Physical Communication 39 (2020) 101001

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey

Fatima Salahdine [*], Naima Kaabouch

School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, United States

ARTICLE INFO

Article history:
Received 10 February 2019
Received in revised form 16 November 2019
Accepted 2 January 2020
Available online 15 January 2020

Keywords:
Cyber security
Physical layer
Cognitive radio networks
Dynamic spectrum access
Primary user emulation
Belief manipulation
Spectrum sensing data falsification
Objective function
Malicious traffic injection
Eavesdropping
Jamming attacks

ABSTRACT

Cyber-security threats and issues have been exponentially increasing over the last two decades, including in cognitive radio networks. These attacks and vulnerabilities negatively impact the normal functioning of these networks. Investigating these vulnerabilities and their countermeasures is a necessary step toward securing the cognitive radio based networks. Although there have numerous survey papers on cognitive radio security, a few papers related to the security issues over the physical layer which has a primordial role in establishing radio communications. Thus, an up to date overview of the ongoing research about the threats, detection, and countermeasures techniques over the physical layer is necessary. In this paper, different attacks targeting the physical layer are described and analyzed. Detection methods and countermeasures corresponding to each attack are also discussed and compared. Challenges and future directions are presented as well.

1. Introduction

Cognitive radio has been proposed to solve the existing wireless communication problems, namely the radio spectrum resource scarcity and the inefficient spectrum management [1,2]. It enhances the utilization of the spectrum by allowing no-licensed users, secondary users (SUs), to dynamically access the available spectrum without causing interferences to the licensed users, primary users (PUs) [3]. Cognitive radio relies on three main layers: physical layer, media access control (MAC) layer, and network layer. New functionalities were added to the functions of the three conventional layers to support the cognitive radio features and to allow the dynamic spectrum access [4]. In general, the physical layer ensures a number of functions related to modulation, coding, and data transmission [5]. It was modified to support the cognitive radio functionalities, including spectrum sensing [3,6] which allows dynamic access to the radio spectrum [7].

As any network, cognitive radio networks are subject to several cyber-attacks that can disrupt their normal operation [8]. Security of cognitive radio has received considerable research impetus. Network security is based on three main requirements: confidentiality, availability, and integrity [9,10]. Confidentiality aims at limiting access to sensitive data through confidentiality agreements between the sender and the receiver. Availability ensures reliable access to information at any time. Integrity ensures that no changes are made to data during transmission such as deletion, addition, and alteration [11,12]. In order to specify a threat, it is necessary to determine which security requirement is violated.

No-licensed users can be either trusted or not trusted nodes. Trusted nodes perform the sensing functions by following the protocols defined in the network while untrusted nodes operate selfishly or maliciously and violate the network security requirements. Selfish users aim at using the available spectrum without sharing it with legitimate SUs by hindering them from accessing the spectrum. Malicious users aim to disturb the normal operation of the network by preventing legitimate SUs from using the spectrum and exploiting the physical layer vulnerabilities [4]. Both these types of untrusted users can cause severe problems to the network and degrade its performance.

In the literature, a number of papers related to security threats targeting the cognitive radio layers have been published [4,8,9,13–34]. However, most of these papers describe security attacks corresponding to the network layer [13] or the MAC layer [4]. Examples of these attacks include low-cost ripple effect [8], wormhole [9,10], hello flood [13], network endo-parasite [14], control

[*] Corresponding author.
E-mail addresses: fatima.salahdine@und.edu (F. Salahdine), naima.kaabouch@und.edu (N. Kaabouch).

https://doi.org/10.1016/j.phycom.2020.101001
1874-4907/© 2020 Elsevier B.V. All rights reserved.

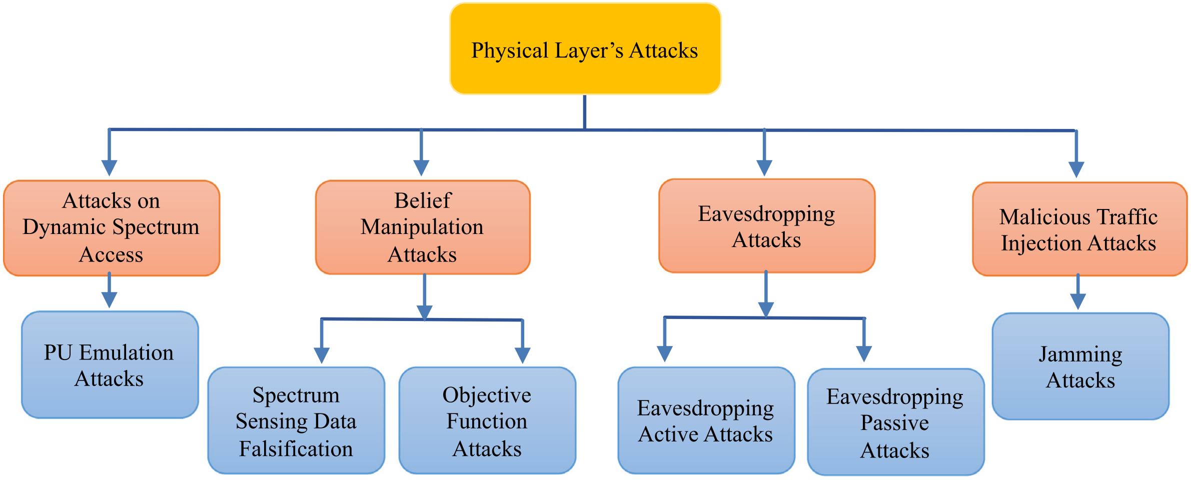
Physical Layer's Attacks
Attacks on Dynamic Spectrum Access
Belief Manipulation Attacks
Eavesdropping Attacks
Malicious Traffic Injection Attacks
PU Emulation Attacks
Spectrum Sensing Data Falsification
Objective Function Attacks
Eavesdropping Active Attacks
Eavesdropping Passive Attacks
Jamming Attacks

Fig. 1. Classification of attacks targeting the CR physical layer.

channel jamming [14,15], sinkhole [16], control channel saturation dos attack [17,18], selfish channel negotiation [19], control channel saturation [20–22], selective forwarding attack [23,24], and routing toward PU [25–27]. Few survey papers have been published about the security of the physical layer [20,28–32]. Other papers did not describe well or completely all the security threats at the physical layer, and a few papers focused on the detection or countermeasures techniques of only attack only [17, 30,33,34].

Therefore, there is a great need for detailed review papers that analyze the different attacks targeting the physical layer, their detection methods, and countermeasures. Thus, this paper describes and analyzes the most recent literature review on security attacks targeting the physical layer in cognitive radio networks. We first provides a classification of these attacks and their descriptions. Then, we analyze the detection and defense strategies to detect and to cope with these attacks. To the best of our knowledge, there is no such survey paper that includes all the attacks, detection techniques, and countermeasures related to the physical layer in cognitive radio networks. The main contributions of this paper are the following:

- Review and classification of the physical layer attacks
- Analysis and comparison of these attacks
- Analysis and comparison of the corresponding detection techniques
- Analysis and comparison of the corresponding countermeasure techniques
- Description of the challenges and some open research directions

The rest of the paper is organized as follows. In Section 2, we classify and describe the cyber-security threats targeting the physical layer of the cognitive radio network. In Sections 3, 4, 5, and 6, we describe attacks and their detection techniques. We also evaluate the different prevention and defense techniques to efficiently counteract these attacks. In Section 7, we compare and discuss the different attacks, their detection, and countermeasures techniques. In Section 8, we discuss some challenges and future directions. Finally, a conclusion is given at the end.

2. Physical layer attacks

Physical layer manages the transmission and reception of bit streams between a sender and a receiver [35,36]. Examples of functions ensured by the physical layer are: signal detection, frequency selection, and modulation. As any of the other layers, the cognitive radio physical layer can be subject to several attacks that can perturb its normal functioning [37]. These attacks can be classified into four main categories: (i) attacks on dynamic spectrum access; (ii) belief manipulation attacks; (iii) Eavesdropping attacks, and (iv) Malicious traffic injection attacks. This classification is based on which process of the cognitive radio is impacted by the attacker.

Attacks on dynamic spectrum access category includes attacks that disturb the spectrum sensing process and prevent the SUs from detecting available channels, including the PU emulation attacks (PUE). Belief manipulation attacks category aims at manipulating the radio parameters leading to wrong sensing decisions. It includes spectrum sensing data falsification and objective function attacks. Eavesdropping attacks category aims at decoding signals during transmission to overhear confidential information. It includes active and passive eavesdropping attacks. Malicious traffic injection attacks category aims at consuming the network resources leading to a denial of service. This category includes jamming attacks.

Attacks classified under each category are illustrated in Fig. 1.

Attackers can be active or passive [38]. Active attackers aim at making changes to the system operating or to the exchanged packets while passive attackers aim at observing and reading the information from the system for later purposes without impacting the system [20].

3. Attacks on dynamic spectrum access category

Attacks under the dynamic spectrum access category target mainly the detection of free channels by the SUs to prevent them from dynamically accessing the available spectrum holes. In this section, we describe one of the most serious attacks targeting the dynamic spectrum access as well as its detection and countermeasure techniques.

3.1. PUE attacks

A PUE attack is an active threat where a malicious user mimics the PU signal to prevent SUs from accessing the free channels [38]. This causes interferences to the PU, preventing SUs from using the PU channel, and enforcing them to vacate it. PUE attackers can be malicious or selfish [39]. Additionally, PUE attackers can be strategic or non-strategic. A strategic attacker follows a specific strategy to effectively achieve its goals while a

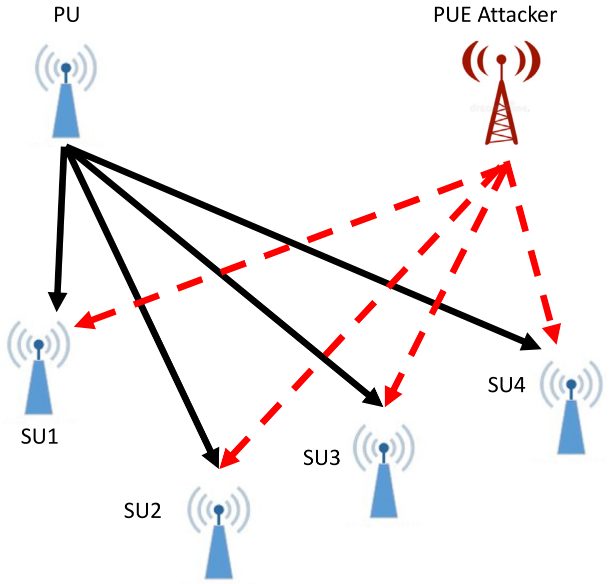

Fig. 2. Example of a PUE attack [41].

non-strategic attacker does not need any rule or strategy to lunch attacks [40]. Fig. 2 shows an example of a PUE attack.

PUE attacks impact the spectrum sensing process by deceiving SUs about the presence or absence of PU. Unreliable decisions are made due to the inability to distinguish between the PU and the attacker signal. In the sensing stage of the cognitive radio cycle, SUs under the PUE attack detect the presence of the PU signal, which is actually the attacker signal. Then, SUs drop that channel and look for another one [41]. PUE attacks can attack multiple channels resulting in busy channels and preventing SUs from accessing them. Since no successful spectrum sensing is performed, PUE attacks target the availability requirements of the network [42], which is considered an important security criterion in cognitive radio. However, PUE attacks are considered as a transient attack as vacating the channel by the attacker ends the attack's impact on the spectrum sensing process launched on SUs [43].

3.2. PUE attacks detection methods

In order to detect PUE attacks in the network, a number of techniques have been proposed [41–54]. These detection techniques which verify the authenticity of PUs can be classified based on the used scheme: cooperative or non-cooperative [41–43]. Examples of these techniques are spectrum sensing techniques, belief propagation, localization, data-base assisted, feature based, intrusion detection system, and learning based [44–51]. Some of the spectrum sensing techniques have been used for detection of PUE attacks including energy, matched filter, and cyclostationary based detection [1]. PUE detection techniques can be also classified into two classes namely location-based and non-location-based [49–54]. These detection techniques are illustrated in Fig. 3.

3.2.1. Sensing techniques

3.2.1.1. Energy detection. Energy detection technique has been used to detect the PUE attack in cooperative and non-cooperative schemes. It operates by comparing the energy of the SU received signal with a predefined threshold for detection decision [3]. For instance, in [44], the authors used energy detection to identify if the source of the transmitted signal is from a legitimate PU or a malicious user. This approach does not require the prior knowledge of the PU energy and it consists of comparing the SU received energy with the energy of the legitimate PU. In [45], the authors studied the performance of the spectrum sensing based energy detection with the presence of PUE attacks. They adopted stationary helper nodes as bridges distributed close to the PUs to communicate the sensing results to the SUs using cryptographic signatures for authentication. SUs compute the optimal number of the bridges and then verify the signatures carried in their signals. Sensing performance was improved in terms of probability of misdetection and probability of false alarm.

3.2.1.2. Other sensing techniques. Matched filter and cyclostationary based detection techniques can also be used in detecting legitimate PU signals [46]. Matched filter sensing technique operates by comparing the convolution product of the PU signal and the SU received signal with a predefined threshold [1]. It performs only when the PU signal features are known, which is not always possible in real scenarios. In [46], the authors proposed a secure authentication protocol using matched filter based detection technique in the presence of PUE attacks. The proposed protocol integrates the matched filter detection with a cryptographic digital signature to securely transmit the sensing measurements between the SUs nodes.

Cyclostationary based detection techniques perform by extracting the embedded PU signal features from the SU received signal. In [47], the authors proposed an approach for PUE attack identification, called DECLOAK, using the second order cyclostationary features. The features were computed using the sub-frequencies of the incoming signal to verify its source. However, an attacker can mimic easily the PU characteristics (modulation, bandwidth, variance, operating frequency, cyclostationary characteristics, ...) and thus SUs may not be able to distinguish between legitimate PU signals and PUE signals. Therefore, there is a great need for more efficient detection techniques to authenticate the legitimate PU while the network is under PUE attacks.

