmission capabilities. In the experiment, a primary base station (PBS) emulation is used for the connection of two PUEs. The purpose of the experiment is to create and detect this centralized PUE at indoor environment with walls and furniture among other obstacles.

2.2 Mobile cognitive radio network

The purpose of the MCRN is to provide services in an independent network without a license, and these services can be phone calls, SMS, or data. The cognitive base station (CBS) senses the environment in a specific frequency range using the spectrum analyzer RTL2832U; if a PU in a primary base station (PBS) is not using its assigned frequency, the CBS use it to communicate with a SU. Even though it is a centralized model with the CBS, the system could be modified as distributed and cooperative environment to improve performance [12].

As mentioned before, the MCRN is implemented in a USRP-N210, with a full operative GSM PBS, the software used is OpenBTS [16, 17]. The CBS allows mobile phone calls and to interchange SMS between two phones. The architecture of the OpenBTS can be seen in Fig. 1 and comprises an “asterisk” server to control the voice, a “SMS queue” to control the short message services (SMS), and a “SIPauthserve” to control the users to be connected to the network. The PUE and CBS use GNU radio to change the OpenBTS parameters and to implement the cognitive protocol.

Another USRP-N210 with OpenBTS is used as a PBS-GSM to probe all operational parameters copying the public parameters from standard mobile operator in Colombia. The test bed used consists in the implementation of the PBS, PUE, and CBS with PU and SU as can be seen in Fig. 2.

Additionally, a cognitive radio network protocol was designed and implemented to switch the CR device frequency depending on the PU or PUEA detection based on [18], and this will be explained in Section 4.

3 Related work

In this section, PUEA, cross-layer design, and IoT security-related works are defined.

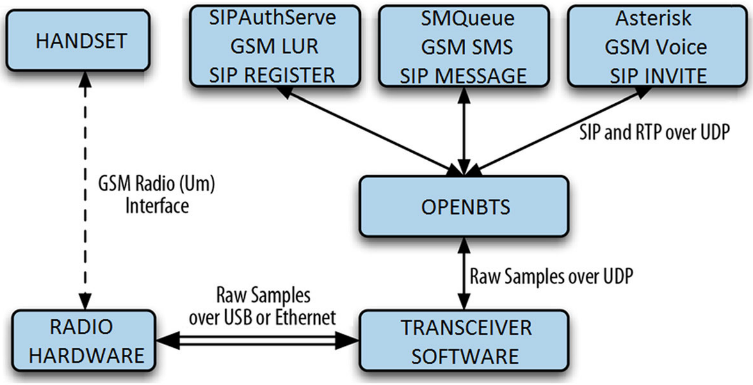


Fig. 1 Open BTS architecture [16]

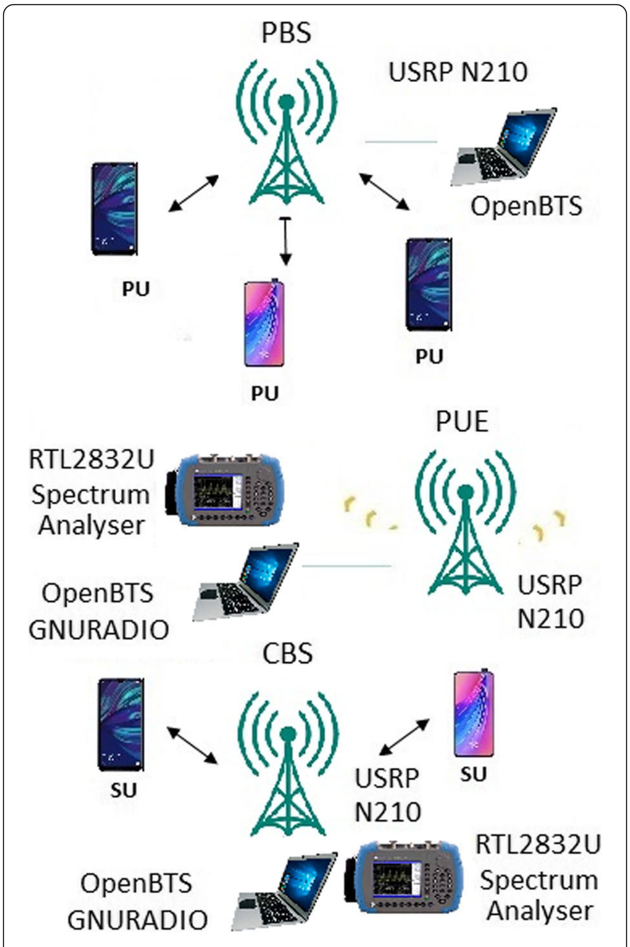


Fig. 2 Proposed test bed

3.1 Primary user emulation attack

In the primary user emulation attack (PUEA), the radio transmission system mimics the primary signal, causing the attacker to be fraudulently identified as a primary user, assigning itself the available frequency. Thus, PUEA on the network causes bandwidth waste, quality of service (QoS) degradation, denial of service (DoS), interference to the primary network, and unreliable connections [6, 19–24], among others, affecting all the cognitive cycle [25], causing a negative impact on the system performance.

Techniques such as energy detection [10], cyclostationary characteristic analysis [26], localization [11], online learning [27], particle swarm optimization [5], and authentication [28] try to provide the ability to distinguish between the primary user and the attacker [29]. However, these techniques were designed for a fixed location attacker, and in most of these techniques with changes on the attacker's location, the system is confused and the probability of the right detection will decrease significantly [29]. The other problem observed is that a number of techniques propose to alter the PU operation, but in principle, the MCRN should not interfere with the PU behavior.

The PUEA classification is described in Table 1, considering the attack purpose, power level, position, and general functionality [22, 29, 30].

3.2 Cross-layer design

Examples of solutions that have been proposed for the detection of PUE in mobile cognitive radio networks consist in the cross-layer design [12, 13], since it facilitates to obtain and share information between non-underlying layers of the network architecture, to optimize security and to mitigate the effects of attacks on the network [12]. The proposed cross-layer design uses information collected from radio, PHY, link, and app layers through a security mechanism, and it is illustrated in Fig. 3.

The authors in [8, 24] pointed out 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 radio resource management (RRM) mechanism in the MAC layer or the routing mechanism in the network layer [8, 24]. Based on this, a

Table 1 PUE classification, adapted from [22, 29, 30]

Classification of the attacker	Category	Definition
Purpose	Selfish	The objective is to use the PU assigned frequency for transmission; it senses the medium to know when there is no PU.
	Malicious	The objective is to interfere the PU frequency; it sends noise signals in a specific frequency.
Power level	Fixed	Constant 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 PU.
Position	Static	The location does not change in time.
	Dynamic	The position changes constantly, making it difficult to search or crawl.
General functionality	Basic	It attacks with a fixed power level at static position at any moment, even in the presence of a primary user.
	Smart	It attacks when there is no PU, position can be static or dynamic, and it can adapt the power level.

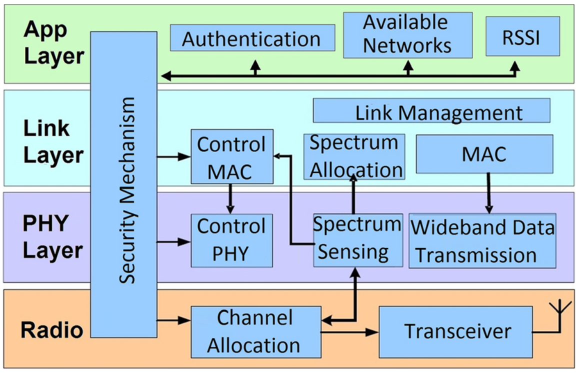


Fig. 3 Proposed cross-layer design for security in cognitive radio networks, adapted from [12]

cross-layer design was implemented in the proposed CBS, in order to use the energy detection of the physical layer, the received signal strength indicator (RSSI), and the authentication information of upper layers, as seen in Fig. 3. This is in order to detect the PUEA in the tested scenarios.

3.3 MCRN and Internet of Things (IoT) security

MCRN infrastructure supports mobile cloud computing implementation and integration with IoT [31, 32]. It is relevant to understand the security issues which refer to policies, technologies, and controls to protect data, applications, and the associated infrastructure [33] including the PUEA [34]. User that adopts this technology should know that all the company's sensitive information would be released to a third-party cloud service provider which is taken as a great risk [35]. On the other hand, as it could be implemented on a MCRN, it is sensitive to PUEA and in works as [36] systems were developed to detect PUEA in IoT, and as a future work, they planned the analysis of the users' mobility which is incorporated in our proposal.

For example, in security of IoT-based healthcare, smart building, or big data, the system needs to have scalability, reliability, adaptability, fault tolerance, and interoperability [37–39], and in case that a PUEA is successful, MCRN will not have anyone of these. A number of authors propose the use of cryptographic techniques [40], but as usual, the PU protocol cannot be changed by SU, and we proposed not to alter the PU operation.

4 Proposed detection system

In this section, the three used detection systems are defined, specifying the algorithms, flowcharts, and equations utilized. Therefore, the energy detection uses the PHY layer information, and the motion detection uses the RSSI and SNR given by APP and the MAC layer.

4.1 Cross-layer design

There are two main test scenarios, the basic and the smart, and to find an optimal solution for both of them, the detection uses an energy detector, motion detection based on trilateration and information from the mobile phone apps.

4.1.1 Energy detection

Most of the authors, such as [9, 41], assume that the PU has high signal power (in the order of kW), considering, for example, TV transmission towers and where the PU or PUE have low power compared with the transmission of the PBS. Hence, the energy detection model tries then to find the optimal threshold to the CRN to distinguish between PU, SU, and PUEA [9]. In mobile networks, BTS is limited to power units in the order of watts (W), and the PU is in order of milliwatts (mW) as well as the PUE's power, but it can be adapted to watts (W) with the use of a power amplifier. In this environment, energy detection cannot identify between PU and PUE but detects a user in the same frequency if it is above the threshold, as illustrated in Fig. 4.

The mathematical definition of PUE considers $n(t)$ as the noise signal, $h(t)$ as the impulse response of the system, $s(t)$ as the received signal from a PU, $s'(t)$ as the mimic signal from the PUEA, and $y(t)$ as the received signal [42], as shown in Eq. 1.

