Marinho et al. EURASIP Journal on Information Security (2015) 2015:4
DOI 10.1186/s13635-015-0021-0

EURASIP Journal on Information Security
a SpringerOpen Journal

REVIEW Open Access

A survey on security attacks and countermeasures with primary user detection in cognitive radio networks

José Marinho[1,2], Jorge Granjal[2,3*] and Edmundo Monteiro[2,3]

Abstract

Currently, there are several ongoing efforts for the definition of new regulation policies, paradigms, and technologies aiming a more efficient usage of the radio spectrum. In this context, cognitive radio (CR) emerges as one of the most promising players by enabling the dynamic access to vacant frequency bands on a non-interference basis. However, the intrinsic characteristic of CR opens new ways for attackers, namely in the context of the effective detection of incumbent or primary users (PUs), the most fundamental and challenging requirement for the successful operation of CR networks. In this article, we provide a global and integrated vision of the main threats affecting CR environments in the context of the detection of primary users, with a particular focus on spectrum sensing data falsification and primary user emulation attacks. We also address solutions and research challenges still required to address such threats. Our discussion aims at being complete and self-contained, while also targeting readers with no specific background on this important topic of CR environments. It is, as far as our knowledge goes, the first work providing a global and clear vision of security threats and countermeasures in the context of primary user detection in CR.

Keywords: Security in cognitive radio; Primary user detection; Primary user emulation; Spectrum sensing falsification

1 Review

1.1 Introduction

The radio spectrum is a finite resource currently experiencing a tremendous increase in demand and, consequently, growing in scarcity. This trend will continue in the future as the number of deployed wireless technologies and devices increases, the same applying to the bandwidth requirements. Additionally, the few existing license-free radio frequencies, such as the industrial, scientific, and medical (ISM) bands, are often overcrowded, especially in densely populated areas. This situation results in contention and interference, and, consequently, in significant performance degradation. Despite such aspects, we can also observe that the majority of the licensed radio spectrum remains unused or underutilized independently of time and location, resulting in numerous vacant spectrum bands [1]. This inefficient usage of the spectrum results directly from the current spectrum regulation policies, which divide the spectrum into static licensed and unlicensed frequencies. The definition of more flexible regulation policies and the development of related and innovative technologies will change this paradigm, with cognitive radio (CR) emerging as one of the key enablers in this context [1,2].

A CR device is intended to possess the capability to observe and learn from its environment, and to dynamically and autonomously adjust transmission parameters such as the operating frequency and transmission power, in order to increase its performance on a non-interference basis. A key component of the CR paradigm is the usage of software-defined radios (SDR), radio communication systems with components implemented in software rather than in hardware. We currently verify an increasing availability of SDR platforms, which are employed in the context of the development of new platforms and research proposals in the area of CR. Through a dynamic spectrum access (DSA) approach [1], CR users, also designated as secondary users (SUs), are able to opportunistically and intelligently access the spectrum holes in a transparent

* Correspondence: jgranjal@dei.uc.pt
[2]DEI-UC - Department of Informatics Engineering, University of Coimbra, Pólo II - Pinhal de Marrocos, 3030-290 Coimbra, Portugal
[3]CISUC - Centre for Informatics and Systems of the University of Coimbra, Pólo II - Pinhal de Marrocos, 3030-290 Coimbra, Portugal
Full list of author information is available at the end of the article

way to the primary users (PUs) and without causing them any harmful interference. The accurate location of spectrum holes appears thus as the most challenging and fundamental issue in CR environments.

It is well assumed in the literature that approaches for the localization of vacant spectrum bands based exclusively on local sensing and learning do not offer satisfactory results [3,4]. The main reasons are missed PU detection and false alarm probabilities, which are inherent to any kind of sensing hardware and may also result from adverse propagation effects such as multipath fading and shadowing. This implies that in practice any spectrum decision must be made taking into account several sources of information. For instance, a fusion rule might be applied to the sensing reports of several SUs and to geo-location data, if available. In this context, the usage of spurious data is a serious threat which can lead to wrong spectrum decisions and, in consequence, to an inefficient protection of PUs (i.e., due to missed detections) or to an inefficient, suboptimal, or unfair usage of the spectrum (i.e., due to false alarms).