3.2.2. Belief propagation

Belief propagation based detection techniques have been used to detect PUE attacks in cooperative based schemes based on graphical models such as Manarkov and Bayesian models [48–52]. These techniques consist of estimating the unobserved and unknown variables or nodes in the system based on the information given by the neighbors. Based on the sum–product message passing, algorithms compute the conditional distribution of the known nodes as well as the marginal distribution of the unknown nodes. In [48], the authors adopted a belief propagation approach to detect attacks by computing the belief about the PU signal source by each SU. After exchanging the belief values between the SUs, the average of the belief values is compared to a threshold. If it is lower than this threshold, then the signal is from a malicious source, otherwise it is from a legitimate source. In [49], a detection technique-based belief propagation was proposed using a Markov random field in which SUs collect the sensing data and exchange the information with neighbors. SUs then compute the belief values until converged and compare the mean of the belief values to a predefined threshold to detect the malicious user. If the mean is lower than the predefined threshold, then the user is malicious. A hybrid detection method was proposed in [50] which combines belief propagation and compressive sensing [51]. It consists of compressing the received signals at a fusion center to get the legitimate PU's location. PU's location is then forwarded to SUs to perform the detection based belief propagation.

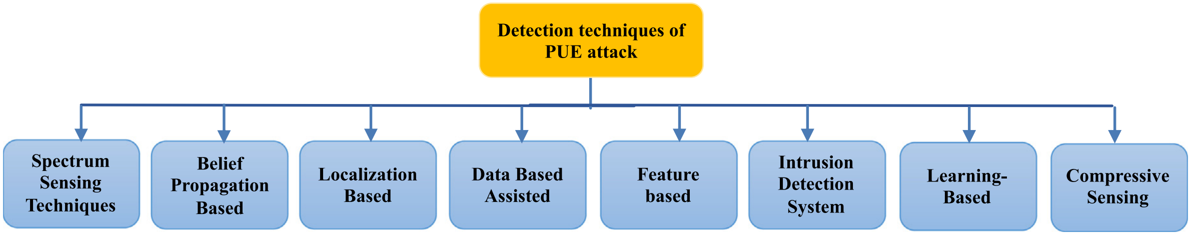

Fig. 3. Detection techniques of the PUE attack.

3.2.3. Localization and non-localization based

3.2.3.1. Localization based. The knowledge of the PU location has been used as information to help detect the PUE attack in scenarios with static or mobile SUs. For instance, the non-cooperative detection methods proposed in [24,53,54] are localization based with incumbent signal modification. In [24], the authors proposed a detection technique using the Neyman Pearson composite hypothesis. This technique requires the SUs to be uniformly distributed (legitimate and non-legitimate users) with a constant transmission power. Considering multiple attacks and highly dynamic wireless environment, this technique gives better results that those of method proposed in [52] in terms of the probability of false alarm and misdetection. In [53], the authors adopted the Fenton's approximation and Wald's sequential probability ratio test algorithms to decide whether the signal was sent by the legitimate PU or a malicious user. This technique requires the attacker's signal power to be constant. It consists of measuring the received signal power at the SUs and comparing its value with a threshold to decide about the spectrum utilization. With this technique, the probability of false alarm and the probability of misdetection decrease when the distance between the attacker and the SUs increases. This technique requires high sensing time and cannot perform well under a dynamic environment where the users' location may be random.

In [54], the work in [53] was improved by considering variable attackers' signal powers. It requires the knowledge of the location of the malicious users, the distance between the PUs and the SUs, and the distance between the SUs and the malicious user, which is not possible in real scenarios. In [55], the authors proposed a PUE detection method requiring the knowledge of the PU location and the received signal strength characteristics to operate. It consists of verifying the received signal strength, estimating the received signal energy, and then locating the transmitter to decide if the transmitter is a legitimate PU or an attacker. The authors considered the TV towers as incumbent transmitters to respect the mobility assumption. However, this assumption cannot be always true as in applications transmitters may be mobile. Also, using the received signal strength characteristics as a metric limits the efficiency of this technique in fading environments or obstacles. In [56], the authors proposed to consider the PU localization instead of the authentication by comparing the PU position and the position of the signal transmitter. If the transmitter's position corresponds to the PU position, then the transmitter is a legitimate PU, otherwise it is a malicious user. This solution requires the knowledge of the PU location by the SUs receiver and can only work for non-mobile PUs. Assuming the PU location is known, several approaches have been proposed to determine the legitimate transmitter location. Distance ratio test (DRT), distance difference test (DDT), and localization-based defense (LocDef) are examples of these techniques [29]. They are mainly performed in cooperative spectrum sensing with the assumption of fixed users in order to verify the transmitter's scheme [57]. Distance ratio test defense technique performs by obtaining the distance ratio of the received signal strength (RSS) from a couple of trusted and verified users. Distance difference test defense technique allows identifying the location of the transmitter using the phase difference of the received signal. Localization-based defense technique consists of using more wireless sensors to snapshot the received signal strength. The received signal strength is then used to identify the location of the transmitter user, which is represented by its peak [8].

3.2.3.2. Non-localization based. A number of non-location-based detection techniques have been proposed [58–61]. These techniques do not require the knowledge of the position of the PU node for PUE detection. In [58], a detection technique-based Fenton approximation method was proposed, which collects and analyzes signal samples to obtain the mean and the variance of the SU received signal. It is performed by applying Markov inequality to obtain the lower bound of the probability of a successful PUE attack. Wald's sequential probability ratio test is then used to detect the attack. All users (PU, SUs, and malicious users) are assumed to be at a fixed location with a constant power, which is not the case in real scenarios [59]. This technique allows decreasing the probability of detection while increasing the distance between the PU and the SUs. However, it requires a huge number of samples to perform and high processing time.

In [60], a detection method based on the lightweight authentication protocol and the channel impulse response was proposed to verify if the position of the PU transmitter changed, which is considered as the authentication signature. It also uses an additional fixed node, called helper node, close to the PU transmitter to enable verifying the cryptographic signatures by the SUs and thus the PU signal signature. In [61], the authors proposed a PUE technique based on the signal activity pattern acquisition and recovery system. This technique does not require any prior information about the PU; however, it requires information about the signal activity pattern such as the period of transmission, ON and OFF of the signal. It recovers the detected signal activity pattern using a recovery model and differentiates between the signal activity pattern of a legitimate PU and the signal activity pattern of an adversary.

3.2.4. Data-base assisted

Data-base assisted category includes detection techniques using databases to collect and record data [39,62–65]. For instance, in [65], the authors proposed a database assisted detection techniques using two databases: local and global. The local database is integrated at each SU restoring historical spectrum sensing results and local detection decisions while the global database is integrated at each SU's base station recording spectrum sensing results, local and global detection decisions, and other information such as the PU location and available channels. SUs check the received signals based on the stored data in the databases to verify signal sources. In [66], a two level database assisted technique combined with multi threshold energy detection was proposed to detect the PUE attacks. It performs by verifying the PU location based on fingerprints. The database assisted detection aims at building reliable and strong databases that include previous users detected malicious with their fingerprints and information. SUs check the databases first before launching the spectrum sensing process neglecting sensing information coming from these malicious PUs [67].

3.2.5. Feature-based detection

For the feature-based detection category, various signal features have been considered to detect the PUE attacks. Variance features, cyclostationary features, and log-covariance descriptors are examples of these features [61–63]. For instance, a variance detection technique was proposed to protect against PUE attacks when a malicious user employs the maximum likelihood estimator to estimate the power of the legitimate PU and transmit malicious signal instead with the same power [68]. This technique requires the prior knowledge of the location of the PU, the distance between the PU and each SU, and the distance between the PU and the malicious user. In [69], the authors proposed two feature-based detection methods in which cyclostationary features of the transmitter' signals and log-covariance descriptors were used to determine the source of the suspected signal and differentiate between the legitimate primary user and the malicious user. They assumed that the PU modulation type is known, only one user can transmit at a time, all users are using the same radio frequency range, and the noise power is low compared to their signal transmission power. In [70], wireless channel characteristics were used as unique channel features, named fingerprints, between the PU and the SUs to detect malicious users.

3.2.6. Intrusion detection systems

Integrating an intrusion detection system into the network allows learning about the normal and the abnormal behavior of the network and detect the presence of intruders in the network. It can be used to detect PUE attacks as well as other attacks targeting the physical layer. These systems can perform three main approaches, namely: signature-based, anomaly-based, and specification-based [71]. Signature-based approaches detect the patterns of the attacker by comparing their signatures to the signatures of well-known attacks. Anomaly-based approaches use statistical measures to identify the deviation from the normal activity of the network. Specification-based approaches use logical specifications to detect the anomalies in the network traffic.

In [72], the authors proposed an anomaly-based intrusion detection system using the non-parametric cumulative sum to detect existing and new attacks, including PUE attacks. It involves two main stages: learning and detecting. During the learning stage, the detection system learns about the normal behavior of the cognitive radio network and creates a profile including the traffic flow, signal power, packet delivery ratio, and PU access time. During the detecting stage, the behavior deviations are detected referring to the created profile and classified as an intrusion. In [73], an intrusion detection system was proposed based on modules named input, output, memory, and detection. It consists of four main functions: (i) manage the incoming data by the input module; (ii) save these data into the memory module; (iii) detect the presence of an attack; and (iv) then get the decision about the intrusion detected in the network by the output module. This technique requires high processing time and large memory storage to store all the information coming from the network. In [74], an intrusion detection system was proposed to store the normal activity patterns and then react when any activity does not much these patterns.

3.2.7. Learning-based

Learning based techniques consist of exploiting machine learning algorithms for intelligent and reliable PUE detection. They perform by using classification models to determine the state of the dynamic network [75]. In [76], a semi-supervised distributed learning based detection technique was proposed to detect PUE attacks. The learning based technique classifies the received data based on the previous learning and updates the dataset accordingly. The data classification is continuously adapted to the observed network state. In [77], the authors investigated how the normal behavior of the network is defined while using an intrusion detection system and how the operating deviations are determined based on machine learning algorithms. Normal behavior of a network was defined manually using some specifications and requirements, which cannot be considered correct as the traffic in a network is dynamic e in real scenarios. Integrating machine learning algorithms into an intrusion detection system permits detecting more efficiently the intrusion in real scenarios. In [78], a new detection method based on Kalman filter was proposed for mobile PUs. It consists of estimating the position of the mobile motional PUs and verify the source of the incumbent signal.

3.2.8. Compressive sensing

Compressive sensing based techniques were also proposed for fast detection of the physical layer attacks [79–82]. In [79], a detection technique based compressive sensing was proposed using cumulative sum anomaly. It consists of using few measurements of the signal to noise ratio to detect malicious users. In [80], the authors used compressive sensing for detecting PU emulation attacks by finding the transmitter's location using the received signal strength. Compressive sensing allows the reduction of the number of samples used to get the measurements for fast detection [81,82]. It is based on adaptive orthogonal matching pursuit technique to adapt the variable number of malicious users. Comparing the proposed method to the conventional one based on a fixed number of measurements, the proposed method represents better performance in terms of channel utilization.

3.3. PUE countermeasures

A number of PUE countermeasures have been proposed. These methods are classified as shown in Fig. 4. Countermeasures based cryptography consist of exploiting the cryptographic methods to keep data secret and ensure their confidentiality. Countermeasures based fingerprint consist of using fingerprints to identify the legitimate PUs. These fingerprints can be a metric or a signal feature. Countermeasures based game theory consist of employing the game theory algorithms to cope with attacks threating the operation of the network. Hybrid Countermeasures combine techniques from the three categories in order to address the limitations of each category and make use of their advantages [83].

3.3.1. Cryptography

Cryptography aims at protecting data by transforming it to codes and hidden information. It secures the information as well as the communication using cryptographic algorithms, which are mathematical models referring to key generation to preserve information privacy and confidentiality. For instance, the authors in [56] proposed a reference signal generated as a signature to identify a PU. In [57], the authors proposed a defense technique using stationary helpers to firstly authenticate the legitimate PU before forwarding the spectrum sensing results to the SUs. A public key is provided to the helper nodes by a legal authority through a trusted certificate. SUs build a trusted manner from

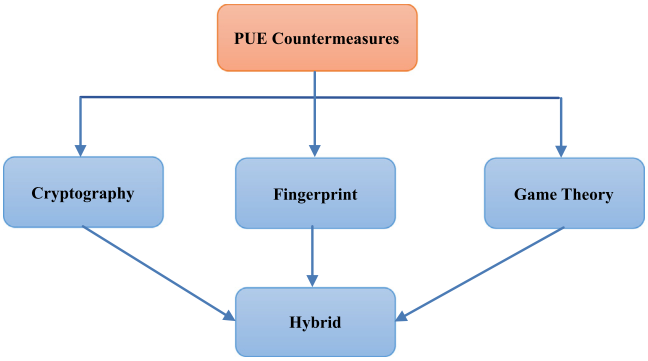

Fig. 4. Classification of existing PUE countermeasures.

the helpers to successfully cope with the attack. This technique can perform even with mobile SUs. When a malicious user is able to intercept and get the information about the PU signal, a displacement algorithm is used to allow the PU's base stations and the SUs to cooperate against the attack.

In [84], the authors proposed a countermeasure method that integrates a cryptographic key within the PU transmitted signal. For each PU signal transmitted, a corresponding key is generated using three parameters: PU identity, current time-stamp, and private key. While sensing the radio spectrum, the digital signature is detached and sent to the SU's base station via a control channel. SUs check if the detected signal was sent from a legitimate PU using a certification authority. The base stations can be subject to attacks like DoS when a malicious user continuously sent fake signals. Consequently, they need to constantly decrypt the received data, which requires more resources. In order to overcome this problem, the authors in [85] proposed to discard the duplicated keys at the SUs. However, malicious users can keep emitting fake signals resulting control channel congestion and resources waste, which can completely saturate the network.

In general, authentication based methods are efficient against PUE attacks as the attacker cannot obtain the cryptographic data to emulate the key. However, according to the regulation required by the FCC, it is not allowed to modify the PU signal. Thus, this solution does not respect the FCC requirements, which limits its efficiency.

3.3.2. Countermeasures-based fingerprint

Countermeasures-based fingerprint consist of identifying legitimate PU by verifying the fingerprint while performing the spectrum sensing [86–89]. A fingerprint represents the transmission characteristics of the PU signal. These techniques are classified into three classes, namely: hardware based, software based, and channel based. The first class measures the hardware imperfections of the radio devices from the transmitted signals [86]. The second class is based on the software characteristics such as software type and used protocols. The last class related to the channel state information [23]. Most of the existing techniques are hardware based and channel based fingerprints. For instance, the feature vector has been used as fingerprint to identify the legitimate PU by extracting the phase noise from the received signal [87]. Moreover, the multi-resolution time frequency characteristic of the wavelet was used to extract the fingerprint from the transmitted signal. In [88], the log-likelihood ratio test and Neyman–Pearson detector were used as a fingerprint for the PU identification. In [89], the time of arrival was used as a fingerprint to determine when the legitimate signal arrived at two different nodes. By computing the difference in times of arrival of the received signals, the mean of correlation is used to estimate the transmitter's position with the accepted time of arrival.