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

In common implementations of MCRN, the location of the PBS and CBS is fixed and the PUEA can be close to the PBS imitating the same power level, or, in fact, depending on the position, the power of the PUEA signal could be higher than the PBS. If a binary hypothesis test is used under the aforementioned conditions, a fixed threshold cannot be identified because it depends on the position of the PBS, PUEA, and CBS. In other words, the CRN can detect a received signal level, but it cannot identify if it is from the PBS or PUEA. In this research, a signal energy detection is used to distinguish between noise and the signal of the PBS or PUEA, allowing the CRN algorithm to change its frequency in case that it is necessary.

4.1.2 Motion detection

Traditional PUEA analysis does not take into account when the PUEA position changes dynamically. From a practical approach, the energy detectors fail when the PUEA is moving. Based on [5, 11, 43], a least square system using RSSI is used. The idea is to install three

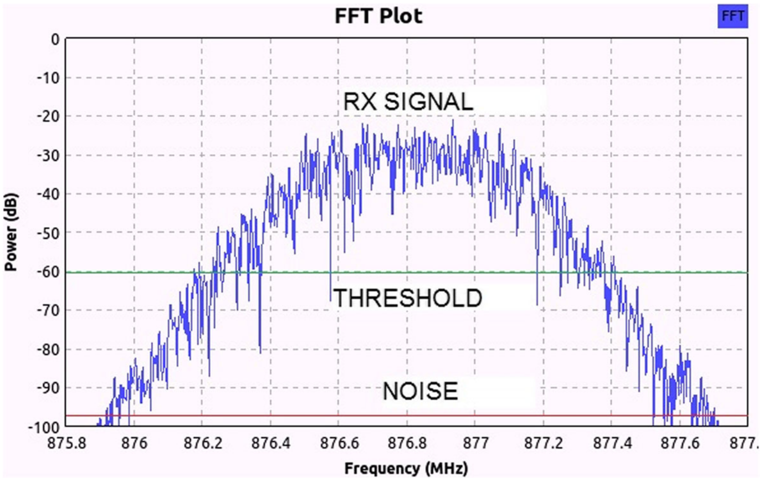


Fig. 4 Energy detection threshold for PU or PUE

sensors to read the RSSI indicator of PUE and estimate its position. Three phones utilized as sensors on the CBS and PBS transmission range are used to read RSSI values. These values have a little variation in time; if the PUEA is fixed, Kalman's filter approach can be used to decrease the error, but with a dynamic location PUEA, this cannot be achieved. The detection system reads the RSSI values in real time and calculates the average with minimum error.

The free space model is commonly used as propagation model, the received signal for model is given by Eq. 2 [43]

$$P_r(d) = \frac{P_t \times G_t \times G_r \times \lambda^2}{(4 \times \pi \times d)^2} \tag{2}$$

where P_r represents the received power, P_t is the transmission power of sender, G_t is the gain of the transmitter, G_r the gain of receiver, and λ the wavelength. The detection system is using the RSSI information given by Eq. 3 [43]

$$\mathrm{RSSI} = -10 \times n \times \mathrm{Log}_{10}(d) + A \tag{3}$$

where n is the propagation path loss exponent, d represents the distance from the sender, and A is the received signal strength in decibels at 1 m of distance from the sender [43].

The used experiment is shown in Fig. 5. The three sensors (mobile phones S1, S2, and S3) were used to read the RSSI from PUE; this information is averaged and transmitted to the CBS.

Based on the RSSI information, the algorithm establishes the current position of the PUE using the least square method. The actual position is calculated in real time and it detects changes in the PUEA position. Thus, the detection of the motion indicates that it is a PUEA due to the PBS is fixed.

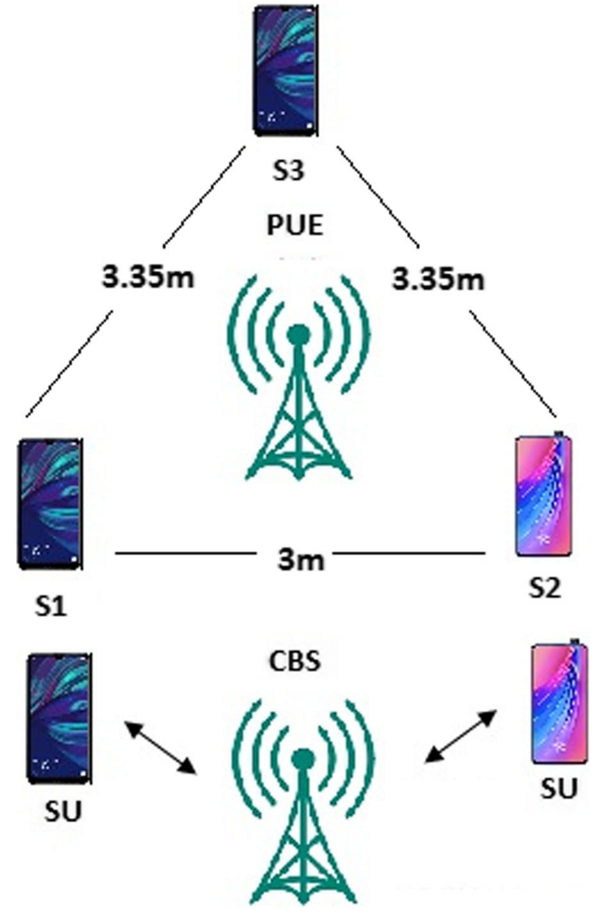


Fig. 5 Proposed motion detection system

The relative positions of the sensors, meaning mobile phones, are known S_1 (x_1, y_1), S_2 (x_2, y_2)… S_n (x_n, y_n), and a blind PUE node is in K (x, y); the distance from S1 to S2 is 3 m, from S1 to S3 is 3.35 m, and from S2 to S3 is 3.35 m, as shown in Fig. 5. Using the least square algorithm, the position can be estimated from the position of the sensors. The distance equations are shown in Eq. 4 [34].

$$\begin{cases} (x_1-x)^2+(y_1-y)^2=d_1{}^2 \\ (x_2-x)^2+(y_2-y)^2=d_2{}^2 \\ (x_m-x)^2+(y_m-y)^2=d_m{}^2 \end{cases} \tag{4}$$

By subtracting the mth equation from the first m−1 in Eq. 4, the linear Eq. 5 is obtained [44]

$$A \times K = b \tag{5}$$

where A is shown in Eq. 6 and b in Eq. 7.

$$A = \begin{cases} 2\times(x_1-x_m) & 2\times(y_1-y_m) \\ 2\times(x_2-x_m) & 2\times(y_2-y_m) \\ 2\times(x_{m-1}-x_m) & 2\times(y_{m-1}-y_m) \end{cases} \tag{6}$$

$$b = \begin{cases} x_1{}^2-x_m{}^2+y_1{}^2-y_m{}^2+d_1{}^2-d_m{}^2 \\ x_2{}^2-x_m{}^2+y_2{}^2-y_m{}^2+d_2{}^2-d_m{}^2 \\ x_{m-1}{}^2-x_m{}^2+y_{m-1}{}^2-y_m{}^2+d_{m-1}{}^2-d_m{}^2 \end{cases} \tag{7}$$

The PUE position is obtained by Eq. 8 [44].

$$K = \left(A^T \times A\right)^{-1} \times A^T \times b \tag{8}$$

The PUE position (x, y) is extracted from K, an array of two numbers [44]; these equations are implemented in Python, and a multithread client-server application was developed in Android Studio to send the information to the CBS.

4.1.3 Application data

Application information is shared by using the sensor network. The first data transmitted are the RSSI of each phone. Information is transmitted by PBS, CBS, or PUE; the data shared are mobile country code (MCC), mobile network code (MNC), short name, location area code (LAC), and cell identification (CID), among others, that conform the global cell identification (GCID); these information is useful to recognize if it is a valid operator, and these information may change in agreement with each country regulations.

Even if the PUEA is smart, there are things that it cannot do. For example, PUEA can mimic the MCC, MNC, and LAC, but it has to assign a different CID, and the