The normal operation of a CR environment depends greatly on the effectiveness of the mechanisms designed to perform spectrum analysis and decision on the SUs. Those mechanisms aim to decide on the availability of spectrum space for the purpose of allowing the SUs to transmit but in practice may be affected by erroneous or falsified data. Erroneous spectrum availability data may be due to hardware imperfections and adverse propagation effects or, on the other hand, to security attacks, particularly data falsification and PU emulation, as we discuss throughout this survey. Attackers with malicious intents may report the opposite of their observations in order to disrupt the operation of the CR network (i.e., reduce the protection of PUs or spectrum usage efficiency). On the other hand, attackers with greedy or selfish intents may positively report the presence of PU activity in order to gain exclusive access to the spectrum. Globally, malicious and greedy attackers have the common objective of causing denial of service (DoS) to legitimate SUs [5]. In Table 1, we summarize the main motivations for attacks against normal CR operations.

The protection against the usage of spurious information in the context of PU detection is of major importance in CR environments and the main focus of our discussion in the survey. Overall, any threat against the normal functioning of mechanisms designed to guarantee detection of PU activity or spectrum availability is potentially disruptive of normal CR operations. Our goal is also to discuss how such threats are addressed by current technological solutions and to identify open issues in this context. Despite the existence of several published works on security issues related to CR environments [6-11], none of them specifically provides a global and clear vision of security threats against normal PU detection in CR environments, together with the available countermeasures and open research challenges, as we address in this survey. Our discussion seeks to provide a detailed discussion on the impact of such threats to the normal operation of CR environments and on how research is dealing with them, both in respect to current proposals and challenges to be faced by future research efforts.

The survey proceeds as follows. Section 1.2 identifies the CR scenarios that contextualize our discussion on security throughout the paper. Section 1.3 discusses the main security requirements and threats applying to CR environments, and in Section 1.4, we discuss the risks that can affect the effectiveness of PU detection as well as existing research proposals in this context. Finally, Section 2 concludes the paper and identifies the existing research challenges in this area.

1.2 Cognitive radio networks

A network employing CR technology may adopt a centralized or distributed architecture, as illustrated in Figure 1. With a centralized approach or infrastructure-based CR network, spectrum decisions are performed and coordinated by a central entity (e.g., a base station) based on the fusion of sensing results collected from several SUs or dedicated sensors. This approach therefore enables a centralized cooperative sensing scheme. The central entity can additionally rely on geo-location databases providing the coordinates of known primary transmitters (e.g.,

Table 1 Characterization of attacks against the normal functioning of CR networks

Motivations	Attack goals	Attack approaches	Attack effects
Greedy/selfish	Maximize the communication performance of the attacker.	Make the SUs believe that vacant portions of the spectrum are busy (i.e., induce false alarms) and access them exclusively.	A global decrease on spectrum sharing efficiency and usage fairness.
Malicious	Disrupt the performance and operations of the SUs and/or PUs.	Make the other SUs believe that vacant portions of the spectrum are busy.	A decrease in spectrum usage efficiency and, therefore, in the performance of the affected SUs.
		Make the SUs believe that busy portions of the spectrum are idle (missed detections).	A decrease in the protection of the affected PUs against interferences caused by (erroneous) SU transmissions.