3.3.3. Countermeasures based game theory

Game theory has been used to find the best strategy to secure the network against the attacker. Countermeasures based game theory models the interactions between the involved players, SUs and PUE attackers, competing to maximize their channel utilization. They aim at selecting the optimal strategy to defeat the strategy followed by the attacker using Nash equilibrium [90–93]. In [90], the authors adopted a differential game to find the best strategy for SUs to maximize their channel usability. In [91], the authors proposed a surveillance game using a network manager to control the unavailable channels. The malicious user and the network manager select their optimal strategies using Nash equilibrium. In [92], a game theory based defense technique was proposed where SUs can choose to use a channel or switch to another channel during an attack. The optimal strategy of the SU depends on the attacker's strategy. If the attacker attacks the network with such probability, SU is required to maximize its spectrum utilization by switching to a channel with a defined probability to avoid the attack. Furthermore, SUs can help PUs to enhance the network security and protect it against attacks. In [93], a cooperative transmission method based on Stackelberg game was proposed to coordinate between the PU and SUs for common objectives, which are maximizing the data rates and the network's security.

3.3.4. Hybrid defense

Hybrid defense approaches combine the previously mentioned countermeasures to efficiency identify malicious users in a network. These techniques have been proposed to address the limitations of existing individual techniques by combining different methods to authenticate the PU. For instance, the authors in [48] proposed a hybrid defense technique that combines energy and variance detection techniques for mobile SUs and a fixed PU. In [94], a PU authentication method was proposed using a helper node for cryptographic signatures. It consists of authenticating the legitimate PU by the helper node and then broadcasting the encrypted spectrum sensing data to the SUs. It allows protecting the legitimate PU signal from adversary, but it needs a dedicated helper node to operate as an authentication and broadcasting entity.

4. Belief manipulation attacks

Belief manipulation attacks perform by manipulating the radio parameters leading to wrong sensing decisions. Threats belonging to the belief manipulation attacks category are based on learning algorithms such as genetic algorithms and hill climbing algorithms [95]. They have been used mostly in cooperative spectrum sensing where a malicious user launches a cheating and fooling attacks against SUs. This category includes two main threats: spectrum sensing data falsification [28,31] and objective function [58], as illustrated in Fig. 5.

4.1. Spectrum sensing data falsification attacks

4.1.1. Attack description

Spectrum sensing data falsification (SSDF) attack, also called Byzantine attack, is mainly related to cooperative spectrum sensing when several SUs are collaborating to sense a specific frequency band [28,31]. It consists of providing false spectrum sensing results by malicious users in order to gain control and degrade the performance of the network [55,95]. For instance, a malicious user can spread a false signal into the network when SUs use high modulation rates, which forces the SUs to perform using low modulation rates. As a result, SUs will believe that avoiding interferences requires operating at low modulation rates. Based on this

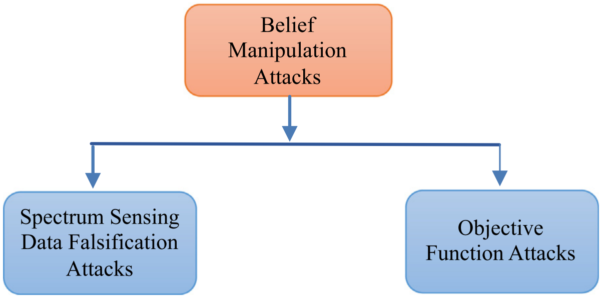
Belief Manipulation Attacks
Spectrum Sensing Data Falsification Attacks
Objective Function Attacks

Fig. 5. Belief manipulation attacks.

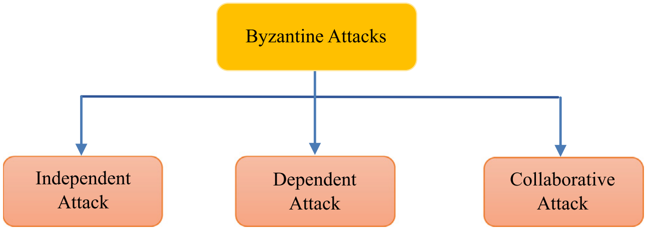

Fig. 6. Classification of Byzantine attacks.

experience, SUs will avoid using higher modulation rates [29]. As SUs exchange the sensing results very fast in distributed spectrum sensing scheme, the spectrum sensing data falsification attack is considered more harmful compared to the centralized spectrum sensing scheme where the fusion center can control the false information propagation [96]. In this last scheme, the attackers send false sensing data to the fusion center leading to wrong sensing decisions. Due to the important role of the fusion center in the cooperative spectrum sensing, the malicious users attack this node by sending wrong sensing data resulting in high sensing error rates, and thus available frequency channels are announced occupied [59]. In [97], the authors classified the Byzantine attacks into three categories based on the attacker's model: Always yes, always no, always false model. In the always yes model, SUs report the presence of the PU activity. In the always no model, SUs declare the absence of the PU activity. In the always false model, SUs declare false observation of the PU state. Moreover, Byzantine attacks can be also classified into three categories based on the attackers strategy: independent, dependent, and collaborative attacks as illustrated in Fig. 6 [98].

With independent Byzantine attack, each malicious user performs its own sensing measurements. With the dependent Byzantine attack, attackers exchange their sensing measurements while they collaborate for the final decision under a collaborative attack. Dependent and collaborative attacks allow minimizing the probability of being disclosed by legitimate SUs while they require attackers to exchange their sensing measurements in advance [99]. Fig. 7 illustrates an example of Byzantine attack where SUs are performing the spectrum sensing with the presence of malicious users.

4.1.2. Detection methods

A number of detection techniques have been proposed allowing identifying the spectrum sensing data falsification attacks [47,59,101–103]. These techniques include user's reputation based [101,104], CatchIt onion peeling [89,103], and data-mining based [59].

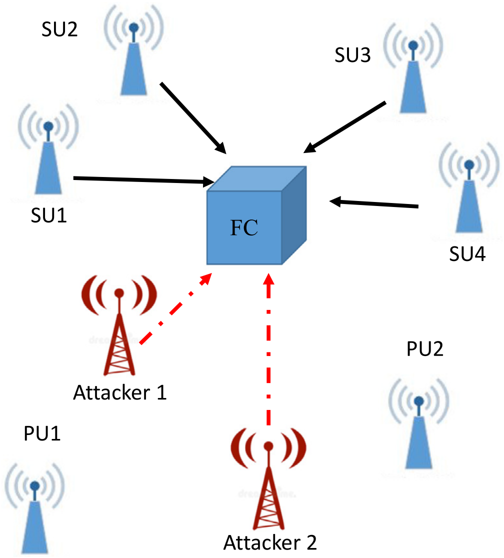

Fig. 7. Example of a Byzantine attack [100].

4.1.2.1. User's reputation based. These detection techniques are based on the reputation of users to identify their identify and trust their transmitted data. For instance, a distributed spectrum sensing method was proposed to protect the final sensing decision from being falsified at the fusion center [101]. It consists of defining tolerate bounds of the false alarm and misdetection probabilities and considering the past behavior history of individual SUs. It performs using two metrics: weight decision and user's reputation. A weight decision is derived from the Wald's sequential probability ratio test as a function of the user's reputation. The user's reputation is then incremented or decremented based on the previous behavior of the user and the decision variable. When the weight decision is included within the tolerate range of the false alarm and the misdetection probabilities, the correct decision corresponds to that weighted decision variable.

4.1.2.2. CatchIt onion peeling. CatchIt onion peeling detection techniques consist of evaluating the level of trust of all users and eliminate suspicious users at each round. In [102], the authors proposed an approach called CatchIt onion peeling to preserve the detection decisions accuracy in centralized cooperative spectrum sensing scheme with the presence of attackers. This technique consists of computing the probability that an involved user is malicious by calculating the suspicious level of all the involved users at every time slot. If the suspicious level of a user is greater than a predefined threshold, the user is considered malicious. Thus, the fusion center excludes the data coming from that particular user. The algorithm is repeated till all the malicious users are eliminated. An extension of the work proposed in [103], was presented in [47] when a Bayesian based detection was applied to progressively exclude all malicious users using previous history [105].

4.1.2.3. Data mining based. Data-mining based detection techniques enable the prediction of malicious activities in the network by searching for anomalies and behavior history of all users. In [58], a data-mining algorithm, called k-proximity, was used to detect non-cooperative malicious users with the presence of the fusion center. It consists of finding the extreme data from the behavior history space. When the behavior history of a particular user is very close or very far from the other users' histories, this user is considered suspicious.

4.1.3. Countermeasures

Various countermeasures have been proposed to cope with spectrum sensing data falsification attacks. These techniques can be classified according to which metric is used to decide about the users identity: reputation and trust.

4.1.3.1. Reputation metric based. In [106], a novel technique was proposed to face this attack allowing the fusion center to distinguish legitimate SUs from attackers. As an intelligent component, the fusion center is able to identify the malicious users and exclude them from the list of trusted SUs in a short period of time. The proposed approach consists of comparing the reputation metric of each user transmitting data to the fusion center to a predefined threshold. If the reputation metric of a user is greater than that threshold, the fusion center does not consider its sent data and remove it immediately from its trusted users' database.

4.1.3.2. Trust metric based. Preventing spectrum sensing data falsification attack consists of detecting illegitimate sensing reports and discarding them during the final detection decision by the fusion center [107]. It allows building the SUs trust, which represents the degree of belief that a user can be trusted and its sensing reports are not malicious. Trust mechanisms consist of assigning initial reputation values to all SUs, which is updated after each spectrum sensing round. Low weights are assigned to SUs with malicious behavior in order to exclude their reported results at the fusion center. In [108], the authors proposed an outliers detection technique to identify suspicious sensing reports in cooperative spectrum sensing. Examples of outliers that can be used are mean and standard deviation of the energy of the sensing signals [109], correlation between the sensing reports [110], Euclidean distance between SUs [111], and decorrelation distance [112]. In [29], a trust based anomaly monitoring technique was proposed to prevent the Byzantine attacks in cognitive radio networks, especially in ad hoc networks. It consists of assigning trust values by each user to its neighbors sharing spectrum occupancy results. This trust value represents the trustworthy of a user in sharing its spectrum occupancy reports. This technique aims to ignore reports coming from malicious users, but not exclude them. In [113], the authors proposed to adopt predefined references to detect any anomalies in the reported measurements. These references represent normal activities performed by legitimate SUs in advance, which will help to identify malicious users and ignore their reported data.

4.2. Objective function attacks

4.2.1. Attack description

Objective function attacks consist of manipulating the radio parameters while computing the objective function by SUs and modifying the results to accommodate the attacker's interests [54]. SUs use several parameters to calculate their objective function. Examples of these parameters are: bandwidth, modulation type, frame size, coding rate, center frequency, encryption type, and power [43]. SUs manipulate these radio parameters over time in order to reach their goals: high rate, low power, and secure communication. For instance, SUs compute these radio parameters to figure out what the parameters are to maximize the data rate and minimize the signal power. This parameter computing is based on a multi attributes channel quality ranking mechanism [114]. When SUs are launching the radio parameters computing, the attackers interfere by taking the control of the results in accordance to their own benefits [86]. Consequently, the attackers can make the SUs believe that a radio parameter, center frequency as an example, is not optimal and must be ignored.

An extension of the objective function attack was presented in [43], called malicious behavior attack, to allow teaching a user how to become unconsciously malicious. The authors presented a scenario where an SU has been taught to behave as a jammer. The scenario consists of a PU occupying the spectrum and SUs sensing that spectrum using spectrum sensing techniques. The PU and SUs use an objective function to equilibrium the throughput with the interferences level by maximizing the throughput while minimizing the level of interferences. The attacker sends a jamming signal undetected by the SU and decreases the throughput when the PU is absent. Consequently, SUs learn that they can use the spectrum only when the PU is present to achieve high throughput, which makes these SUs act as jammers.

4.2.2. Detection methods

Detecting objective function attacks consists of verifying all the radio parameters values [115,116]. Examples of detection techniques include optimization, intrusion detection system, alarm, and voting based techniques.

4.2.2.1. Optimization, intrusion detection system, and threshold based. In [114], a multi-objective programming method was proposed to verify all the radio parameters and then adapting when solving the objective functions online. The algorithm is based on particle swarm optimization to find the optimal values of the radio parameters. It allows preventing malicious users from adapting these new radio parameters values. In [117], a defensing strategy was proposed by defining thresholds for each radio parameter. The network detects an attack when a radio parameter does not respect the threshold value and the communication is broken. In another work, the authors suggested to get help from an intrusion detection system to cope with the attack.

4.2.2.2. Alarm and voting based. In [118], the authors proposed an alarm based detection technique to mitigate the objective function attacks by embedding detection thresholds at each SU node according to the distance between SUs. The attacker cannot guess all the thresholds of all the SUs neighbors, which enable the generation of an alarm to the other SUs. While the authors in [119] proposed to use the voting rule between the SUs neighbors to detect the attacker. Each SU collects the sensing measurements from its immediate SUs neighbors and votes about the neighbors legitimacy by computing the mean of the reports. The votes are then exchanged between neighbors to classify users with more than the half of votes as malicious.

4.2.3. Countermeasures

Several solutions have been proposed to deal with the objective function attacks. In [120], SUs adopted a high level security in order to protect the radio parameter learning's process. However, the malicious user can react immediately by starting a jamming attack on the system, which decreases the objective function. Consequently, SUs cede the high security to avoid reducing the objective function. In [121], the authors argue that there is no such solution to mitigate this attack and protect SUs than selecting a list of thresholds for each radio parameter before running the learning process. The communication has to be stopped when a parameter is not up to the fixed threshold value. In [43], the authors presented a scenario where legitimate SUs try a number of parameters as inputs to measure the bit error rate. Then, legitimate SUs evaluate the objective function to find which parameter is giving the best results. At the parameters learning stage, the attackers can interfere in the process by manipulating the objective function and forcing low security level, which can be easily broken. In addition, most these countermeasures are suitable for small-scale centralized schemes with high computational complexity [122]. In [115], the authors proposed a defending technique based on the differential game for large scale where the networks data corresponds to Big data.