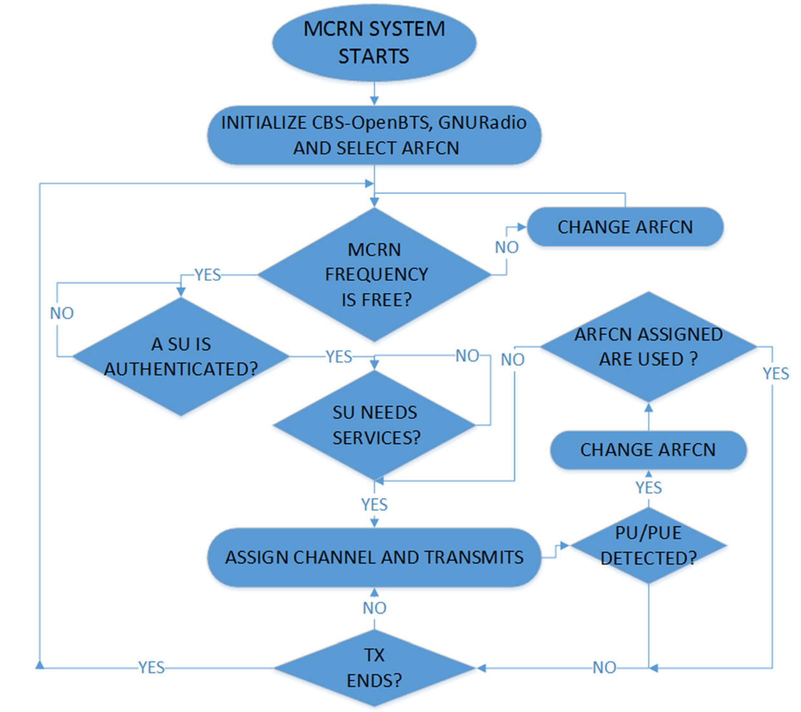


Fig. 6 Proposed MCRN algorithm

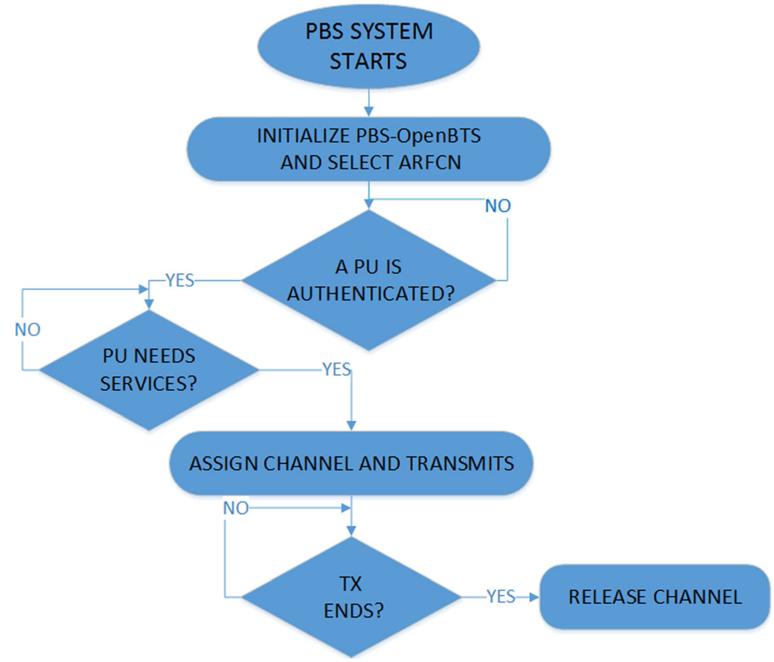


Fig. 7 Proposed PBS algorithm

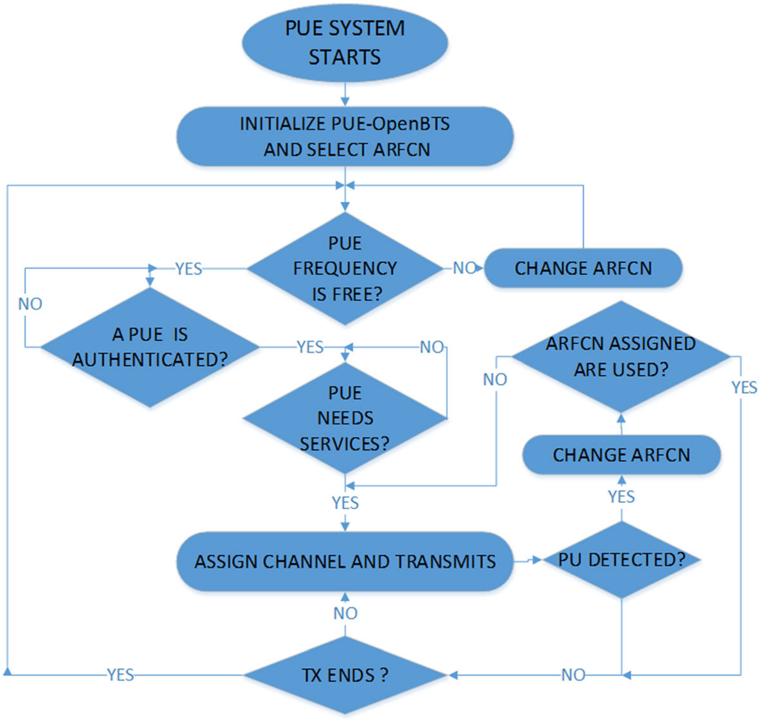


Fig. 8 Proposed PUE algorithm

short name cannot be the same of the real PBS, so it cannot mimic all the information required. A GSM network uses the same short name and different CID, and the network is connected to a shared home location register (HLR) that contains the PU information and based on signaling mobile user can do the handoff between PBS. As the PUE does not have a connection to the shared HLR, it does not know if a user is PU or SU, then PUE has two ways to deal with this. The first option is to allow access to the network to everyone without considering the type of phone, operator, or SIM card. The other option is to allow access to selected users. Then, the detection system attempts to connect to the network and to send the information to the CBS, such as the GCI, short name, and the authentication answer. A site survey was made to know the operator's short name and global values to be able to compare them with the PUEA information.

4.1.4 Primary user emulation defense

The combination of the three methods described before, i.e., energy detection, localization detection, and the use of the application data, allows to detect the PUEA with accuracy. The next step in order to defend from PUEA is to save the information as a fingerprint in a database in the BS, as a blacklist. From a regulatory point of view, the crucial information could be shared to the PU or to the primary network to let them know the characteristics of the attacker, and thereby, they can take the pertinent legal actions, depending on each country's regulations.

The SU connected to the MCRN must authenticate and its IMSI is saved in a database, and thus, only authenticated users can access the system. There are two alternatives for authentication from the PUE's point of view, one alternative is to allow only to the users that want to subscribe and the other way is to let everyone to connect to the network freely, which is not the best choice for the PUE in terms of security.

4.2 Detection system flowchart

Algorithms are described in this section, corresponding to the MCRN, PBS, PUE, and detection system.

4.2.1 MCRN algorithm

The MCRN algorithm initializes the CBS and OpenBTS and selects an absolute radio frequency channel number

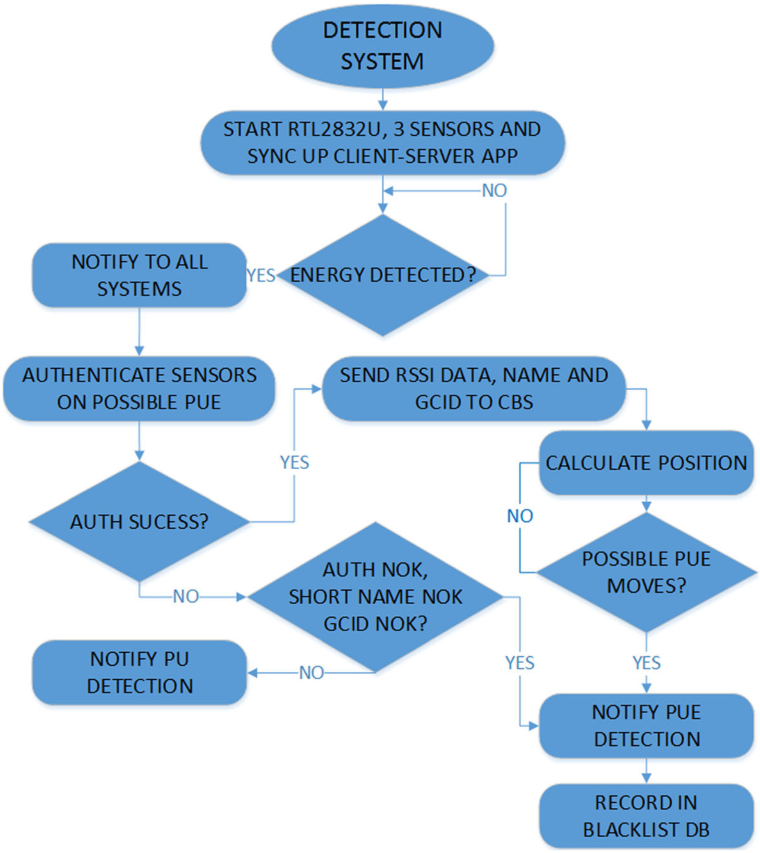


Fig. 9 Proposed detection algorithm

Table 2 Energy detector simulation parameters

Parameter	Description
Simulation method	Monte Carlo
Sample points	N = 10,000
Signal to noise ratio	− 8 dB, − 10 dB, − 12 dB, − 14 dB, − 16 dB
DL frequency	876.8 MHz
Noise signal	AWGN
Transmitted signal	$x(t) = 2 \times \cos(2 \times pi \times 878.8 MHz \times t)$

(ARFCN) in the selected range; this is the frequency assigned to downlink (DL) and uplink (UL) for a PU to communicate with the PBS. For this scenario, we use GSM-850 MHz, and after a site survey, we found that ARFCN 166 and 172 and upper frequencies are not used, the 166 frequency band was chosen which is 876.8 MHz in DL and 831.8 MHz in UL, and the 172 frequency band which is 878 MHz in DL and 833 MHz in UL, since they are not used. The presence of PU or PUE are constantly verified by energy detection, and in case of PU or PUE detection, the operation is changed to another frequency, or it is stopped if there is no available free frequencies, as illustrated in the algorithm in Fig. 6.

4.2.2 PBS algorithm

The PBS mimics, a real, i.e., an operative PBS mobile operator called XX, identified with MCC: 732, MNC: 10X, LAC: 5XX, and CID: 21XXX. We called XX_ to the experimental network with our imitated PBS. The used frequencies are the same as the assigned to XX (850 MHz), and they allow phone calls or SMS between two phones. The PBS is used to control the calls and the spectrum access for PU in laboratory conditions.

The PBS algorithm initializes the PBS, and if a PU is authenticated and needs service, it assigns a channel and transmits as it is shown in Fig. 7.

4.2.3 PUE algorithm

The PUE mimics the operative PBS of the XX operator, and it is identified with MCC: 732, MNC: 10X, LAC: 5XX, and CID: 21XXX. The short name for the experimental network is XX2. The used frequencies are the same as the assigned to XX (850 MHz), and they allow phone calls or SMS between two phones. The PUE has a dynamic location to represent the case scenario conditions of a mobile attacker. Then, it transmits in the absence of the PU and the signal is stable to the PUEs connected to it, i.e., the power is constant. In another scenario, the power could be adaptive, but in practice, this causes instability in the PUE connection. The PUE only allows the connection of previously phones configured for PUEA in its database. If other phone tries to connect, the connection is rejected. The PUE moves randomly in the coverage area. The use of the spectrum analyzer is reserved for smart attacks, and thus, it was not required in case of a basic attack.