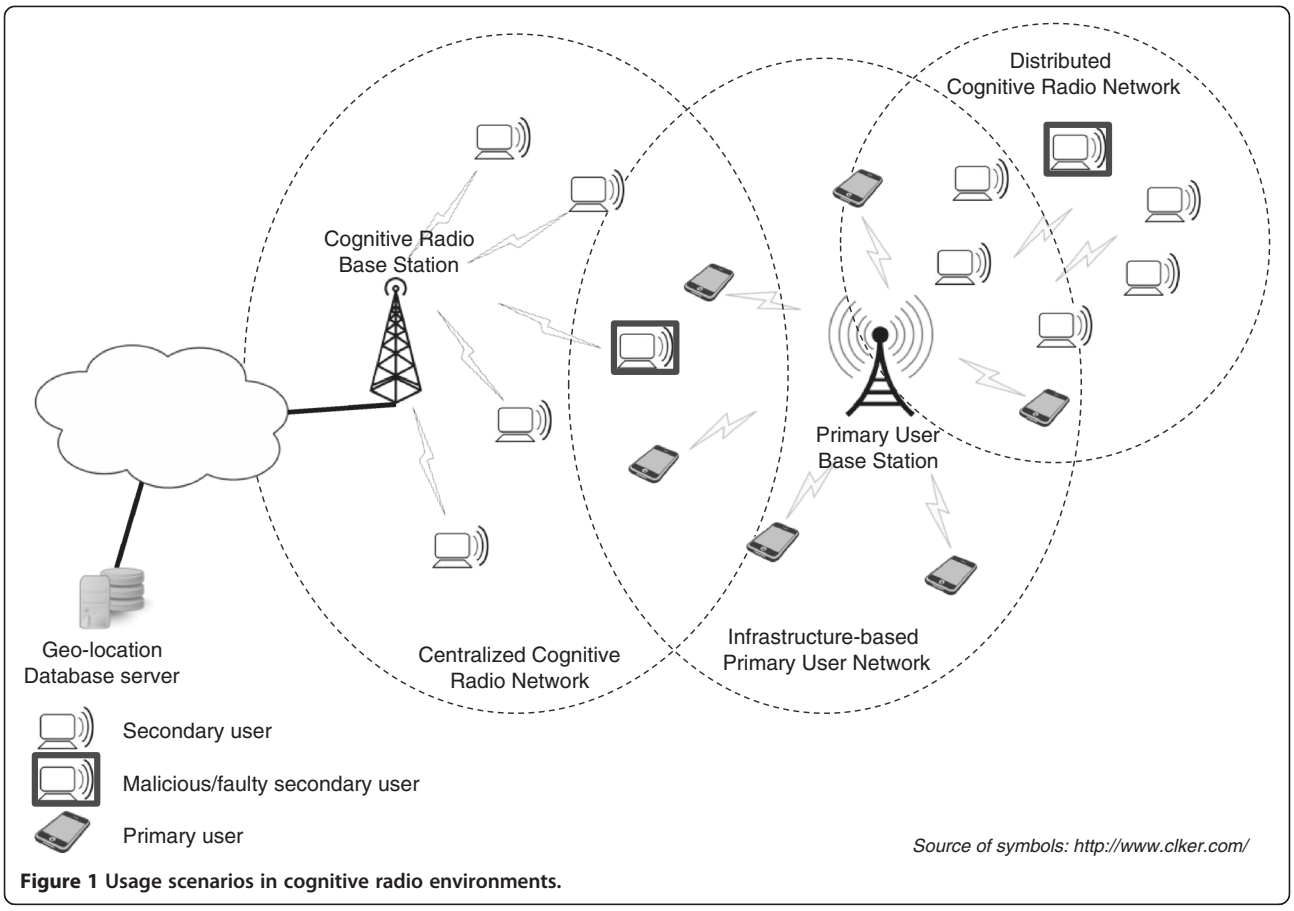

Figure 1 Usage scenarios in cognitive radio environments.

television transmitter towers) and their respective regions of potential interference. This is the approach adopted in the recent IEEE 802.22 standard [12], which targets CR operations over television frequency bands (54 to 862 MHz) in order to enable the deployment of wireless regional networks. IEEE 802.22 uses both spectrum sensing and geo-location databases for the detection of spectrum holes, with regulatory bodies being responsible for the maintenance of the information describing the locations of the primary systems. When this information is not available, all the television channels are considered potential opportunities and only sensing is used.