5. Eavesdropping attacks

In radio frequency and broadcast wireless communications, attackers can tune their receivers to the proper frequency to intercept signals broadcasted by legitimate users and overhear the information transmission. As a result, junk messages can be injected into the network [123].

5.1. Attack description

In cognitive radio networks, eavesdroppers can easily listen and access to the transmitted messages by SUs as the wireless communication is performed using open medium. Eavesdropping attack may be performed at the physical layer [124,125] or at the network layer [126]. Fig. 8 represents an example of a system model of the physical layer security under eavesdropping attack where Alice is transmitting confidential information to Bob while Eve is listening to their communication channel [127].

Eavesdropping attacks can be classified into two main categories: active and passive [129]. An active eavesdropping attack performs by reacting after overhearing the confidential information. The eavesdropper launches a reply or impersonation attack to establish communication with PU using fake identity. The presence of fake PU is then declared over the network. A passive eavesdropping attack refers to eavesdropping when the channel state information of eavesdropper is unknown for the transmitter SU. The eavesdroppers operate silently to spy on the wireless transmission to extract confidential information for malicious purposes [130–134]. Passive eavesdroppers can be visible or hidden. Hidden eavesdroppers only read and listen to the network using passive receivers without injecting malicious signals into the traffic, which makes it difficult to detect these attackers. Although these passive receivers may emit very weak radio frequency signals, these signals can be buried and missed by the current radio devices. An eavesdropper can switch between active and passive attacks to achieve its purposes. An attacker performs a passive attack by operating offline to read confidential information or an active attack by operating malicious activities online such as modification of the security policy, installation of malware software, or injection of jamming messages over the traffic.

5.2. Detection

Eavesdropping attacks are usually addressed using cryptography solutions by implementing cryptographic algorithms at the application layer. However, these approaches cannot be always efficient when it is not possible to distribute the cryptographic key [135]. Consequently, physical layer security is important to efficiently handle these attacks by exploiting the channels characteristics. A number of parameters were used to detect the eavesdropping activities in the network, including secretary capacity [136], power constraint, secrecy outage probability, and leakage probability. In [137], the authors proposed a secretary system of wiretap channel model to allow legitimate transmitter sending confidential information to legitimate receiver with the presence of eavesdroppers. This secretary system consists of performing data transmission below a predefined transmission secretary rate. This secretary capacity refers to how much information the legitimate users and the eavesdropper share. In [138], the authors enhanced the transmission security against passive eavesdropping by imposing that the PU interference power and the SU maximum transmitted power do not exceed predefined thresholds. The impact of these two power constraints leads to computing a new expression of the secrecy outage probability to detect eavesdroppers in the network [139]. A security gap was used to detect eavesdropping attacks, which is the ratio of the legitimate receiver's SNR with low bit error rate to the eavesdropper's SNR with high bit error rate. Secure transmission is achieved with small security gap [140]. In [141], the leakage probability was used to detect eavesdropping activities over SUs transmission. It is the probability that the attacker had accessed the confidential information with a probability of error lower than its bit error rate. Regarding the passive eavesdropping attack, the authors of [142] designed a new device, called Ghostbuster, able to detect leak signals under ongoing noisy transmission. This device allows detecting hidden presence of eavesdroppers in a wireless network.

5.3. Countermeasures

Preventing eavesdropping attacks requires minimizing the capacity of the channel between a transmitter and an attacker, called the wiretap channel, while maximizing the capacity of the channel between the transmitter and the receiver [143]. To achieve this goal, a number of countermeasures and prevention techniques have been proposed, as illustrated in Fig. 9, including relay based [144], multi antenna based [145], security oriented beamforming [146], artificial noise aided [147], and spoofing based techniques [148].

5.3.1. Relay based

Relay based techniques consist of employing multiple relays to relay signals to the legitimate SUs while avoiding eavesdroppers when the channel state information of the legitimate and the wiretap channels are known. When the channel state information is unknown, a relay with a high capacity is involved to assist the signals transmission by forwarding the received signals to the legitimate receiver. The relay performs using an amplify and forward technique or a decode and forward technique in cooperative schemes [149]. With an amplify and forward technique, the relay amplifies and retransmits the received noisy signal to the legitimate SU. Amplifying the received signal adds more noise to it which may degrade the performance of the signal decoding at the legitimate receiver. With the decode and forward technique, the relay first decodes the received signal and then transmits the decoded signal to the legitimate SUs [150].

5.3.2. Multi antenna based security oriented beamforming

Multiple antenna based techniques are based on multiple input multiple output (MIMO) and the multipath propagation to increase the link capacity. Using multiple antennas to transmit and receive signals increases the capacity of the channel and prevent eavesdropping attacks [151].

Security oriented beamforming techniques perform by sending signals in a specific direction to the receiver for high capacity channels with less interferences than the wiretap channels. These beamforming based approaches allow the transmitter and the receiver to transmit signals in specific direction [152].

5.3.3. Artificial noise injection

Artificial noise injection techniques consist of creating interference to the eavesdropper by generating an artificial noise to decrease the capacity of the wiretap channel and increases the secrecy capacity of the legitimate channel [153]. These techniques require the knowledge of the eavesdropper and need more energy to generate the artificial noise. Relay based and artificial noise based techniques can be combined for better results. Instead of forwarding the received legitimate signal, the relay generates an artificial noise or interferences in order to prevent eavesdropping attacks.

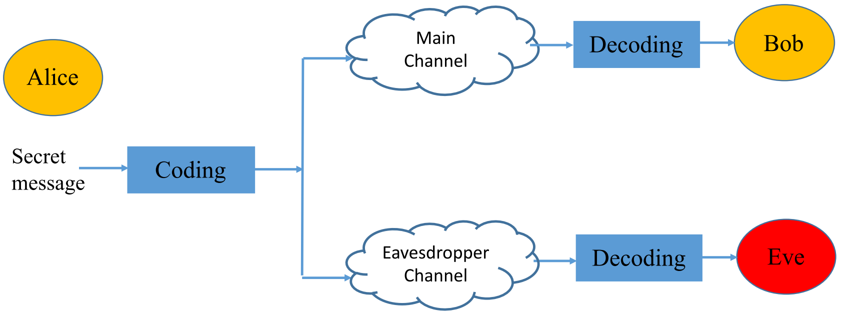

Fig. 8. Example of eavesdropping attack [128].

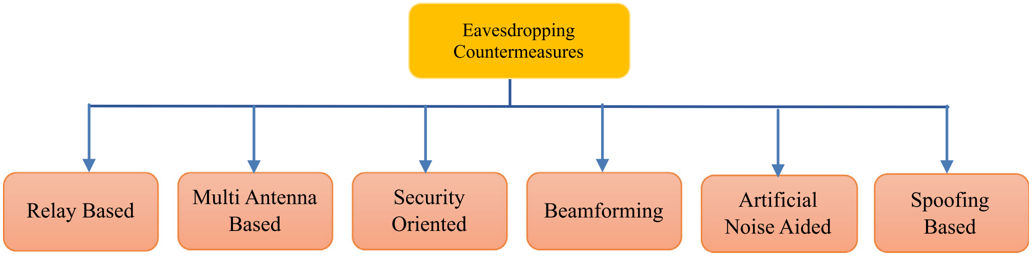

Fig. 9. Eavesdropping countermeasures.

5.3.4. *Spoofing based techniques*

Instead of developing prevention techniques against eavesdropping attacks, the authors of [153] focused on analyzing and evaluating the eavesdropping behavior in order to better protect a wireless transmission against eavesdropping attacks. In [154], the authors proposed a defense technique based spoofing to help legitimate users protect their confidential transmitted information against eavesdropping attacks. This technique performs by using a spoofing node to emit falsified signals over the network to mask the main signals. Spoofing rate and spoofing probability were used as metrics to evaluate the performance of the proposed technique. Preventing network eavesdropping attacks requires strong authentication protocols in order to ensure no passwords are transmitted over the network. Kerberos protocol is an example of these strong authentication protocols [155].

6. Malicious traffic injection attacks

Malicious traffic injection attacks consist of injecting junk messages into the network causing network congestion. They aim mainly at consuming high bandwidth prohibiting the legitimate users from using the network resources. The malicious users send continuously and simultaneously junk packets to the network, leading to denial of service in the network [156]. Malicious users can also target a channel dedicated for exchanging the spectrum sensing results between the different SUs. SUs subject to these attacks are obstructed from transmitting or receiving data, which interrupts the spectrum sensing process [157]. Active eavesdropping attacks can also classified under the malicious traffic injection attacks as the eavesdropper can inject fake messages into the network after accessing the communication channel.

6.1. *Jamming attacks description*

Jamming attacks consist of broadcasting high energy signals continuously to hamper legitimate users and force them to receive these junk packets consuming high bandwidth leading to deny of service in the network [29]. They can perform by spreading flat spectrum power in the jamming band or by generating sinusoidal waveforms on the jamming tone, which is the target carrier frequency. This strategy is more expensive in terms of hardware but more disruptive. Jamming attacks can be classified into four categories based on the attacker's state: constant jammer; (ii) deceptive jammer; (iii) random jammer; and (iv) reactive jammer [158]. A constant jammer sends continuous signals to corrupt transmitted signals over a targeted channel [159]. A deceptive transmits streams similar to the legitimate user' traffic. A random jammer swaps between sleep and jamming mode in order to save energy. Reactive jammer targets particular channels during the sensing, which results in data collisions [4,160]. Moreover, jamming attacks can be classified into three main categories according to which band is targeted, namely: broad band, partial band, and a narrow band [161]. Broad band jamming attacks target the entire radio spectrum and require more energy. Partial band jamming attacks target a portion of the frequency band. Narrow band jamming attacks target only a small and specific portion of the spectrum [162].

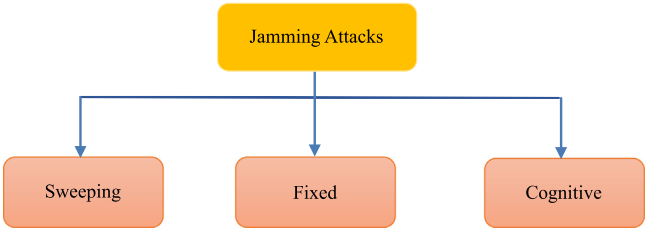

Fig. 10. Jamming attacks.

Moreover, jamming attacks can be classified into three types based on how the attacker selects the channel to attack: sweeping [163], fixed [164], and cognitive strategies [165], as shown in Fig. 10.

With a sweeping strategy, the attacker launches the jamming attack on a random channel without checking its state or activity. When transmitting junk messages on free channels, SUs signals are not affected by any interference, which wastes the attacker's resources [166]. With a fixed strategy, the attacker senses the spectrum to find the channel being used by the SUs. Then, the attacker generates an interfering signal to transmit it on that identified channel. However, SUs continuously perform the spectrum sensing to identify free and better channels and switch to them, which may deceive the attacker [167]. With cognitive strategy, the attacker is aware of its environment with cognitive radio embedded, which implies that the attacker can identify the channel being used by SUs even after they switch to better one [168].

6.2. Detection methods

Several types of detection techniques have been proposed, including intrusion algorithms, game theory, and machine learning. In [169], the authors investigated the efficiency of intrusion detection systems in detecting illegitimate activities over the network to assess the secrecy and the reliability of a transmission under jamming or active eavesdropping attacks. Game theory has been used through two games: basic and extended games to analyze the network. Basic game consists of analyzing the behavior of any suspicious users while extended game aims at modeling the interactions between the legitimate transmitter and the suspicious users. Combining the stochastic game theory with the intrusion detection system allows detecting efficiently any malicious activities in the network. In [170], the authors proposed a novel jamming attacks detection technique based on machine learning to successfully detect malicious users. The proposed approach allows detecting the state of the transmission link between SUs based on its features, namely bad packet ratio, packet delivery ratio, received signal strength, and clear channel assessment. The proposed approach achieves high detection rates with less resources and processing time.

6.3. Countermeasures

There are two possible ways to countermeasure jamming attacks: escape the denial of service or spatial retreat. The first method applies the frequency channel hopping by scanning different channels in order to detect the attack. The second method consists of changing the spatial location of the legitimate users to escape from the interferences created by the attacker. Legitimate users are required to leave the range of frequencies occupied by the attacker while keeping a reasonable distance between them in order to continue communicating. Countermeasures against jamming attacks can be classified into four main categories: hopping [179], location based [180], directional antennas [181], and spread spectrum [182]. Information hopping techniques can be performed by switching channels or frequency during spectrum sensing process. It is used when SUs switch to better channels when detecting that the previous channel is under attack. When a SU detects that the channel is under jamming attack, the information is forwarded to the other SUs and the hopping information is exchanged over a shared safe control channel [183]. Location based countermeasures perform by finding the location of the attacker in order to prevent its interferences. Appropriate security actions can be easily taken by SUs when the position of the attacker is known [184]. Directional antennas based prevention techniques direct the transmission in the direction of the legitimate receiver in order to minimize the level of intentional and unintentional interferences in the network. Spread spectrum based countermeasures techniques consist of transmitting over a wideband spectrum in order to increase the resistance against interferences [185,186]. These countermeasures can be classified into three main categories: direct sequence spread spectrum, frequency hopping spread spectrum, and hybrid technique. Direct sequence spread spectrum performs by multiplying the RF incoming signals with a pseudo noise signal, which is a pseudo random sequence of ±1 with frequency higher than the frequency of the signal to transmit. This multiplication makes the signal noisy in a wide bandwidth, but it ensures filtering the noise from the signal at the receiver. Frequency hopping spread spectrum performs by switching the frequency among many other frequencies to transmit signals. The frequency switching is performed using a shared algorithm between the transmitted and the receiver. Hybrid spread spectrum combines the two countermeasures for effective defense against jamming attacks.