The PUE algorithm initializes the PUE; if the PUE frequency is free, PUE is authenticated and needs services, and it assigns a channel and transmits; if a PU is detected, it makes a frequency hop or ends the

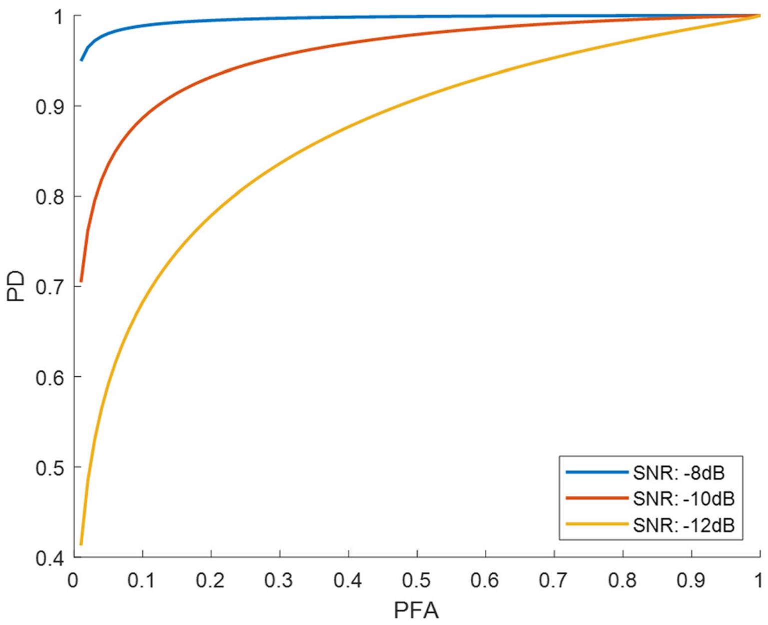


Fig. 10 Probability of detection vs probability of false alarm results for AWGN channel

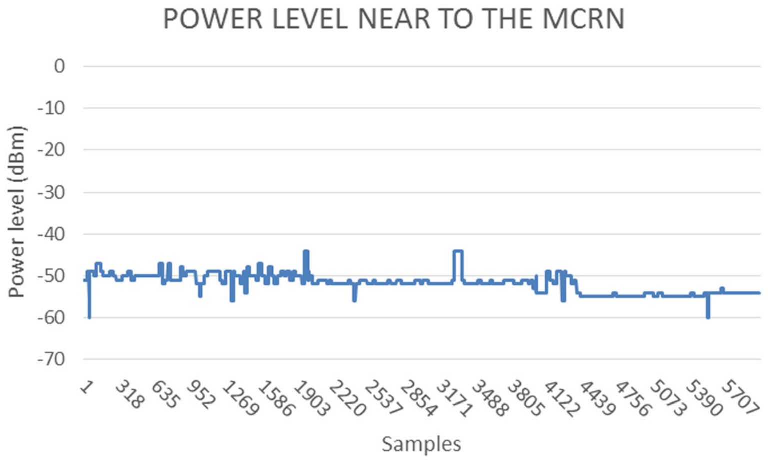


Fig. 11 Power level measured near to the MCRN

transmission if there are no more free channels as is shown in Fig. 8.

4.2.4 Detection algorithm

The first part of the detection algorithm is to use the energy detection to find if there is a PU or PUE transmitting in the selected ARFCN. The advantage of this is that in less than 100 ms, the detection system indicates that CBS has to release the frequency, as shown in the Section 5. At this point, when the energy detection is activated, the system starts the server to communicate with the client applications in the mobile phones used as sensors. It identifies the networks transmitting, XX_ or XX2, and try to authenticate. If it can make authentication (Auth), it sends the short name and GCID information to the CBS, and it takes the three RSSI and applies the least square algorithm to locate the position of the PUE.

Therefore, the system can identify if the information is out of the used standard for telecommunication operators. In parallel, the system reads the position in real time, and if the movement is more than 30 cm in any direction, it is identified as a PUE. In our system, if the detection algorithm identifies PUEA by means of the energy detection and more than one of the other used methods detect it, then the system shows a positive flag of PUE in the MCRN software and saves the information in a blacklist database to avoid future connection attempts.

The detection algorithm is shown in Fig. 9.

5 Results and discussion

In this section, the results of the test scenarios are presented and analyzed.

5.1 Energy detection

In MCRN, the double threshold Eq. 1 is transformed to Eq. 9.

$$y(t) = \begin{cases} n(t) & SU \\ h(t) * s(t) + n(t) & PU/PUE \end{cases} \tag{9}$$

This is because the energy detector cannot differentiate between PU and PUE by itself.

A binary hypothesis test is used to find out the probability of detection (PD) and the probability of false alarm (PFA); this is defined in Eq. 10.

$$Y(n) = \begin{cases} w(n) & H0 \\ s(n) + w(n) & H1 \end{cases} \tag{10}$$

It is assumed an additive white Gaussian noise (AWGN) channel, with a constant spectral density, noise with zero mean, and variance one and is assumed to be

Table 3 Parameters for energy detection

Parameter	Description
Number of samples	6000 at each point of the grid
Total samples	*N* = 600,000
Signal to noise ratio	− 9 dB
Threshold value	− 60 dBm
DL frequency	876.8 MHz
Noise signal	AWGN
Primary users	2 (PU1, PU2)
Service	One phone call
Time of measurement	10 min for each point of the grid
Confidence level	95%
Margin of error	4%

white over the bandwidth of consideration; $w\ (n)$ is AWGN, n is sample index, and $s\ (n)$ is the PU/PUE signal. Hypothesis H0 states that there is no PU/PUE detected in the channel. H1 indicates that PU/PUE is present. We use an energy detection based in [45, 46]; N is the total number of samples of the energy, and $Y(n)$ are added during one S_i detection interval, as shown in Eq. 11.

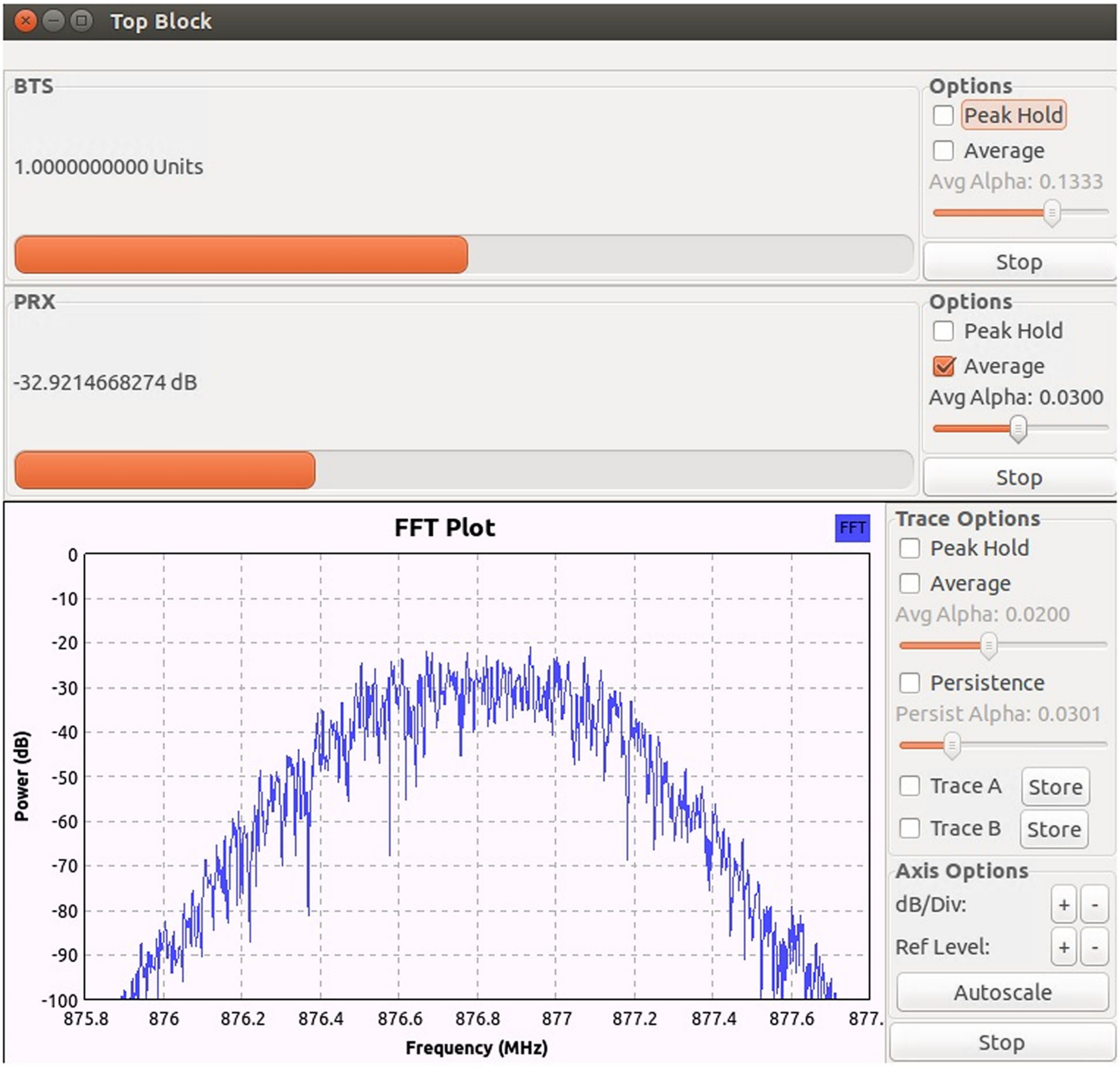
$$Z(Y_n) = \frac{1}{N}\sum_{n=1}^{N} |Y(n)|^2 \tag{11}$$

Comparing Z with a threshold λ, the CBS decides about presence or absence of PU/PUE signals. The probability of detection and the probability of false alarm for the energy detection are defined in Eq. 12.

$$\begin{aligned} P_d &= p(Z \geq \lambda|\mathrm{H1}),\\ P_{fa} &= p(Z \geq \lambda|\mathrm{H0}). \end{aligned} \tag{12}$$

Z is a Gaussian random variable with zero mean and variance ${\sigma_m}^2$, and γ is the signal to noise ratio (SNR).