In distributed or *ad hoc* CR networks [13], each SU supports its own spectrum decisions based on local observation and learning. With a cooperative scheme, each SU also considers the signaling information provided by its neighbors (e.g., sensing reports), therefore acting as a data fusion center. Cooperative schemes have more communication overhead than non-cooperative solutions but may result in higher spectrum usage efficiency and sensing accuracy [4]. We also note that, although the distributed CR network illustrated in Figure 1 follows a one-hop approach, given that every SU is in the transmission range of each other, multi-hop approaches are also possible.

As Celebi and Arslan [14] state, centralized and distributed approaches are the two extreme cognition limits between which various approaches can be developed. For instance, a CR mesh network may be considered, where spectrum decision is performed by several mesh gateways or by the SUs themselves (as with a pure distributed approach), with optional usage of geo-location databases accessible through the gateways. In order to support our following discussion on security in the context of CR environments, in Figure 1 we also illustrate the presence of SUs which are supposed to be malicious, faulty, or both. For the sake of realism, in practice we must also consider that any sensing device is characterized by non-null missed detection and false alarm probabilities, which may occasionally influence erroneous decisions.

1.3 Cognitive radio security threats and requirements

Security threats against CR networks may be motivated not only by the wireless nature of such communication environments (and that are in fact inherent of any wireless communications technology) but also by the employment of specific cognitive operations. In Figure 2,

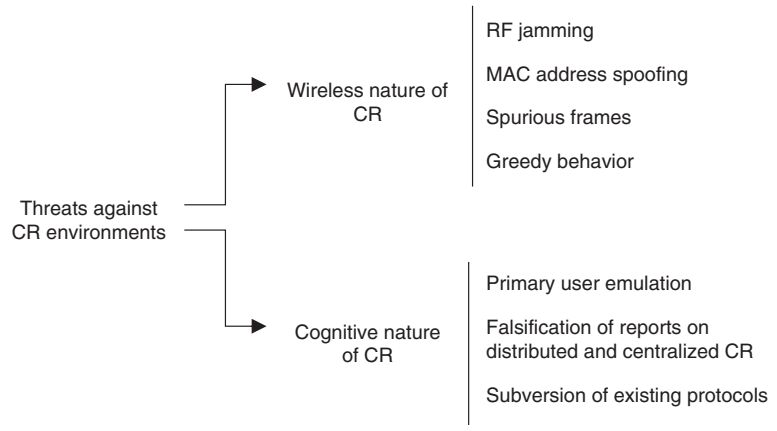

Figure 2 Taxonomy of (security) threats against the cognitive nature of CR environments.

we illustrate a taxonomy of the security threats against CR environments, considering such two different and complementary perspectives.

Given its wireless nature, CR environments may be open to attacks against wireless communications, particularly at the physical and medium access control (MAC) layers. For example, radio frequency (RF) jamming may target the physical layer and disrupt the network operations. Attacks at the MAC layer may include address spoofing, transmission of spurious MAC frames, and greedy behavior by cheating on the back off rules established by the MAC protocol. On the other hand, security concerns due to the cognitive nature of CR networks motivate the development of mechanisms to protect both primary and secondary users [15] and are the main focus of our discussion in this survey.

In CR environments, a SU can be fooled by malicious elements of its environment, as it relies on observation and possibly on cooperation for spectrum decision and learning. Among various types of threats, two assume particular importance on CR environments and motivate our analysis throughout the survey: *PU emulation* and *data falsification* attacks. Data falsification attacks in the context of CR networks may involve for example the reporting of false spectrum sensing data, as we discuss in detail later. Security threats that are out of the scope of our discussion may include attacks aiming the installation of malicious code in the cognitive radio devices, with the goal of subverting existing CR protocols. Such protocols are expected to assure that only vacant channels are accessed by the SUs and that the channels are evacuated by the SUs upon the return of PU activity.