Moreover, other defense strategies have been proposed over the literature. For instance, in [60], a cooperative defense based multi-tier proxy technique was proposed to face cooperative jammers trying to break down the communication in a centralized scheme. It consists of computing the spectrum availability rates of each user, where users are followers or proxy users. Proxy users behave like a relay between the followers and the base station. This collaborative defense strategy follows these steps: follower users connect to the proxy users, proxy users forward the connection to the base station, and then proxy users rely the base station to the followers. It allows improving the spectrum availability rates and effectively avoid jamming attacks. In [156], the authors proposed an optimal sensing disruption method performs by determining the channels targeted by the attacker as well as the attacker's transmission power assuming the attacker has a limited power budget. This strategy allows each legitimate SU to transmit with a power higher than the power budget of the attacker over all the channels resulting in high false alarm rates. An extension to this work [156] was presented in [157] by studying the tradeoff between jamming and spoofing threats and how the attacker alternates between them. The jamming is performed by emitting energy to prevent legitimate users from initiating a communication over a radio frequency while spoofing is performed by launching energy to cause incumbent emulation over the spectrum sensing process. The power budget controls the attacker's reaction toward the network to maximize the network damage. The demand of spectrum is variable, which makes the SUs' number changing over time between higher and lower values. Jammer shifts to spoofer when the SUs' number increases and shifts to jamming when the SUs' number decreases. As a result, the attacker wastes its power budget in alternating between jamming and spoofing [158,159].

In [29], an anti-jamming strategy, named dogfight, was proposed when channel statistics are unknown in order to solve the blind dogfight problem radio spectrum [187]. It involves two groups of users: defenders (SUs) and attackers (jammers). Jammers observe the channel and forward these data to the defenders, but defenders cannot help the jammers. In the same context, an anti-jamming based on stochastic game and minimax-Q learning was proposed to allow SUs to gradually learn the optimal defense strategy. It performs by observing the channels along the game getting the spectrum utilization, the attacker's strategy, and the channel quality. Based on these results, SUs decide about the safe channels to switch between them and transmit their data [163,164]. In [188], the authors proposed to model the interactions between the SUs and the jammers as a stochastic game in order to maximize the throughput of the SUs. SUs observe and sense the spectrum to check the availability and the quality of the channels as well as the strategy followed by the attacker. Based on the sensing results and the jammer behavior, SUs decide which channels to keep or which channel to switch to in order to update their data and control channels database. Because these techniques rely on observations of jammers behavior, they are more robust against jammers than the previous ones. Moreover, countermeasures for active eavesdropping attacks may be also used to prevent jamming attacks by enhancing the throughput of the transmission link.

Table 1
Physical layer attacks comparison.

Attacks	Description	Attack results or outcomes	Impacts	Impacted security requirements
PU emulation	Imitation of PU signal characteristics	-Prevent SUs from accessing the PU channel	-Unable to distinguish between PU signal and attacker signal -Work in multiple channels -Active attacks	-Availability
Spectrum sensing data falsification	Sending wrong spectrum sensing results	-Lead SUs to wrong sensing decision	-Causing interferences to PUs -Active attacks	-Availability -Integrity
Objective function	Manipulate the radio parameters to minimize the objective function values	-Maximizing the data rate -Minimizing the signal power	-Wrong decisions	-Availability
Eavesdropping	Overhearing signal transmission	-Get access to exchanged confidential information	-Inject junk messages -Install malware software -Active attacks	-Confidentiality
Jamming	Broadcasting signals	-Prevent SUs from accessing resources-Delay functioning of the network -Denial of service	-Causing network congestion -Preventing users from sending/receiving data	-Availability

Table 2
Detection techniques comparison.

Attacks	Detection methods	Advantages	Limitations
PU Emulation	Energy detection based [44]	-Easy to implement -Low complexity -Prior knowledge about PU energy is not required	-Not appropriate when attacker can mimic PU parameters -Inefficient spectrum sensing technique (Energy detection) is used -Limited to fixed PUs -Helper nodes are required [46]
	Matched filter based [45]	-Robust against noise	-PU characteristics can be emulated easily -Requires prior knowledge about PU signal -Cannot distinguish between the legitimate PU signal and those of the malicious user
	Cyclostattonary based [45]	-Robust in detecting PU signal	- PU characteristics can be easily emulated
	Belief propagation based [47–51]	-No need for expensive hardware -Low complexity -Belief convergence -Low processing time [49]	-High number of collaborators is required -Untrusted collaborative users -Not efficient in fading environment -Fixed threshold -Unknown and variable distance between PU and attacker
	Localization-based [24,47–49]	-Malicious user with inconstant transmission power is considered -High detection rates when long distance between PU and attacker -Less complexity -Incumbent signal modification -Respect FCC requirements [171] -Detection rates improved -Malicious users' location not always required	-Synchronization required -Not appropriate for mobile PU -High number of collaborators is required -Trusted collaborators are required -Separate sensors is required -Attacker's transmission power required to be constant -Received signal strengths metric - Not efficient in fading environment -High processing time
	Non-location-based [22,55]	-Authentication protocol and channel impulse response -Based cryptographic signatures -Distinguish between the signal activity pattern of a legitimate PU the attacker	-Additional helper node is required -No PU information is required -Information about signal activity required
	Database assisted based [39,61]	-FCC requirements are respected -No modification of PU signal -No synchronization or hardware algorithms are required	-High processing time -Short distance between PU and malicious user is assumed -High memory storage is required -Based historical results
	Feature-based [58,59]	-No synchronization or hardware algorithms are required	-Signal features can be emulated -Prior knowledge about PU is required
	Learning-based	-High detection rates -Low false alarm rates	-Suitable dataset training and testing is required for learning
	Intrusion detection system based [63,64]	-No centralized IDS is required -Allow learning normal and abnormal network's behavior -Used to detect PUE and other attacks	-High false alarm rates -High memory required
	Compressive sensing [79,172]	-Fast detection -Less number of sensors	-Information may be lost after recovery -Efficiency decrease due to compression

(*continued on next page*)

Table 2 (*continued*).

Attacks	Detection methods	Advantages	Limitations
Spectrum sensing data falsification	Reputation based	-Multiple attackers are considered -Robust distributed spectrum sensing	-Based on past behavior history -Reputation metric depends on the fusion center's output, which can be faulty -Reputation metric is not restored
	CatchIt onion peeling [56,173]	Centralized cooperative scheme supported	-Predefined threshold -High processing time
	Bayesian based [45]	Centralized cooperative scheme supported	-Predefined threshold -High processing time -Based on previous history
	K-proximity based [53]	-Data mining advantages	-Only non-cooperative users are considered -History based
Objective function	Based threshold	-Easy to implement -Compare each radio parameter with threshold value	-Fixed threshold -Online
	Intrusion detection system	-No centralized IDS is required	-High false alarm rates -High memory storage is required
	Particle swarm optimization based [83]	-Genetic algorithms advantages [174,175]	-Online
	Alarm or voting based	-Cooperate immediate neighbors -Robust	-Threshold based -Distance between SUs required
Eavesdropping	Cryptography	- Cryptographic algorithms advantages	-Not always efficient -Implementation complexity
	Channels characteristics based	-Efficient -Works for passive and active attacks	-Threshold based -High complexity
Jamming	Frequency hopping [17]	- Low complexity -Suitable for static/dynamic spectrum allocation -Different hopping sequences are used by each node	- Only half duplex is considered
	Spatial retreat	-Location-based -Suitable for static/dynamic spectrum allocation	-Legitimate users are required to leave the range of frequencies occupied by the attacker -Legitimate users are required to keep a reasonable distance from the attacker

7. Comparison and discussion

Each physical layer attack is characterized by certain features, strengths, and weaknesses. Table 1 compares these attacks by highlighting their consequences, strengths, features, and impacted security requirements.

Table 2 compares the different detection techniques by highlighting their advantages and limitations.

Table 3 discusses the different defense techniques to counteract each attack by highlighting their advantages and disadvantages.

8. Challenges and future directions

8.1. Challenges

A number of detection and defense methods have been proposed in order to enhance the security over the physical layer of cognitive radio networks. These methods are related to the available information about the involved users, primary, secondary, and malicious [189]. Despite these efforts to address and to mitigate the issues imposed by the attackers, physical layer's security still presents a number of challenges [34]. For instance, localization based techniques rely on the PU location knowledge, which is not always available in real scenarios. Advanced anti-jamming methods require higher energy consumption and design complexity, which limit their efficiency [190]. For cryptography based techniques, they are under resource constraint such as power and bandwidth. They also require running the same protocol by PU and SUs on the same layer for authentication. For example, SUs use TCP/IP protocol suite while PUs, example of TV towers, do not use that protocol suite [191]. Thus, cryptography based solutions require trusted and secure highly infrastructure. Authentication based techniques are also constrained by the FCC requirements that impose no modification of the PU signals [192]. Therefore, it is not possible to directly apply techniques modifying the PU signal and using cryptography. Strategies based on intrusion detection systems require high memory capacity to process and analyze the flowing traffic, which excludes SUs with restricted memory. They also represent high false alarm rates causing additional network overhead. Note that users can be highly mobile in real scenarios and thus the channel state information cannot be used for PU authentication because the introduced noise by the hardware is random. Considering multiple classes of PUs with different signal activity patterns is also a challenge. It is not practically possible to protect a simple SU engine from detecting an attacker as the legitimate PU, which requires developing efficient spectrum sensing techniques with low probability of false alarm rates [193]. Furthermore, developing spectrum sensing techniques able to distinguish signals coming from a legitimate PU from signals coming from a malicious user is a must. Additionally, protecting SUs during their learning stage is challenging and requires algorithms to prevent the adversary users from changing the SU's beliefs. For fingerprint based techniques, devices record the fingerprints for identification, tracking, and cloning detection. Malicious devices can pretend to be known or unknown by hiding their real identity with genuine fingerprints. They can use an e-password to clone the PU engine by generating fingerprints using a device of external appearance similar to the PU device. This attack is feasible and cannot be successfully detected without using arbitrary waveform generators or certain software defined radios [49,194]. It also requires additional software and hardware to implement.

For spectrum detection based techniques, they are not efficient in detecting malicious activities in the network. Energy detection based techniques are not efficient in sensing and cannot distinguish legitimate signals from noise. Matched filter based

Table 3
Defense techniques comparison.

Attacks	Defense methods	Advantages	Limitations
PU Emulation	Cryptography based [29,74,81]	-Confidentiality respected -PU authentication -Efficient -Key cannot be emulated -Mobile users are considered	-Does not respect FCC requirements -PU location required - Possible control channel congestion and wasted resources
	Fingerprint based [23,84]	-Efficient -Hardware fingerprint cannot be emulated -Hardware and software fingerprint are considered	-Channel state information can be emulated
	Game theory based [90]	-Game theory advantages -Optimal solution -Maximize data rates	-Mobile players required
	Hybrid [48]	-Combining other techniques advantages	-Complex -Mobile SUs and fixed PU are required
Spectrum Sensing Data Falsification	Trust based anomaly monitoring [29]	-Ad hoc networks considered	-Trust value assignment [176] -Fixed trust value -Malicious users are ignored but not excluded in the network
	Fusion center based [83]	-Able to distinguish legitimate SUs from attackers -Immediate response	-Reputation metric based [177] -Fixed threshold
	Reputation-based	-Central node and control channel are not required -Efficient	-High complexity -Inaccurate
Objective Function	Security level based	-Efficient	-Low security level is forced -Suitable for small-scale centralized schemes -High computational complexity
	Threshold based	-Simple	-Threshold selection -Fixed threshold -Online learning -Suitable for small-scale centralized schemes -High computational complexity
	Bit error rate based [43]	-Simple	-Attackers can manipulate the objective function forcing low security level -Suitable for small-scale centralized schemes -High computational complexity
	Differential game for large scale [103]	-Big data are considered -Game theory advantages	-High complexity
Eavesdropping	Relay based	-Efficient	-Multiple relays are required -Trusted relays are required -Channel state information of the legitimate and the wiretap channels are known -Amplify and forward technique add more noise
	Multi-antenna based	-MIMO technology advantages	-Multiple antenna are required
	Beamforming advantages	-Less interferences	-High complexity
	Artificial noise injection	-Efficient	-More noise is added -Knowledge of the eavesdropper required -Energy consuming
	Spoofing	-No need for anti-eavesdropping	-Strong authentication protocols required
Jamming	Multi-tier proxy based [58]	-Spectrum availability enhanced -Efficient in avoiding jamming attacks	-High complexity
	Optimal sensing disruption [98]	-Allow SUs to transmit higher power than the power budget of the attacker	-High complexity -High false alarm rates
	Tradeoff between jamming and spoofing [158]	-Wasting the attacker's power budget in alternating between jamming and spoofing	-Not suitable for fixed nodes
	Dogfight [29,178]	-Make the jammer help by observing and sending the channels information to the defenders	-Not suitable when channel statistics are known
	Stochastic game and minimax-Q learning based [91]	-Allow SUs to gradually learn the optimal defense strategy -Game theory advantages	-High false alarm rates

techniques cannot distinguish between signals coming from legitimate sources and those coming from malicious source. Cyclostationary based techniques are limited as malicious users can easily emulate the PU characteristics and behave like a legitimate PU [195]. For threshold based techniques, their efficiency depends mainly how this threshold is selected. Fixed and predefined thresholds to verify certain radio parameters limit the efficiency of these techniques. Adaptive thresholds can enhance these techniques [61], however these thresholds have to be measured which is challenging in some cases. For feature based techniques, attackers can easily emulate the legitimate PU signal features, which is another challenge for the network security [25]. Anti-eavesdropping systems allow detecting and blocking active attacks but passive eavesdropper can always keep listing in silent mode to get information to use for later analysis. Advanced anti-eavesdropping systems are required to be employed in the network in advance. Game theory based solution represent high complexity and require more players to perform. For trust, reputation, and secrecy metrics based techniques, they operate by assigning trust or reputation values to all users in advance and then update them after each round according to the attack detection reports. Assigning these values to users can be also corrupted and thus false metrics cannot be reliable. They also require more processing time to assign, compute, and update these security metrics at each round. In addition to the technical challenges, time varying wireless channels limit the efficiency of existing security solutions.

Regarding handling uncertainty in measurements, few works investigated the uncertainty impact of the network security [196, 197]. Thus, there is a great need for developing and investigating practical detection and defense strategies that can work with real network imperfections. For machine learning based techniques, models are trained in advance before the system is subject to any attack in order to acquire how to react when some known problems arise [198]. The learning process is restricted by the high training data growing with antennas number and the users' mobility over time and space. The cognition nature of SUs allows attackers to manipulate this nature for their benefits as cited in [43] "*Any radio that can learn from its environment can also be taught by its environment*", which is challenging. Thus, SUs should launch the learning process very carefully by avoiding permanent online learning and collaborate with to develop coherent beliefs against attacks.