The probability of false alarm (PFA) and the probability of detection (PD) are defined in Eq. 13



Top Block

BTS

1.0000000000 Units

Options

□ Peak Hold

□ Average

Avg Alpha: 0.1333

Stop

PRX

-32.9214668274 dB

Options

□ Peak Hold

☑ Average

Avg Alpha: 0.0300

Stop

Trace Options

□ Peak Hold

□ Average

Avg Alpha: 0.0200

□ Persistence

Persist Alpha: 0.0301

□ Trace A Store

□ Trace B Store

Axis Options

dB/Div: + -

Ref Level: + -

Autoscale

Stop

Fig. 12 GNU-radio view of the experiment of downlink DL-876.8 MHz

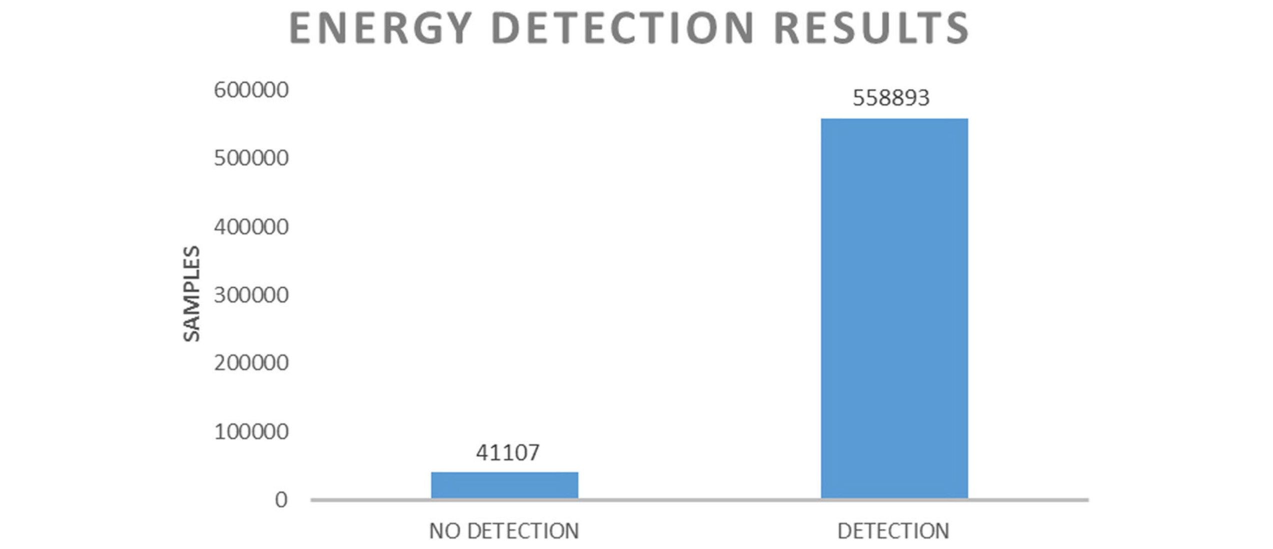


Fig. 13 Energy detection results

$$\begin{aligned} P_d &= Q\left(\frac{\lambda - N - N\times\gamma}{\sqrt{2\times N + 4\times N\times\gamma}}\right) \\ P_{fa} &= Q\left(\frac{\lambda - N}{\sqrt{2\times N}}\right) \end{aligned} \tag{13}$$

where $Q(.)$ is the Gaussian complementary function [46]. Table 2 shows the simulation parameters for energy detector.

Figure 10 shows the results of the receiver operating characteristics (ROC) for different SNR values, which are consequent with [46, 47]. These curves serve as a parameter to study the performance of the sensing scheme [46, 47].

In the detection model, the total coverage radio was divided in a grid with 100 parts as shown in Fig. 14. We measure the power signal in each point of the grid in case of the presence and absence of the PU or PUE. According to [47], the IEEE 802.22 standard recommends PFA < 0.1 for spectrum sensing. Analyzing the simulation results for this PFA, we expect an 88% of detection. To find an optimal threshold to the experiment, PU power level was measured and 600,000 samples were taken in the lowest part of the grid close to MCRN; the lowest power measured was − 60 dBm as shown in Fig. 11, and it is used as the threshold for the experiments. With these samples, the confidence level is 95% and margin of error is 4%. The margin of error is the range of values below and above the sample statistic in a confidence interval.

To probe the energy detector, the power signal in the frequency assigned is measured every 1 ms; to avoid error, 100 values are averaged according to Eq. 11. In 100 ms, the system detects the presence of a PU/PUE signal, comparing with empirical threshold from Eq. 12.

The parameters shown in Table 3 were considered for the experiment.

As an example of received signal, Fig. 12 shows the GSM downlink spectrum measured at 876.8 MHz, with a 200-kHz bandwidth, using the GNU-radio platform [48]. The algorithm calculates the average, and using a specific threshold, a PU/PUE is detected and the CBS is notified with a binary result, one for detection and zero for no detection of PU signal.

Software was programmed to save the binary data results from energy detection. Results from experiment show the detection of 93% of positive PU presence as shown in Fig. 13.

5.2 Motion detection

The motion detection has two parts, the learning process and the position estimation. In the learning process, the mobile phones used as sensors are placed and the distances are calibrated with a PUE; the parameters for the

Table 4 Parameters for motion detection learning process

Parameter	Description
Number of samples	10,000 at each point of the grid
Total samples	*N* = 1,000,000
Averaged values	50
Location algorithm	Least square
Sensor phone type	Samsung J7 (S1), Alcatel 5026a, Kempler & Strauss plus 5.5″
Service	One phone call
Time of measurement	4 min for each point of the grid
Confidence level	95%
Margin of error	4%

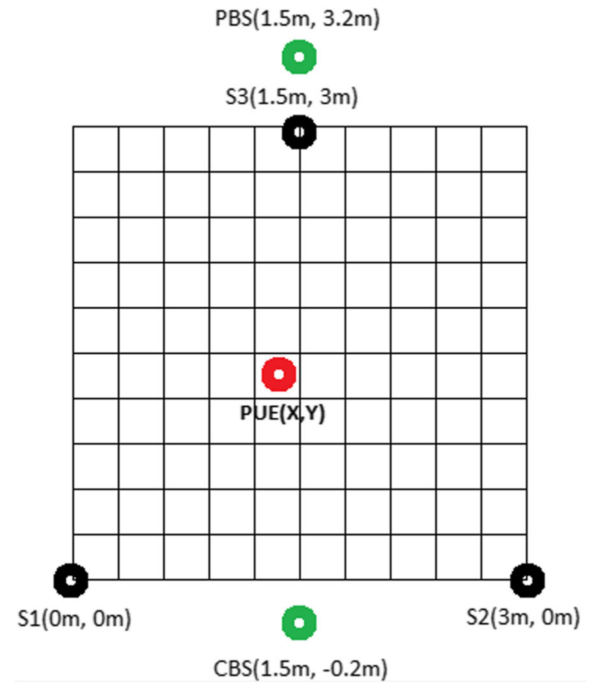


Fig. 14 Position grid

least square algorithm are updated. The second part consists in reading the averaged RSSI values from the three sensors and to estimate the position. In order to get reasonable measures in real time, for the average, 50 values are taken. Kalman's filter cannot be implemented because the PUE could be in movement. The parameters for motion detection learning process are shown in Table 4.

For this experiment, 10,000 samples were taken in each one of the 100 steps of the grid, the position of each component for the experiment is shown in Fig. 14.

The last step in the motion detection is to measure the variation of position against the first one taken. If this variation is more than 30 cm (one grid step), the system detects a movement and identifies it as a PUEA. If there is a negative position, it indicates out of the grid, but it can read the movement too. Figure 15 shows one example of the RSSI variation before the average with a fluctuation of +/− 4 dBm.

Figure 16 shows the RSSI variation after average RSSI.

The average position error is less than 15 cm (5%) of the total grid; this is the reason why the assigned position variation is set to 30 cm move. The position error measured to a distance from 0 to 3 m can be seen in Fig. 17.

The generated movement is random to test the system. Ten thousand RSSI signals were measured and the movement condition is one grid (≥ 30 cm). Therefore, if the movement is more or equal to 30 cm, it is detected as PUE. The experiment starts with PUE in one position of the grid, then it makes random movements, and the algorithm compares with the initial position marking it as PUE. The PUE is placed in 100 points at the grid for the experiment, and the position is evaluated after 10 s to detect possible movement. The experiment parameters are shown in Table 5.

Results are saved as a binary flag (0, no movement, or 1, movement); the system detects that a suspicious PUE is moving 97% of the times because of the RSSI variation error as shown in Fig. 18.

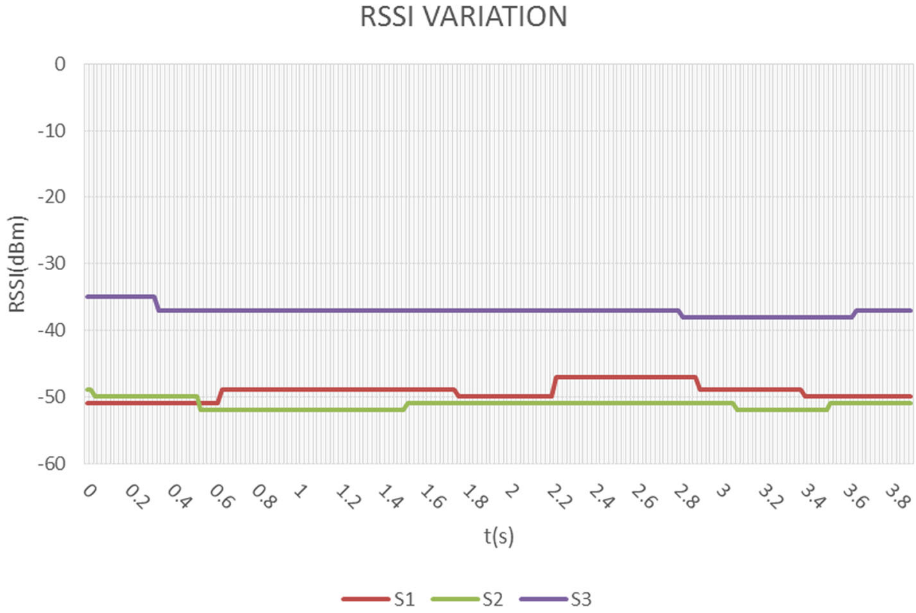


Fig. 15 Static position variation in time

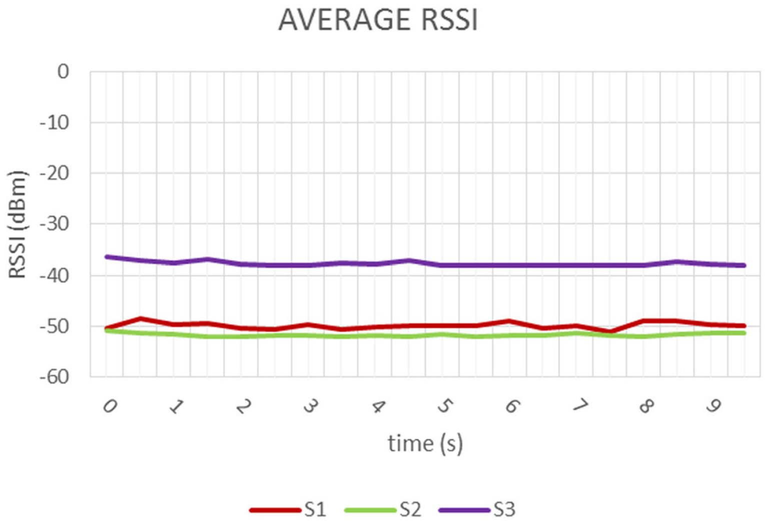


Fig. 16 Average RSSI with static position in time

5.3 Application data

Based on measures of the site survey and the experiments' configuration settings in the PU and the PUE, data from operators in Colombia were identified with the following information: MCC = 732, MCN = 101-Claro, 102-movistar, 111-tigo, 142-une, and 154-virgin. Then, the application sends information such as the short name of the network, the MCC, and MNC to the CBS. The CBS compares received data with the real operator's information and thus identify it as a possible PU or PUE. In addition, the sensors S1, S2, and S3 are authenticated at the network. If both the information and the authentication are alright, the suspicious mobile finally is identified as PU. On the contrary, the mobile is marked as PUE. The mobile phones used as sensors are configured as 2G operation mode on its internal configuration, and an example of this is shown in Fig. 19, and the mobile phone lists the available networks in Fig. 20. This is an example of the mobile phone screen, where the software made it automatically.

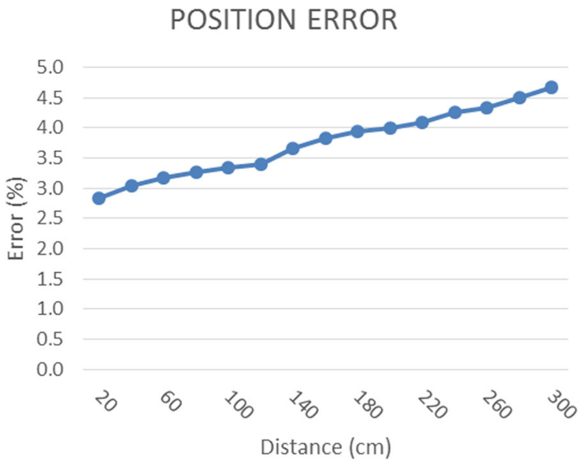


Fig. 17 Position error

In case of the presence of any other short name in the system, i.e., another operator, the sensors will try to connect and extract its information in parallel with action taken by the motion detection algorithm. In the experiments, the default name of the PUEA is "01-001" or also the "range network," depending on the SDR, but if it is imitating a true PU, the attacker appears similar, for example, like Operator_. We start the test making a smart PUE that mimics a PU, but as the system identifies a no valid short name, or if the authentication fails, it is marked as PUE, as seen in Fig. 21.

If PUE mimics the real short name of the operator, the algorithm detects a duplicate name and tries to authenticate both to identify the PU and the PUE correctly.

The parameters for the experiment are shown in Table 6.

The results are saved as a binary result (0, authentication OK, and 1, no authentication). They show that detection of authentication is made at 100%, as shown in Fig. 22.

5.4 Computational complexity

The computational complexity is calculated according to [49] by counting only the number of real multiplications, real additions, and comparisons. These operations are calculated in the CBS. It is denoted as the number of averaging values N_{AV}, the number of fast Fourier transform (FFT) points is N_{FFT}, and the number of subchannel is N_C. The number of real operations for energy detection (C_e), motion detection (C_m), and application data (C_a) are described below in Eq. 14.

Table 5 Parameters for motion detection

Parameter	Description
Number of samples	100 at each point of the grid
Total samples	N = 10,000
Signal to noise ratio	− 9 dB
Movement threshold	30 m
DL frequency	876.8 MHz
Noise signal	AWGN
Secondary users	2 (PUE1, PUE2)
Service	One phone call
Time of measurement	10 s for each measure
Confidence level	95%
Margin of error	4%

$$\begin{aligned} C_e &= 7N_{\mathrm{AV}}N_{\mathrm{FFT}} + 5N_{\mathrm{FFT}}\,\log_2 N_{\mathrm{FFT}} - \frac{N_{\mathrm{FFT}}}{N_C} \\ C_m &= 174N_{\mathrm{AV}} \\ C_a &= 9N_{\mathrm{AV}} \end{aligned} \tag{14}$$

For energy detection, the complexity indicator is medium and for motion detection and application data is low. Energy detector in frequency is at the same level that superimposed training (ST) [50], covariance-based detection, and wavelet-based detection [49]. The motion detection and application data are classified at the same level that energy detection in time, but most of the methods are in medium complexity [49].

5.5 Analysis of the results

The empirical threshold for energy detection was acquired by measures in the whole coverage area; this is in order to obtain better detection results. The motion detection system responds to a 30-cm movement; it detects 97% of the PUE with dynamic location by comparing the initial position with samples of the position every second. The proposed application extracts every 30 s crucial information based on authentication, RSSI, and the list of available networks. This is in order to test if there is presence of the PU or the PUE. And thus, this method detects 100% of PUE attacks.

In case that the PUE mimics the short name of the network, the system detects identity duplication. The PU is not able to connect to the network because PUE does not share the database with a real network, and thus, it cannot make the handoff. PUE is not able to authenticate the PU or SU because it does not have previous knowledge of the IMSI or any information of the users. In order to authenticate users, PUE must know the IMSI previously.

After the detection system identifies a PUE attack, the MCRN knows that it is not a PU and it can continue transmitting data to SU. If PUE attack continues, it could be considered as a jammer for PU and SU affecting both the primary network and the secondary network.

The computational complexity is low for motion detection and application data. Energy detection complexity is medium as most of the methods found in the literature.

6 Contributions

The main contribution of this paper is that it implements the MCRN, the PBS, and the PUE attack and establishes three methods to detect it through a novel cross-layer design technique which includes analysis in the physical, medium access control, and the application data with users and PUE in motion.

This attack detection technique was tested in a test bed using software-defined radio equipment and mobile phones at indoor scenarios with static and dynamic

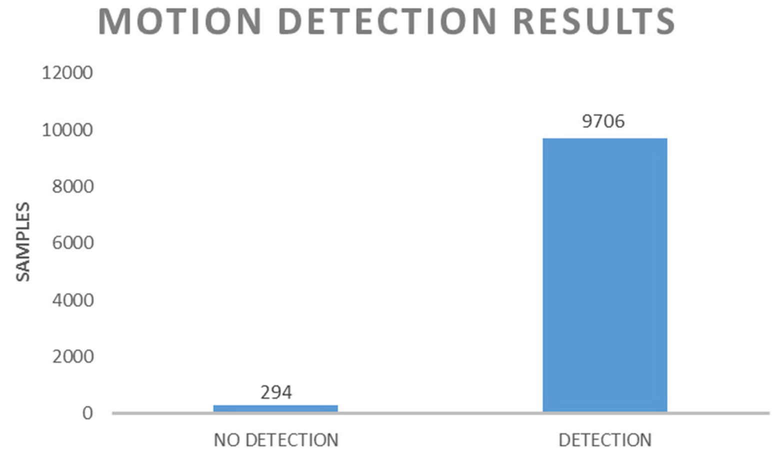
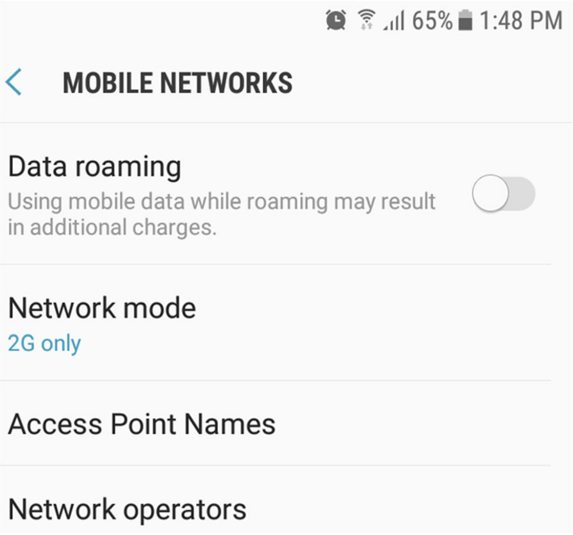


Fig. 18 Motion detection results



65% 1:48 PM

MOBILE NETWORKS

Data roaming
Using mobile data while roaming may result in additional charges.

Network mode
2G only

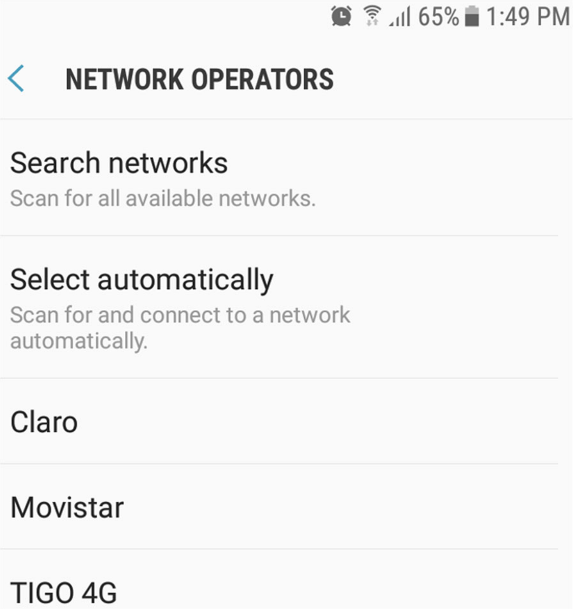
Access Point Names

Network operators

Fig. 19 2G configuration view of the mobile screen

locations to generate the MCRN. The attacks and a mobile phone base station were also built up with software-defined radio to emulate a PBS.