8.2. Future directions

There are still many interesting open questions to be explored and that should be investigated in future works. For instance, current defense techniques are designed to withstand one of the existing attacks on the physical layer [199,200]. Thus, it is necessary to develop frameworks that detect and cope with all possible attacks. Combining mitigation techniques at the physical layer and the MAC layer could be a future research direction to overcome the limitations of security each layer. Techniques at MAC layer can feed SUs reliable information using cryptographic protocols in order to help them to learn and reason about their neighbors [201]. Thus, SUs can collect fair and specific details about each user and build a network database allowing quantifying how reliable neighbors are. Higher layers are less vulnerable to attacks compared to physical layer [202]. This idea can be a great future work to figure out how the higher security level can be spread over the different layers of the open systems interconnection model [25].

Localization based techniques depend on the information about the PU location, which is not possible in real scenarios [104]. Thus, it is necessary to develop advanced techniques that do not require the knowledge of the PU location. Cooperative based schemes use fusion rules to decide about the PU presence in the spectrum. OR, AND, and voting rules employed in distributed and centralized schemes could be exploited by the attackers to change the final decision [203]. More advanced fusion centers able to efficiently perform the sensing decision are required. In addition, in order to effectively mitigate any kind of attacks, it is very important to develop real time detection and defense strategies to address the attacks with minimum delays [21]. Moreover, existing works use simple cases where a single PU and a single cell are considered. Detecting an active threat in multi-cell and multi-user systems is one of the open research topics deserving investigation. With multi-cell and multi-user systems, existing detection strategies fail to distinguish attackers from different PUs. Finally, real implementation are required for testing the detection and the defense techniques in order to effectively investigate how to overcome the present challenges.

9. Conclusion

Security issues in cognitive radio networks arise due to the increase of the number of services and applications operating in networks. Security issues at the physical layer are critical and deserve more attention because of the importance of this layer in establishing a communication through physical medium. In this paper, we provided an analytical survey of the different physical layer attacks and their classification. We discussed the different detection and defense methods to face these attacks. We also presented some security challenges and future directions in order to highlight the growing interests for open research.

Declaration of competing interest

No author associated with this paper has disclosed any potential or pertinent conflicts which may be perceived to have impending conflict with this work. For full disclosure statements refer to https://doi.org/10.1016/j.phycom.2020.101001.

CRediT authorship contribution statement

Fatima Salahdine: Writing - original draft, Writing - review & editing. **Naima Kaabouch:** Writing - original draft, Writing - review & editing.

References

[1] F. Salahdine, H. El Ghazi, N. Kaabouch, W.F. Fihri, Matched filter detection with dynamic threshold for cognitive radio networks, in: International Conference on Wireless Networks and Mobile Communicationsommunications, 2015, pp. 1–6.

[2] N. Kaabouch, W.-C. Hu, Handbook of research on software-defined and cognitive radio technologies for dynamic spectrum management, IGI Glob. J. (2014).

[3] M.R. Manesh, S. Apu, N. Kaabouch, W. Hu, Performance evaluation of spectrum sensing techniques for cognitive radio systems, in: Ubiquitous Computing, Electronics & Mobile Communication Conference, IEEE Annual, 2016, pp. 1–6.

[4] M. Manesh, N. Kaabouch, Security threats and countermeasures of MAC layer in cognitive radio networks, Ad Hoc Netw. 70 (2018) 85–102.

[5] Z. Shu, Y. Qian, S. Ci, On physical layer security for cognitive radio networks, IEEE Netw. 27 (3) (2013) 28–33.

[6] Y. Saleem, M.H. Rehmani, Primary radio user activity models for cognitive radio networks: A survey, J. Netw. Comput. Appl. 43 (2014) 1–16.

[7] A. Celik, A.E. Kamal, Green cooperative spectrum sensing and scheduling in heterogeneous cognitive radio networks, IEEE Trans. Cogn. Commun. Netw. 2 (3) (2016) 238–248.

[8] M. Padmadas, N. Krishnan, V.N. Nayaki, Analysis of attacks in cognitive radio networks, Int. J. Adv. Res. Comput. Commun. Eng. 4 (8) (2015) 170–174.

[9] B. Wu, J. Chen, J. Wu, M. Cardei, A survey on attacks and countermeasures in mobile Ad Hoc networks, Wirel. Mob. Netw. Secur. (2007) 103–135.

[10] M. Kim, A survey on guaranteeing availability in smart grid communications, in: 14th International Conference onAdvanced on Communication Technology, 2012, pp. 314–317.

[11] W. Al Shehri, A survey on security in wireless sensor networks, Int. J. Netw. Secur. Appl. 9 (1) (2017) 25–32.

[12] R.Q. Hu, H. Chen, H.T. Mouftah, Cyber security for smart grid communications: Part I, IEEE Commun. Mag. 50 (8) (2012) 16–17.

[13] M. Bouabdellah, N. Kaabouch, F. El Bouanani, H. Ben-Azza, Network layer attacks and countermeasures in cognitive radio networks: A survey, J. Inf. Secur. Appl. 38 (2018) 40–49.

[14] R.C. Qiu, et al., Cognitive radio network for the smart grid: Experimental system architecture, control algorithms, security, and microgrid testbed, IEEE Trans. Smart Grid 2 (4) (2011) 724–740.

[15] W. El-hajj, H. Safa, M. Guizani, Brief Overview of Cognitive Radio Technology, 2012, pp. 1–18.

[16] K. Chauhan, A. Kumar, S. Sanger, Survey of security threats and attacks in cognitive radio networks, in: 2014 International Conference on Electronics and Communication Systems, 2014, pp. 1–5.

[17] S. Bhagavathy Nanthini, M. Hemalatha, D. Manivannan, L. Devasena, Attacks in cognitive radio networks (CRN) - A survey, Indian J. Sci. Technol. 7 (4) (2014) 530–536.

[18] A. Khare, M. Saxena, R.S. Thakur, K. Chourasia, Attacks & preventions of cognitive radio network- A survey, Int. J. Adv. Res. Comput. Eng. Technol. 2 (3) (2013) 1002-1006.

[19] B. Danev, H. Luecken, S. Capkun, K. Defrawy, Attacks on physical-layer identification, J. Immunol. (2010) 89–98.

[20] K. Anbukkarasi, Countermeasure against physical layer attack in cognitive radio networks, Int. J. Electron. Commun. Eng. (March) (2017) 195–200.

[21] N. Thalia, A Survey on Security Issues and Primary User Emulation Attack Detection Techniques in Cognitive Radio Network, 2005, pp. 10–15.

[22] B. Chen, G.K. Tummala, Y. Qiao, K. Srinivasan, In-Band wireless cut-through: Is It Possible?, in: ACM workshop on Hot topics in wireless, 2014, pp. 1–6.

[23] Y. Zou, J. Zhu, X. Wang, V. Leung, Improving physical-layer security in wireless communications using diversity techniques, IEEE Netw. 29 (1) (2015) 42–48.

[24] D. Kapetanović, G. Zheng, F. Rusek, Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks, IEEE Commun. Mag. 53 (6) (2015) 21–27r.

[25] Y.C. Yu, L. Hu, H.T. Li, Y.M. Zhang, F.M. Wu, J.F. Chu, The security of physical layer in cognitive radio networks, J. Commun. 9 (12) (2014) 916–922.

[26] G. Blinowski, The Feasibility of Launching Physical Layer Attacks in Visible Light Communication Networks, 2016.

[27] W. Fassi Fihri, F. Salahdine, H. El Ghazi, N. Kaabouch, A survey on decentralized random access MAC protocols for cognitive radio networks, in: 2016 International Conference on Advanced Communication Systems and Information Security, 2017, pp. 1–6.

[28] Z. Yuan, Z.S. Han, H. Li, J.B. Song, Routing-toward-primary-user attack and belief propagation-based defense in cognitive radio networks, IEEE Trans. Mob. Comput. 12 (9) (2013) 1750–1760.

[29] S. Bhattacharjee, S. Sengupta, M. Chatterjee, Vulnerabilities in cognitive radio networks: A survey, Comput. Commun. 36 (13) (2013) 1387–1398.

[30] D.X. Wang, P. Ren, Q. Du, L.S. Yichen, Signal conversion: Combat eavesdropping for physical layer security improvement, in: IEEE Vehicular Technology Conference, 2017, pp. 1–6.

[31] J. Ha, Physical Layer Security and Its Applications, KAIST Present, 2010, pp. 1–40.

[32] Y. Zou, J. Zhu, L. Yang, Y.C. Liang, Y.D. Yao, Securing physical-layer communications for cognitive radio networks, IEEE Commun. Mag. 53 (9) (2015) 48–54.

[33] J. Hernandez-Serrano, O. León, M. Soriano, Modeling the lion attack in cognitive radio networks, EURASIP J. Wirel. Commun. Netw. 2011 (2011).

[34] E.-K. Lee, M. Gerla, S. Oh, Physical layer security in wireless smart grid, IEEE Commun. Mag. 50 (8) (2012) 46–52.

[35] M.H. Yilmaz, H. Arslan, A survey: spoofing attacks in physical layer security, in: Proc. - Conf. Local Comput. Networks, LCN, vol. 2015–Decem, 2015, pp. 812–817.

[36] S. Parvin, F.K. Hussain, O.K. Hussain, S. Han, B. Tian, E. Chang, Cognitive radio network security: A survey, J. Netw. Comput. Appl. 35 (6) (2012) 1691–1708.

[37] X. Zhang, C. Li, The Security in cognitive radio networks: A survey, in: International Conference on Wirel. Commun. Mob. Comput., 2009, pp. 309–313.

[38] I. Gupta, O.P. Sahu, An Overview of primary user emulation attack in cognitive radio networks, in: IEEE International Conference on Computing Methodologies and Communication, 2018, pp. 27–31.

[39] R. Yu, et al., Securing cognitive radio networks against primary user emulation attacks, IEEE Netw. Mag. 30 (6) (2016) 62–69.

[40] Y. Wang, X. Xu, W. Wu, J. Bao, A primary user emulation attack countermeasure strategy and energy-efficiency analysis in cognitive radio networks, J. Commun. 12 (1) (2017) 1–7.

[41] D. Das, S. Das, Primary user emulation attack in cognitive radio networks: A survey, Int. J. Comput. Netw. Wirel. Commun. 3 (3) (2013) 312–318.

[42] M. Ammar, N. Riley, M. Mehdawi, A. Fanan, M. Zolfaghari, Physical layer security in cognitive radio networks, in: Int. Conf. Artificial Intelligence, Energy and Manufacturing Engineering, 2015, pp. 7–8.

[43] T.C. Clancy, N. Goergen, Security in cognitive radio networks: Threats and mitigation, in: 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008, pp. 1–8.

[44] A.W. Min, K.H. Kim, K.G. Shin, Robust cooperative sensing via state estimation in cognitive radio networks, in: 2011 IEEE Int. Symp. Dyn. Spectr. Access Networks, DySPAN 2011, 2011, pp. 185–196.

[45] W. Wang, H. Li, Y. Sun, Z. Han, Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks, EURASIP J. Adv. Signal Process. 2010 (2010).

[46] F.M. Salem, M.H. Ibrahim, I.I. Ibrahim, Energy detection based sensing for secure cognitive spectrum sharing in the presence of primary user emulation attack, IEEK Trans. Smart Process. Comput. 3 (6) (2013) 312–318.

[47] Z. Yuan, et al., Defeating primary user emulation attacks using belief propagation in cognitive radio networks, IEEE J. Sel. Areas Commun. 30 (10) (2012) 1850–1860.

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

[49] F. Salahdine, N. Kaabouch, Metrics for evaluating the efficiency of compressing sensing techniques, in: International Conference on Information Networking, 2020, pp. 1–6.

[50] F. Salahdine, N. Kaabouch, H.E. Ghazi, One-bit compressive sensing vs. multi-bit compressive sensing for cognitive radio networks, in: Proceedings of the IEEE International Conference on Industrial Technology, 2018, 2018.

[51] Y. Zhou, D. Niyato, H. Li, J. Song, Z. Han, Defeating primary user emulation attacks using belief propagation in cognitive radio networks, IEEE J. Sel. Areas Commun. 30 (10) (2012) 1850–1860.

[52] Z. Jin, K. Subbalakshmi, Detecting Primary user emulation attacks in dynamic spectrum access networks, in: IEEE International Conference on Communications, 2009, pp. 1–5.

[53] Z. Chen, T. Cooklev, C. Chen, C. Pomalaza-Raez, Modeling primary user emulation attacks and defenses in cognitive radio networks, in: IPCCC, 2009, pp. 208–215.

[54] R. Chen, J.-M. Park, J.H. Reed, Defense against primary user emulation attacks in cognitive radio networks, IEEE J. Sel. Areas Commun. 26 (1) (2008) 25–37.

[55] A.G. Fragkiadakis, E.Z. Tragos, I.G. Askoxylakis, A survey on security threats and detection techniques in cognitive radio networks, IEEE Commun. Surv. Tutor. 15 (1) (2013) 428–445.

[56] R. Chen, J.-M. Park, Ensuring trustworthy spectrum sensing in cognitive radio networks, in: Proc. IEEE Workshop Networking Technologies for Software Defined Radio Networks, Sept. 2006.

[57] Z. Jin, S. Anand, K.P. Subbalakshmi, Detecting primary user emulation attacks in dynamic spectrum access networks, in: Proc. IEEE International Conference on Communications, 2009, pp. 1–6.

[58] Z. Jin, S. Anand, K.P. Subbalakshmi, Detecting primary user emulation attacks in dynamic spectrum access networks, in: Proc. IEEE Int. Conf. Communications, 2009, pp. 1–5.

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

[60] C. Xin, S. Member, M. Song, S. Member, Detection of PUE attacks in cognitive radio networks based on signal activity pattern, 13 (5) (2014) 1022–1034.

[61] N.T. Nguyen, R. Zheng, Z. Han, On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification, IEEE Trans. Signal Process. 60 (2012) 1432–1445.

[62] D. Pu, Y. Shi, A.V. Ilyashenko, A.M. Wyglinski, Detecting primary user emulation attack in cognitive radio networks, in: IEEE Global Telecommunications Conference, 2011, pp. 1–5.