To the best of the authors' knowledge, the cross-layer design proposal for PUE has not been presented before in literature with experiments neither, with mobility conditions of the attacker as presented in this research work.



65% 1:49 PM

NETWORK OPERATORS

Search networks
Scan for all available networks.

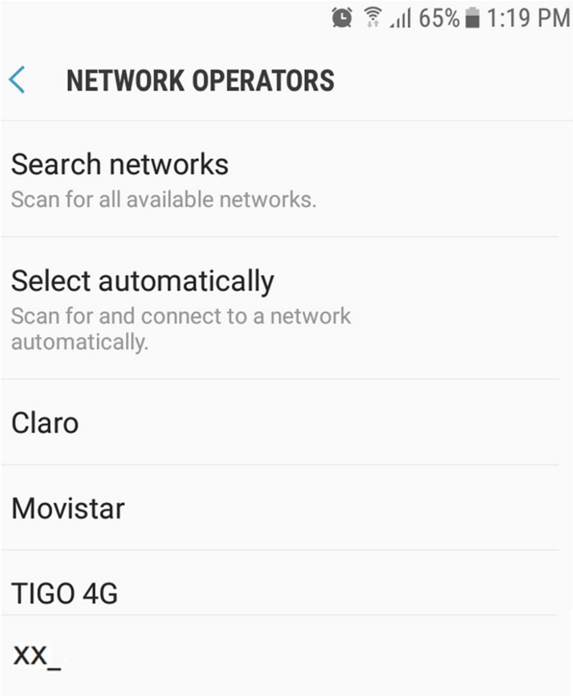
Select automatically
Scan for and connect to a network automatically.

Claro

Movistar

TIGO 4G

Fig. 20 Network short name view of the mobile screen



65% 1:19 PM

NETWORK OPERATORS

Search networks
Scan for all available networks.

Select automatically
Scan for and connect to a network automatically.

Claro

Movistar

TIGO 4G

XX_

Fig. 21 Available networks with PUE screen in mobile phone

7 Conclusions

We have studied the methods for detection of primary user emulation and proposed a novel technique using cross-layer design with a static or dynamic location of the attacker. The experiments using mobile phones and a software-defined radio test bed probed were useful in showing a lot of possibilities to test the cognitive radio technology, under a mobile attacker.

The results show that the cross-layer design combining the three proposed techniques, energy detection, motion estimation, and application information analysis, is able to optimize the detection of the primary user

Table 6 Parameters for authentication

Parameter	Description
Number of samples	600
Signal to noise *r*	− 9 dB
Movement	Random
DL frequency	876.8 MHz
Noise signal	AWGN
Secondary users	2 (PUE1, PUE2)
Service	Authentication of sensors
Time of measure	30 s for each measure
Confidence level	95%
Margin of error	5%

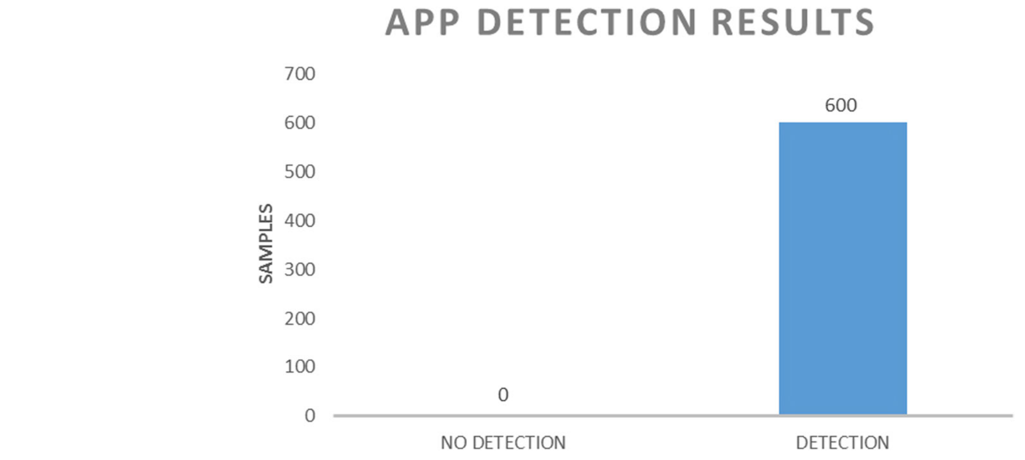


Fig. 22 Application data authentication results

emulation attack with static or dynamic location with 100% accuracy on MCRN. The energy detection system detects 93% of the signal from both primary users (PU) and primary user emulator (PUE) with a sample every 100 ms even though the signal to noise ratio (SNR) is about − 9 dB. This system detects the signals with accuracy, which helps to the mobile cognitive radio network (MCRN) to prevent interference. Motion detection system responds to a 30-cm change, and it detects 97% of the PUE movement with dynamic location by comparing the initial position with samples of the position taken every second and reported every 10 s. The proposed information application extracts crucial information every 30 s based on authentication, RSSI, and the list of available networks. This detects the presence of PU or the PUE. These results show a practical and effective approach to detect primary user emulation attacks.

As future research, we suggest to explore what to do after PUEA detection. Systems can make an advertisement to operators or regulators about PUE presence, with specific characteristics in a specific area.

Abbreviations

ARFCN: Absolute radio frequency channel number; AWGN: Additive white Gaussian noise; CBS: Cognitive base station; CID: Cell identification; CRN: Cognitive radio network; DL: Downlink; GCID: Global cell identification; HLR: Home location register; LAC: Location area code; MCC: Mobile country code; MCRN: Mobile cognitive radio network; MNC: Mobile network code; PBS: Primary base station; PD: Probability of detection; PFA: Probability of false alarm; PU: Primary user; PUE: Primary user emulation; PUEA: Primary user emulation attack; QoS: Quality of service; ROC: Receiver operating characteristics; RRM: Radio resource management; RSSI: Received signal strength indicator; SDR: Software-defined radio; SNR: Signal to noise ratio; SU: Secondary user; UL: Uplink; USRP: Universal software radio peripheral

Acknowledgements

We express our gratitude to Colciencias, Universidad Nacional de Colombia, for the founding of this project, and also to the Autonomous Metropolitan University, Iztapalapa in Mexico City, to Professor Victor Rangel from the National Autonomous University of Mexico, and to the University Distrital Francisco José de Caldas, Bogotá Colombia. E. Rodriguez-Colina is also grateful to the Council of Science and Technology of Mexico (CONACyT).

Authors' contributions

The algorithms proposed in this paper have been conceived by EC, and EC, ER, LP, and IP designed the experiments. EC and ER performed the experiments and analyzed the results. EC is the main writer of this paper. All authors participated in the discussion and proofreading work. All authors read and approved the final manuscript.

Funding

This research was funded by a grant of Colciencias, Doctorado Nacional 757.

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Systems and Industrial Department, College of Engineering, Universidad Nacional de Colombia, Bogota, Colombia. [2]Electrical Engineering Department, Autonomous Metropolitan University, Iztapalapa, Mexico City, Mexico. [3]Technological Faculty, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. [4]Systems and Industrial Department, College of Engineering, Universidad Nacional de Colombia, Bogota, Colombia.

Received: 2 September 2019 Accepted: 26 January 2020
Published online: 02 March 2020

References

1. J. Mitola, Software radios: Survey, critical evaluation and future directions, IEEE Aerosp. Electron. Syst. Mag. 8, 25 (1993). pp. 25-36.
2. L. F. Pedraza, A. Molina, and I. Páez, Spectrum occupancy statistics in Bogota-Colombia. Paper presented at IEEE Colombian Conference on Communications and Computing. COLCOM (2013), Medellín, Colombia. 22-24 Mayo 2013. pp. 1-6. https://doi.org/10.1109/ColComCon.2013.6564815.
3. L. F. P. Martínez, F. Forero, and I. P. Páez, Evaluación de ocupación del espectro radioeléctrico en Bogotá-Colombia. Ingeniería y Ciencia. Vol. 10 (2014). pp. 127–143.
4. L. Pedraza, C. Hernandez, K. Galeano, E. Rodríguez, and I. Páez, Ocupación espectral y modelo de radio cognitiva para Bogotá, (Univ. Dist. Francisco José Caldas, 2016).
5. W. R. Ghanem, R. Essam, and M. Dessouky, Paper presented at 2018 35th Natl. Radio Sci. Conf. NRSC (IEEE, 2018), pp. 309–318. https://doi.org/10.1109/NRSC.2018.8354378.
6. 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. 14 (2012). pp. 355-379.