[63] R.K. Sharma, D.B. Rawat, Advances on security threats and countermeasures for cognitive radio networks: A survey, IEEE Commun. Surv. Tutor. 17 (2) (2015) 1023–1043.

[64] J. Soto, M. Nogueira, A framework for resilient and secure spectrum sensing on cognitive radio networks, Comput. Netw. 79 (2015) 313–322.

[65] R.Y. Guizani, Y. Zhang, Y. Liu, S. Gjessing, M. Guizani, Securing cognitive radio networks against primary user emulation attacks, IEEE Netw. Mag. 30 (6) (2016) 62–69.

[66] Z.M.F. Fouda, et al., Intrusion detection system (IDS) for combating attacks against cognitive radio networks, IEEE Netw. 27 (3) (2013) 51–56.

[67] L. Hung-Jen, R. Chun-Hung, L. Ying-Chih, T. Kuang-Yuan, Intrusion detection system: A comprehensive review, J. Netw. Comput. Appl. 36 (1) (2013) 16–24.

[68] S. Kar, S. Sethi, M.K. Bhuyan, Security challenges in cognitive radio network and defending against Byzantine attack: A survey, Syst. Distrib. 17 (2) (2016) 120–146.

[69] Y. Zhou, D. Niyato, H. Li, J. Song, Z. Han, Defeating primary user emulation attacks using belief propagation in cognitive radio networks, IEEE J. Sel. Areas Commun. 30 (10) (2012) 1850–1860.

[70] A. Phillip, A. Khisti, Y. Liang, S. Tomasin, Secure communications via physical-layer and information-theoretic techniques [Scanning the issue], Proc. IEEE 103 (10) (2015) 1698–1701.

[71] I. Hanen, K. Daimi, M. Saed, Security challenges in cognitive radio networks, in: Proceedings of the World Congress on Engineering, vol. 1, 2014, pp. 1–7.

[72] T. Selvapriya, S. Sharmila S. Sharmila, M. Sindhuja, V. Sinthuja, C. Jayasri, A database assisted detection against primary user emulation in cognitive radio network, Int. J. Innov. Res. Electric. Electron. Instrum. Control Eng. 5 (3) (2017) 1–6.

[73] T.D. Ganesh, Kumar, A survey on advances in security threats and its counter measures in cognitive radio networks, Int. J. Eng. Technol. 7 (2.8) (2018) 372–378.

[74] Olga León, Hernández-Serrano, R. RománJuan, Towards a cooperative intrusion detection system for cognitive radio networks, in: International Conference on Research in Networking, 2011, pp. 231–242.

[75] A. Weinand, A. Ambekar, M. Karrenbauer, D. Schotten, Providing physical layer security for mission critical machine type communication, in: IEEE 21st International Conference on Emerging Technologies and Factory Automation, 2016, pp. 1–4.

[76] S. Srinivasan, M.B. Shivakumar, Mohammad, Semi-supervised machine learning for primary user emulation attack detection and prevention through core-based analytics for cognitive radio networks, Int. J. Distrib. Sens. Netw. 5 (9) (2019) 1550147719860365.

[77] Z. El Mrabet, Y. Arjoune, H. El Ghazi, B. Abou Al Majd, N. Kaabouch, Primary user emulation attacks: A detection technique based on Kalman filter, J. Sens. Actuator Netw. 7 (3) (2018) 26.

[78] S.C. Lin, C.Y. Wen, W.A. Sethares, Two-tier device-based authentication protocol against PUEA attacks for IOT application, IEEE Trans. Signal Inf. Process. Netw. 4 (1) (2018) 33–47.

[79] D. Manman, Z. Zhao, H. Zhang, Detection of primary user emulation attacks based on compressive sensing in cognitive radio networks, in: IEEE Int. Conf. Wireless Commun. Signal Process. 2013, pp. 1–5.

[80] M. Dang, Z. Zhifeng, Z. Honggang, Detection of primary user emulation attacks based on compressive sensing in cognitive radio networks, in: International Conference on Wireless Communications & Signal Processing, 2013, pp. 1–6.

[81] F. Salahdine, N. Kaabouch, H. El Ghazi, A survey on compressive sensing techniques for cognitive radio networks, Phys. Commun. 20 (2016) 61–73.

[82] F. Salahdine, N. Kaabouch, H. El Ghazi, H. El Ghazi, A Bayesian recovery with Toeplitz matrix for compressive spectrum sensing in cognitive radio networks, Int. J. Commun. Syst. 30 (15) (2017) 1–13.

[83] I. Ohaeri, O. Ekabua, B. Isong, M. Esiefarienrhe, M. Motojane, Mitigating intrusion and vulnerabilities in cognitive radio networks, 4 (3) (2015) 1–10.

[84] K. Zeng, K. Govindan, P. Mohapatra, Non-cryptographic authentication and identification in wireless networks security and privacy in emerging wireless networks, IEEE Wirel. Commun. 17 (5) (2010).

[85] C. Zhao, W. Wang, L. Huang, Y. Yao, Anti-PUE attack base on the transmitter fingerprint identification in cognitive radio, in: 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009, pp. 1–5.

[86] J. Hillenbrand, T. Weiss, F.K. Jondral, Calculation of detection and false alarm probabilities in spectrum pooling systems, IEEE Commun. Lett. 9 (4) (2005) 349–351.

[87] R. Chen, J.-M. Park, J.H. Reed, Defense against primary user emulation attacks in cognitive radio networks, IEEE J. Sel. Areas Commun. 26 (1) (2008).

[88] F. Zachariah, P. Khargonekar, Generalized engage or retreat differential game with escort regions, IEEE Trans. Automat. Control 62 (2) (2017) 668–681.

[89] Y. Wu, K.J.R. Liu, An information secrecy game in cognitive radio networks, IEEE Trans. Inf. Forensics Secur. 1 (3 PART 1) (2011) 831–842.

[90] M. Yuksel, X. Liu, E. Erkip, A secure communication game with a relay helping the eavesdropper, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 818–830.

[91] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, T. Basa, Physical layer security: Coalitional games for distributed cooperation, in: Proc. 7th WiOpt, 2009.

[92] M. Amitav, S. Ali, A. Fakoorian, J. Huang, A. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey, IEEE Commun. Surv. Tutor. 16 (3) (2014) 1550–1573.

[93] S. Onur, G. Seop, J. Deng, on Collaboration, Securing cognitive radio networks against belief manipulation attacks via trust management, in: 2014 IEEE International Conference on Collaboration Technologies and Systems, 2014, pp. 158–165.

[94] A. Weinand, A. Ambekar, M. Karrenbauer, H. Schotten, Providing physical layer security for mission critical machine type communication, in: IEEE 21st International Conference on Emerging Technologies and Factory Automation, 2016, pp. 1–4.

[95] X. He, H. Dai, P. Ning, A Byzantine attack defender in cognitive radio networks: The conditional frequency check, IEEE Trans. Wireless Commun. 12 (5) (2013) 2512–2523.

[96] C. Yifeng, M. Yijun, K. Ota, L. Changqing, D. Mianxiong, L. Yang, Optimal data fusion of collaborative spectrum sensing under attack in cognitive radio networks, IEEE Netw. 28 (1) (2014) 17–23.

[97] J. Li, Z. Feng, Z. Feng, P. Zhang, A survey of security issues in cognitive radio networks, China Commun. 12 (3) (2015) 132–150.

[98] R. Cao, Y. Lu, On Study of physical-layer attack detection for large volumes of data, in: IEEE Second International Conference on Data Science in Cyberspace, 2017, pp. 30–34.

[99] L. Zhang, Q. Wu, G. Ding, S. Feng, J. Wang, Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing, EURASIP J. Adv. Signal Process. 2014 (1) (2014) 81.

[100] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, J. Wang, Byzantine attack and defense in cognitive radio networks: A survey, IEEE Commun. Surv. Tutor. 17 (3) (2015) 1342–1363.

[101] R. Cao, A physical-layer attack detection method using continuous secured side information, 2017, arXiv preprint arXiv:1701.01590.

[102] W. Wenkai, H. Li, Y. Sun, Z. Han, CatchIt: Detect malicious nodes in collaborative spectrum sensing, in: IEEE Global Telecommunications Conference, 2009, pp. 1–6.

[103] L. Duan, J. Min, A.W. Huang, K.G. Shin, Attack prevention for collaborative spectrum sensing in cognitive radio networks, IEEE J. Sel. Areas Commun. 30 (9) (2012) 1658–1665.

[104] H. Xiaofan, H. Dai, Adversary Detection for Cognitive Radio Networks, Springer International Publishing, 2018.

[105] R. Kishore, C.K. Ramesha, K.R. Anupama, Bayesian detector based superior selective reporting mechanism for cooperative spectrum sensing in cognitive radio networks, Procedia Comput. Sci. 93 (September) (2016) 207–216.

[106] A.S. Rawat, P. Anand, H. Chen, P.K. Varshney, Countering Byzantine attacks in cognitive radio networks, in: IEEE International Conference on Acoustics, Speech and Signal Processing, 2010, pp. 3098–3101.

[107] A. Rawat, P. Anand, C. Hao, K. Varshney, Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks, IEEE Trans. Signal Process. 59 (2) (2011) 774–786.

[108] D. Hlavacek, J.M. Chang, A layered approach to cognitive radio network security: A survey, Comput. Netw. (2014).

[109] M. Dillinger, K. Madani, N. Alonistioti, Software Defined Radio: Architectures, Systems and Functions, John Wiley & Sons, 2005.

[110] A. Min, K. Shin, X. Hu, Secure cooperative sensing in IEEE 802.22 wrans using shadow fading correlation, IEEE Trans. Mob. Comput. 10 (10) (2010) 1434–144728.

[111] Kelly. J., J. Ashdown, Sensing falsification detection in dense cognitive radio networks using a greedy method, in: IEEE National Aerospace and Electronics Conference, 2018, pp. 144–151.

[112] P. Kaligineedi, M. Khabbazian, V. Bhargava, Secure cooperative sensing techniques for cognitive radio systems, in: IEEE International Conference on Communications, 2008, pp. 19–23.

[113] T. Qin, H. Yu, C. Leung, Z. Shen, C. Miao, Towards a trust aware cognitive radio architecture, Mob. Comput. Commun. Rev. 13 (2) (2009) 86–95.

[114] Y. Arjoune, Z. El Mrabet, N. Kaabouch, Multi-attributes, utility-based,channel quality ranking mechanism for cognitive radio networks, Appl. Sci. 8 (4) (2018) 1–13.

[115] W. El-Hajj, H. Safa, M. Guizani, Survey of security issues in cognitive radio networks, Surv. Secur. Issues Cogn. Radio Netw. (2011) 1–18.

[116] Q. Pei, H. Li, J. Ma, et al., Defense against objective function attacks in cognitive radio networks, Chin. J. Electron. 1 (2011) 138–142.

[117] O. León, J. Hernández-Serrano, M. Soriano, Securing cognitive radio networks, Int. J. Commun. Syst. 5 (2010) 633–652.

[118] N. Ermolova, O. Tirkkonen, Consensus based spectrum sensing in cognitive radio networks, in: IEEE INFOCOM, 2012, pp. 900–908.

[119] C. Chen, M. Song, C. Xin, M. Alam, A Robust malicious user detection scheme in cooperative spectrum sensing, in: IEEE Global Communications Conference, 2012, pp. 4856–4861.

[120] R. Arpan, D. Kim, K.S. Trivedi, Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees, in: IEEE Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2012, pp. 1–12.

[121] Q. Pei, H. Li, J. Ma, et al., Defense against objective function attacks in cognitive radio networks, Chin. J. Electron. 1 (2011) 138–142.

[122] O. León, J. Hernández-Serrano, M. Soriano, Securing cognitive radio networks, Int. J. Commun. Syst. 5 (2010) 633–652.

[123] H. Tran, H. Zepernick, Proactive attack: A strategyf for legitimate eavesdropping, in: IEEE 6th International Conference on Communications and Electronics, 2016, pp. 457–461.

[124] A. Chorti, M. Perlaza, Z. Han, H. Poor, Physical layer security in wireless networks with passive and active eavesdroppers, in: IEEE Global Communications Conference, 2012, pp. 4868–4873.

[125] V. Nguyen, T. Duong, O. Shin, A. Nallanathan, G. Karagiannidis, Enhancing PHY security of cooperative cognitive radio multicast communications, IEEE Trans. Cogn. Commun. Netw. 3 (4) (2017) 599–613.

[126] M. Hasnat, S. Rurnee, M. Razzaque, M. Mamun-Or-Rashid, Security study of 5G heterogeneous network: Current solutions, limitations & future direction, in: IEEE International Conference on Electrical, Computer and Communication Engineering, 2019, pp. 1–4.

[127] J. Hamamreh, H. Furqan, H. Arslan, Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1773–1828.

[128] S. Ahmad, T. Shahabuddin, J. Kumar, A. Okwuibe, I. Gurtov, M. Ylianttila, Security for 5G and beyond, IEEE Commun. Surv. Tutor. (2019) 1.

[129] H. Idoudi, K. Daimi, M. Saed, Security challenges in cognitive radio networks, World Congr. Eng. 1 (2014) 2–4.

[130] A. Houjeij, W. Saad, T. Başar, Evading eavesdroppers in adversarial cognitive radio networks, in: IEEE Global Communications Conference, 2013, pp. 611–616.

[131] R. Wan, L. Ding, N. Xiong, X. Zhou, Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks, Int. J. Distrib. Sens. Netw. 15 (9) (2019) 1550147719870645.

[132] V. Vu, I.T.H. Thien, Koo, A repeated games-based secure multiple-channels communications scheme for secondary users with randomly attacking eavesdroppers, Appl. Sci. 9 (5) (2019) 868.

[133] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead, IEEE J. Sel. Areas Commun. 36 (4) (2018) 679–695.

[134] H. Dai, X. Li, Q. Wang, A. Vasilakos, Macau Univ of Science, Anti-Eavesdropping Shelter for Protection of Wireless Communication, U.S. Patent 9,800,367, 2017.

[135] S. Holcomb, D. Rawat, Recent security issues on cognitive radio networks: A Survey, in: Southeast Conference, 2016, pp. 1–6.

[136] G. Rathee, H. Saini, Security concerns with open research issues of present computer network, Int. J. Comput. Sci. Inf. Secur. 14 (4) (2016) 406.