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 (2017). pp. 1535–1542.
8. 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. 19 (2015). pp. 799–802.
9. 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. Paper presented at 2016 2nd IEEE Int. Conf. Comput. Commun. ICCC (IEEE, 2016), pp. 1076–1081. https://doi.org/10.1109/CompComm.2016.7924870.
10. K. Yadav, S. D. Roy, and S. Kundu, Enhanced throughput performance under primary user emulation attack in cognitive radio networks by optimal threshold selection approach. Paper presented at 2018 2nd Int. Conf. Electron. Mater. Eng. Nano-Technol. IEMENTech (IEEE, 2018), pp. 1–6. https://doi.org/10.1109/IEMENTECH.2018.8465340.
11. 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. Paper presented at 2017 Int. Symp. Netw. Comput. Commun. ISNCC (IEEE, 2017), pp. 1–6. https://doi.org/10.1109/ISNCC.2017.8071979.
12. Y. Peng, F. Xiang, H. Long, and J. Peng, The research of cross-layer architecture design and security for cognitive radio network. Paper presented at Inf. Eng. Electron. Commer. 2009 IEEC09 Int. Symp. On (IEEE, 2009), pp. 603–607. https://doi.org/10.1109/IEEC.2009.133.
13. 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. 27 (2013). pp. 34-39. https://doi.org/10.1109/MNET.2013.6523806.
14. M. Dabaghchian, A. Alipour-Fanid, K. Zeng, and Q. Wang, Online learning-based optimal primary user emulation attacks in cognitive radio networks. Paper presented at 2016 IEEE Conf. Commun. Netw. Secur. CNS (IEEE, 2016), pp. 100–108. https://doi.org/10.1109/CNS.2016.7860475.
15. S. U. Rehman, K. W. Sowerby, and C. Coghill, Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios. IET Commun. 8, 1274 (2014). pp. 1274-1284. https://doi.org/10.1049/iet-com.2013.0568.
16. D. A. Burgess, H. S. Samra, and others, the openbts project (2008). http://www.openbts.org. Accessed 1 Dec 2019.
17. M. Iedema, Getting Started with OpenBTS: Build Open Source Mobile Networks (O'Reilly Media, Inc., 2015). ISBN: 9781491924280.
18. J. Hernandez-Guillen, E. Rodriguez-Colina, R. Marcelin-Jimenez, and M. P. Chalke, CRUAM-MAC: A novel cognitive radio MAC protocol for dynamic spectrum access. Paper presented at 2012 IEEE Lat.-Am. Conf. Commun. (IEEE, 2012), pp. 1–6. https://doi.org/10.1109/LATINCOM.2012.6505997.
19. S. Rizvi, J. Mitchell, and N. Showan, Analysis of security vulnerabilities and threat assessment in Cognitive Radio (CR) networks. Paper presented at Appl. Inf. Commun. Technol. AICT 2014 IEEE 8th Int. Conf. On (IEEE, 2014), pp. 1–6. https://doi.org/10.1109/ICAICT.2014.7035911.
20. J. Sen, A survey on security and privacy protocols for cognitive wireless sensor networks. Journal of Information and Network Security. Vol. 1. ArXiv Prepr. (2013). pp. 1-30.
21. Ö. Cepheli and G. K. Kurt, Physical layer security in cognitive radio networks: A beamforming approach. Paper presented at Commun. Netw. BlackSeaCom 2013 First Int. Black Sea Conf. On (IEEE, 2013), pp. 233–237. https://doi.org/10.1109/BlackSeaCom.2013.6623415.
22. K. K. Chauhan and A. K. S. Sanger, Survey of Security threats and attacks in cognitive radio networks. Paper presented at Electron. Commun. Syst. ICECS 2014 Int. Conf. On (IEEE, 2014), pp. 1–5. https://doi.org/10.1109/ECS.2014.6892537.
23. L. Jianwu, F. Zebing, F. Zhiyong, and Z. Ping, A survey of security issues in cognitive radio networks. China Commun. 12, 132 (2015). pp. 132-150. https://doi.org/10.1109/CC.2015.7084371.
24. R. Yu, Y. Zhang, Y. Liu, S. Gjessing, and M. Guizani, Securing Cognitive Radio Networks against Primary User Emulation Attacks. IEEE Netw. 30 (2016). pp. 62-69. https://doi.org/10.1109/MNET.2016.1200149NM.
25. 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. 15, 428 (2013). pp. 428-445. https://doi.org/10.1109/SURV.2011.122211.00162.
26. D. Pu, Y. Shi, A. V. Ilyashenko, and A. M. Wyglinski, Detecting Primary User Emulation Attack in Cognitive Radio Networks. Paper presented at Glob. Telecommun. Conf. GLOBECOM IEEE (IEEE, 2011), pp. 1–5. https://doi.org/10.1109/GLOCOM.2011.6134419.
27. M. Dabaghchian, A. Alipour-Fanid, K. Zeng, Q. Wang, and P. Auer, Online Learning With Randomized Feedback Graphs for Optimal PUE Attacks in Cognitive Radio Networks. IEEEACM Trans. Netw. TON 26 (2018). arXiv:1709.10128. pp. 2268-81.
28. J. Avila, S. Prem, S. Rajapradeepa, and K. Thenmozhi, Authentication Based Primary User Emulation Attack Mitigation in Cognitive Radio. Paper presented at 2018 Int. Conf. Comput. Commun. Inform. ICCCI (IEEE, 2018), pp. 1–4. https://doi.org/10.1109/ICCCI.2018.8441397.
29. M. Khasawneh and A. Agarwal, A survey on security in Cognitive Radio networks. Paper presented at Comput. Sci. Inf. Technol. CSIT 2014 6th Int. Conf. On (IEEE, 2014), pp. 64–70. https://doi.org/10.1109/CSIT.2014.6805980.
30. 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. Paper presented at Pervasive Comput. ICPC 2015 Int. Conf. On (IEEE, 2015), pp. 1–6. https://doi.org/10.1109/PERVASIVE.2015.7086985.
31. A. N. Akhtar, F. Arif, and A. M. Siddique, Spectrum Decision Framework to Support Cognitive Radio Based IoT in 5G. Cogn. Radio 4G-5G Wirel. Commun. Syst. 73 (2018). pp. 73-92. https://doi.org/10.5772/intechopen.80991.
32. M. A. Shah, S. Zhang, and C. Maple, Cognitive radio networks for Internet of Things: Applications, challenges and future. Paper presented at 2013 19th Int. Conf. Autom. Comput. (IEEE, 2013), pp. 1–6.
33. C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, Secure integration of IoT and cloud computing. Future Gener. Comput. Syst. 78, (2018). pp. 964-975. https://doi.org/10.1016/j.future.2016.11.031.
34. A. A. Khan, M. H. Rehmani, and A. Rachedi, Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions. IEEE Wirel. Commun. 24 (2017). pp. 17-25. https://doi.org/10.1109/MWC.2017.1600404.
35. S. Christos and K. E. Psanis, Recent advances delivered by mobile cloud computing and Internet of Things for Big data applications: A Survey. International Journal of Network Management Vol. 27 (Wiley, 2016). pp. 19-30. https://doi.org/10.1002/nem.1930.
36. S.-C. Lin, C.-Y. Wen, and W. A. Sethares, Two-tier device-based authentication protocol against PUEA attacks for IoT applications. IEEE Trans. Signal Inf. Process. Netw. 4 (2017). pp. 33-47. https://doi.org/10.1109/TSIPN.2017.2723761.
37. A. P. Plageras, K. E. Psannis, Y. Ishibashi, and B.-G. Kim, IoT-based surveillance system for ubiquitous healthcare . Paper presented at IECON 2016-42nd Annu. Conf. IEEE Ind. Electron. Soc. (IEEE, 2016), pp. 6226–6230. https://doi.org/10.1109/IECON.2016.7793281.
38. A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, and B. B. Gupta, Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings. Future Gener. Comput. Syst. 82 (2018). pp. 349-3587. https://doi.org/10.1016/j.future.2017.09.082.
39. C. Stergiou and K. E. Psannis, Multimed. Efficient and secure big data delivery in cloud computing. Tools Appl. 76 (2017). pp. 22803-22822. https://doi.org/10.1007/s11042-017-4590-4.
40. C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, B.-G. Kim, and others, Algorithms for efficient digital media transmission over IoT and cloud networking. J. Multimed. Inf. Syst. 5 (2018). pp. 27-34. https://doi.org/10.9717/JMIS.2018.5.1.27.
41. F. Bao, H. Chen, and L. Xie, Analysis of primary user emulation attack with motional secondary users in cognitive radio networks. Paper presented at 2012 IEEE 23rd Int. Symp. Pers. Indoor Mob. Radio Commun.-PIMRC (IEEE, 2012), pp. 956–961. https://doi.org/10.1109/PIMRC.2012.6362922.
42. F. Jin, V. Varadharajan, and U. Tupakula, Improved detection of primary user emulation attacks in cognitive radio networks. Paper presented at 2015 Int. Telecommun. Netw. Appl. Conf. ITNAC (2015), pp. 274–279. https://doi.org/10.1109/ATNAC.2015.7366825.
43. W. F. Fihri, Y. Arjoune, H. El Ghazi, N. Kaabouch, and B. A. El Majd, A particle swarm optimization based algorithm for primary user emulation attack detection. Paper presented at 2018 IEEE 8th Annu. Comput. Commun. Workshop Conf. CCWC (IEEE, 2018), pp. 823–827. https://doi.org/10.1109/CCWC.2018.8301616.
44. G. Li, E. Geng, Z. Ye, Y. Xu, J. Lin, and Y. Pang, Indoor positioning algorithm based on the improved RSSI distance model. Sensors 18, 2820 (2018). pp. 1-15. https://doi.org/10.3390/s18092820.
45. M. J. Saber and S. M. S. Sadough, Optimal energy detection in cognitive radio networks in the presence of malicious users. Paper presented at ICCKE 2013 (IEEE, 2013), pp. 173–177. https://doi.org/10.1109/ICCKE.2013.6682814.

46. E. M. Yousef, H. Y. Soliman, and A. M. Ghuniem, Sensing-Throughput tradeoff with primary user traffic and cooperative sensing in cognitive radio. Paper presented at 2017 2nd Int. Conf. Comput. Commun. Syst. ICCCS (IEEE, 2017), pp. 121–127. https://doi.org/10.1109/CCOMS.2017.8075280.
47. P. Pandya, A. Durvesh, and N. Parekh, Energy Detection Based Spectrum Sensing for Cognitive Radio Network. Paper presented at 2015 Fifth Int. Conf. Commun. Syst. Netw. Technol. (2015), pp. 201–206. https://doi.org/10.1109/CSNT.2015.264.
48. M. Abirami, V. Hariharan, M. Sruthi, R. Gandhiraj, and K. Soman, Exploiting GNU radio and USRP: an economical test bed for real time communication systems. Paper presented at 2013 Fourth Int. Conf. Comput. Commun. Netw. Technol. ICCCNT (IEEE, 2013), pp. 1–6. https://doi.org/10.1109/ICCCNT.2013.6726630.
49. X. Liu, B. G. Evans, and K. Moessner, Comparison of reliability, delay and complexity for standalone cognitive radio spectrum sensing schemes. IET Commun. 7 (2013). pp. 799-813. https://doi.org/10.1049/iet-com.2013.0037.
50. L. Lopez-Lopez, M. Cardenas-Juarez, E. Stevens-Navarro, U. Pineda-Rico, A. Arce, and A. G. Orozco-Lugo, Superimposed Training Combined Approach for a Reduced Phase of Spectrum Sensing in Cognitive Radio. Sensors 19, 2425 (2019). pp. 1-24. https://doi.org/10.3390/s19112425.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.