[137] S. Bashar, Z. Ding, C. Xiao, On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input, IEEE Commun. Lett. 15 (5) (2011) 527–529.

[138] M. Elkashlan, L. Wang, Q. Duong, K. Karagiannidis, A. Nallanathan, On the security of cognitive radio networks, IEEE Trans. Veh. Technol. 64 (8) (2014) 3790–3795.

[139] M. Bouabdellah, F. El Bouanani, H. Ben-Azza, Secrecy outage probability in cognitive radio networks subject to Rayleigh fading channels, in: IEEE International Conference on Advanced Communication Technologies and Networking, 2018, pp. 1–5.

[140] N. Kolokotronis, K. Fytrakis, A. Katsiotis, N. Kalouptsidis, Cooperation for secure wireless communications with resource-bounded eavesdroppers, in: IEEE Globecom Workshops, 2014, pp. 1379–1384.

[141] X. Xu, W. Yang, Y. Cai, S. Jin, On the secure spectral-energy efficiency tradeoff in random cognitive radio networks, IEEE J. Sel. Areas Commun. 34 (10) (2016) 2706–2722.

[142] A. Chaman, J. Wang, J. Sun, H. Hassanieh, R. Choudhury, Ghostbuster: Detecting the presence of hidden eavesdroppers, in: 24th Annual International Conference on Mobile Computing and Networking, 2018, pp. 337–351.

[143] P. Thanh, T. Hoan, H. Vu-Van, I. Koo, Efficient attack strategy for legitimate energy-powered eavesdropping in tactical cognitive radio networks, Wirel. Netw. 25 (6) (2019) 3605–3622.

[144] J. Tian, Y. Liang, X. Kang, G. Yang, Eavesdropping via pilot relay attack, in: International Conference on Communications in China, 2017, pp. 1–6.

[145] J. Tugnait, Detection of active eavesdropping attack by spoofing relay in multiple antenna systems, IEEE Wirel. Commun. Lett. 5 (5) (2016) 460–463.

[146] W. Mou, W. Yang, Y. Huang, X. Xu, Y. Cai, K. Wang, On the security of cooperative cognitive radio networks with distributed beamforming, EURASIP J. Wireless Commun. Networking 2017 (1) (2017) 144.

[147] B. Kailkhura, V. Nadendla, P. Varshney, Distributed inference in the presence of eavesdroppers: A survey, IEEE Commun. Mag. 53 (6) (2015) 40–46.

[148] Y. Zeng, R. Zhang, Active eavesdropping via spoofing relay attack, in: IEEE International Conference on Acoustics, Speech and Signal Processing, 2016, pp. 2159–2163.

[149] S. Pahuja, P. Jindal, Cooperative communication in physical layer security: Technologies and challenges, Wirel. Pers. Commun. (2019) 1–27.

[150] C. Kundu, S. Ghose, R. Bose, Secrecy outage of dual-hop regenerative multi-relay system with relay selection, IEEE Trans. Wireless Commun. 14 (8) (2015) 4614–4625.

[151] H. Lei, M. Xu, I. Ansari, G. Pan, K. Qaraqe, M. Alouini, On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection, IEEE Trans. Green Commun. Netw. 1 (2) (2017) 192–203.

[152] V. Nguyen, T. Duong, O. Dobre, O. Shin, Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks, IEEE Trans. Inf. Forensics Secur. 11 (11) (2016) 2609–2623.

[153] H. Dai, H. Wang, H. Xiao, X. Li, Q. Wang, On eavesdropping attacks in wireless networks, in: IEEE International Conference on Computational Science and Engineering, 2016, pp. 138–141.

[154] O. Topal, O. Demir, G. Dartmann, A. Schmeink, G. Ascheid, A. Pusane, G. Kurt, Physical layer spoofing against eavesdropping attacks, in: 8th Mediterranean Conference on Embedded Computing, 2019, pp. 1–5.

[155] H.I. Reyes, N. Kaabouch, Jamming and lost link detection in wireless networks with fuzzy logic, Int. J. Sci. Eng. Res. 4 (2) (2013) 1–7.

[156] B. V, A. Krings, On the impact of jamming attacks on cooperative spectrum sensing in cognitive radio networks, in: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, 2013, pp. 1–6.

[157] S. Rizvi, N. Showan, J. Mitchell, Analyzing the integration of cognitive radio and cloud computing for secure networking, Procedia Comput. Sci. 61 (2015) 206–212.

[158] K. Barbara, L. Cambacédès, P. Schweitzer, DAG-based attack and defense modeling: Don't miss the forest for the attack trees, Comput. Sci. Rev. 13 (2014) 1–38.

[159] T. Kavitha, D. Sridharan, Security vulnerabilities in wireless sensor networks: A survey, 5 (November 2009) (2010) 31–44.

[160] W. Wang, S. Bhattacharjee, M. Chatterjee, K. Kwiat, Collaborative Jamming and Collaborative Defense in Cognitive Radio Networks, J. Pervasive Mobile Comput. (2012).

[161] Q. Peng, P.C. Cosman, L.B. Milstein, Optimal sensing disruption for a cognitive radio adversary, IEEE Trans. Veh. Technol. 59 (4) (2010) 1801–1810.

[162] K. Gai, M. Qiu, Z. Ming, H. Zhao, L. Qiu, Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks, IEEE Trans. Smart Grid 8 (5) (2017) 2431–2439.

[163] W. Wang, S. Bhattacharjee, M. Chatterjee K. Kwiat, Collaborative jamming and collaborative defense in cognitive radio networks, Pervasive Mobile Comput. 9 (4) (2013) 572–587.

[164] F. Slimeni, B. Scheers, B. Le Nir, Z. Chtourou, R. Attia, Learning multi-channel power allocation against smart jammer in cognitive radio networks, in: International Conference on Military Communications and Information Systems, 2016, pp. 1–7.

[165] R. Di Pietro, G. Oligeri, Jamming mitigation in cognitive radio networks, IEEE Netw. 27 (3) (2013) 10–15.

[166] V. Balogun, A. Krings, On the impact of jamming attacks on cooperative spectrum sensing in cognitive radio networks, in: Eighth Annual Cyber Security and Information Intelligence Research Workshop, 2013, p. 31.

[167] H. Li, Z. Han, Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems, in: IEEE Global Telecommunications Conference, 2009, pp. 1–6.

[168] A. Sampath, H. Dai, H. Zheng, B. Zhao, Multi-channel jamming attacks using cognitive radios, in: 16th International Conference on Computer Communications and Networks, 2007, pp. 352–357.

[169] A. Salem, X. Liao, Y. Shen, X. Jiang, Provoking the adversary by detecting eavesdropping and jamming attacks: A game-theoretical framework, Wirel. Commun. Mob. Comput. (2018) 1–6.

[170] Y. Arjoune, F. Salahdine, Md. Islam, E. Ghribi, N. Kaabouch, A novel jamming attacks detection approach based on machine learning for wireless communication, in: International Conference on Information Networking, 2020, pp. 1–6.

[171] R. Yenumula, Security issues and threats in cognitive radio networks, in: Advanced International Conference on Telecommunications, 2013, pp. 84–89.

[172] F. Salahdine, N. Kaabouch, H. El Ghazi, Bayesian compressive sensing with circulant matrix for spectrum sensing in cognitive radio networks, in: The 7th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, 2016, pp. 1–6.

[173] Z. Jin, K. Subbalakshmi, Detecting primary user emulation attacks in dynamic spectrum access networks, in: Proc. ICC, 2009, pp. 1–5.

[174] B. Wang, Y. Wu, K.J.R. Liu, T.C. Clancy, An anti-jamming stochastic game for cognitive radio networks, IEEE J. Sel. Areas Commun. 29 (4) (2011) 877–889.

[175] M. Riahi, A. Quadri, S. Subramaniam, N. Kaabouch, An optimized SNR estimation technique using particle swarm optimization algorithm, in: IEEE Computing and Communication Workshop and Conference, 2017, pp. 1–6.

[176] H. Xiaonan, X. Yang, Z. Shen, H. He, W. Hu, C. Bai, Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON, IEEE Photonics Technol. Lett. 27 (23) (2015) 2429–2432.

[177] O. Francesco, S. Romano, A reputation-based metric for secure routing in wireless mesh networks, in: IEEE Global Telecommunications Conference, 2008, pp. 1–5.

[178] L. Husheng, Z. Han, Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems—Part II: Unknown channel statistics, IEEE Trans. Wireless Commun. 10 (1) (2011) 274–283.

[179] H. Zhu, C. Fang, Y. Liu, C. Chen, M. Li, S. Shen, You can jam but you cannot hide: Defending against jamming attacks for geo-location database driven spectrum sharing, IEEE J. Sel. Areas Commun. 34 (10) (2016) 2723–2737.

[180] R. Jover, AT&T Intellectual Property, Base station antenna beam forming based jamming detection and mitigation, U.S. Patent Application 14/081,926, 2015.

[181] I. Azogu, M. Ferreira, J. Larcom, H. Liu, A new anti-jamming strategy for VANET metrics-directed security defense, in: IEEE Globecom Workshops, 2013, pp. 1344–1349.

[182] A. Wood, J. Stankovic, G. Zhou, DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks, in: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007, pp. 60–69.

[183] K. Pelechrinis, L. Koutsopoulos, I. Broustis, S. Krishnamurthy, Lightweight jammer localization in wireless networks: system design and implementation, in: Global Telecommunications Conference, 2009, pp. 1–6.

[184] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, M. Srivastava, Pycra: Physical challenge-response authentication for active sensors under spoofing attacks, in: 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 1004–1015.

[185] K. Grover, A. Lim, Q. Yang, Jamming and anti–jamming techniques in wireless networks: A survey, Int. J. Ad Hoc Ubiquitous Comput. 17 (4) (2014) 197–215.

[186] F. Salahdine, N. Kaabouch, Social engineering attacks: A survey, Future Internet 11 (4) (2019) 89.

[187] K. Zhang, Y. Mao, S. Leng, S. Fang, Efficient anti-jamming strategies in multi-channel wireless networks, in: International Conference on Computational Problem-solving, 2013, pp. 1–6.

[188] H. Li, Z. Han, Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part I: Known channel statistics, IEEE Trans. Wireless Commun. 9 (11) (2010) 3566–3577.

[189] S. Bhattacharjee, R. Rajkumari, N. Marchang, Cognitive Radio Networks Security Threats and Attacks: A Review, 2014, pp. 16–19.

[190] X. Wenyuan, W. Trappe, Y. Zhang, Anti-jamming timing channels for wireless networks, in: Proceedings of the first ACM conference on Wireless network security, 2008, pp. 203–213.

[191] G. Lim, Q. Yang, Jamming and anti-jamming techniques in wireless networks: A survey, Int. J. Ad Hoc Ubiquitous Comput. 17 (4) (2014) 197–215.

[192] Shiu Yi-Sheng, Shih Yu Chang, Hsiao-Chun Wu, Scott C.-H. Huang, Hsiao-Hwa Chen, Physical layer security in wireless networks: A tutorial, IEEE Wirel. Commun. 18 (2) (2011).

[193] M. Riahi, S. Apu, N. Kaabouch, W.-C. Hu, Performance evaluation of spectrum sensing techniques for cognitive radio systems, in: IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, IEEE, 2016, pp. 1–7.

[194] F. Salahdine, H. El Ghazi, A real time spectrum scanning technique based on compressive sensing for cognitive radio networks, in: IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, 2018, pp. 506–511.

[195] S. Jin, K. Subbalakshmi, Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing, in: ACM SigMobile Computing and Communication Review, 2009, pp. 74–85.

[196] E. Altman, K. Avrachenkov, A. Garnaev, Jamming in wireless networks under uncertainty, Mobile Netw. Appl. 16 (2) (2010) 246–254.

[197] F. Salahdine, N. Kaabouch, H. El Ghazi, Techniques for dealing with uncertainty in cognitive radio networks, in: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference, 2017, pp. 1–6.

[198] A. Patel, H. Ram, A.K. Jagannatham, P.K. Varshney, Robust cooperative spectrum sensing for MIMO cognitive radio networks under CSI uncertainty, IEEE Trans. Signal Process. 66 (1) (2018) 18–33.

[199] Y. Muhammad, B. Mazumdar, J. Rajendran, O. Sinanoglu, Hardware security and trust: Logic locking as a design-for-trust solution, in: The IoT Physical Layer, Springer, 2019, pp. 353–373.

[200] D. Deepa, S. Das, Primary user emulation attack in cognitive radio networks: A survey, Int. J. Comput. Netw. Wirel. Commun. 3 (3) (2013) 312–318.

[201] F. Yawen, Z. Zhang, M. Trinkle, A. Dimitrovski, J. Song, H. Li, A cross-layer defense mechanism against GPS spoofing attacks on Pmus in smart grids, IEEE Trans. Smart Grid 6 (6) (2015) 2659–2668.

[202] C. Blackwell, A multi-layered security architecture for modelling complex systems, in: Proceedings of the ACM Annual Workshop on Cyber Security And Information Intelligence Research: Developing Strategies To Meet The Cyber Security And Information Intelligence Challenges Ahead, 2008, p. 35.

[203] K. Mona, Y. Dubey, Advanced technique for cooperative spectrum sensing optimization in cognitive radio network, Int. J. Eng. Tech. Res. 8 (5) (2019).

Dr. Fatima Salahdine got her Ph.D., M.S., and B.S. in Electrical Engineering from the Communications Systems Department at the National Institute of Posts and Telecommunications, Morocco. She was a Fulbright Scholar in the Electrical Engineering Department at the University of North Dakota, USA. She is currently working on cybersecurity in collaboration with Dr. Naima Kaabouch. Her research area includes cybersecurity, machine learning, cognitive radio, compressive sensing, and wireless communications. Fatima.salahdine@gmail.com.

Dr. Naima Kaabouch is Professor in the Electrical Engineering Department at the University of North Dakota, USA. She is the Director of two research laboratories located within the College and Engineering & Mines at UND. She got her Ph.D., M.S., and B.S. in Electrical Engineering from the University of Paris 6 and the University of Paris 11, France. Her research interests include signal/image processing, sensing, smart systems, and cognitive radio systems. Examples of her current projects include: radio spectrum access and management, payloads and algorithms for space applications, radars to remotely monitor vital signs, cybersecurity, and breast micro calcifications detection. naima.kaabouch@engr.und.edu.