Looking more closely at the problems of PU emulation and spectrum sensing data falsification, a PU emulation attack allows an attacker to mimic a PU in order to force other CR users to vacate a specific frequency band and consequently cause the disruption of the network's operations and unfairness on spectrum sharing. We may also note that this attack is specific to CR networks. On the other hand, the falsification of reports in cooperative schemes consists in providing false information to the neighbors or to a data fusion center and affects the effectiveness of spectrum decision. In Table 2, we identify the applicability, the effects, and possible approaches or countermeasures against primary user emulation and spectrum sensing data falsification attacks. Our discussion throughout the survey explores in detail the aspects described in this table.

Many existing CR proposals employ statistics collected about the observed PU activity, in order to learn and make predictions based on beliefs that result from current and past observations. In this context, manipulated and faulty data may lead to what Clancy and Goergen [16] designate as belief-manipulation attacks. In fact, learning capabilities (e.g., based on neural and evolutionary algorithms) not only result in great benefits to CR scenarios but also offer new opportunities for attackers. Any manipulation may potentially affect future spectrum selections, as the SUs employ all their experiences in order to derive long-term behavior. This also implies that learned beliefs should never be permanent. In non-cooperative networks, an attack against a SU does not affect the others, since every SU is able to make its own spectrum sensing and spectrum decisions. On the contrary, when a cooperative or centralized scheme is employed, an attack to a single device may affect the outcome of the entire CR network. Overall, intentional and unintentional anomalies may result in a decrease in terms of the performance of PU protection and spectrum usage, and in spectrum access unfairness among the various SUs. Security is thus of prime importance for the normal functioning of CR network operations, as we proceed to discuss.

Table 2 Attacks against CR environments and applicable countermeasures

Attack	Applicability	Effects	Countermeasures
PU emulation	CR networks based on non-cooperative schemes. Note: in such environments an attack against a specific SU may only affect that SU.	False alarms due to fake signals.	Sensing techniques that consider *a priori* known characteristics of the legitimate PU signals.
		The affected SUs are denied access to the affected spectrum holes due to greedy or malicious motivations, and, therefore, their performances are likely to decrease.	Solutions based on capabilities such as location determination techniques and access to geo-location information about *a priori* known PUs.
Spectrum sensing data manipulation/ falsification	CR networks based on cooperative schemes. Note: in such environments, attacks against a single SU may affect several SUs or the entire network.	Cooperative spectrum sensing accuracy decreases due to the propagation of false alarms and/or missed detections that are forged.	Solutions for providing characteristics such as mutual authentication, data integrity, and data encryption.
		If learning is considered, the behavior of the SUs is likely to suffer a negative impact on the long-term basis due to the usage of manipulated data in the learning process.	Outlier detection techniques.
		Malicious attacks may impact on PUs by inducing missed detections.	Approaches based on the exploration of spectrum spatial correlation and location techniques.
		Malicious and greedy attacks may impact the performance of the SUs by inducing false alarms.	Schemes that enable determining the trustiness of the SUs and, therefore, dropping reports from untrustworthy sources.
			Deployment of dedicated trusty sensors.
			Usage of mechanisms to selectively forget past information in order to make beliefs and learning outputs temporary.

1.4 Approaches to attack-tolerant primary user detection on CR environments

Various security threats are transversal to wireless environments and may consequently also affect CR applications and communication mechanisms. For example, a beacon falsification attack in IEEE 802.22 environments may allow the transmission of false spectrum or geo-location information to users, allowing the subversion of normal spectrum space access and usage rules. As in most wireless environments, well-known security solutions may be of help in circumventing many of such attacks in CR networks. In this context, the security layer 1 as defined in IEEE 802.22 defines encryption and authentication mechanisms offering protection for geo-location information as reported by the SUs using the co-existence beacon protocol (CBP).

Other than the employment of classic cryptographic approaches to support security mechanisms designed for CR environments, we may note that the most important challenges to research and standardization work regarding security reside in the design of security solutions to cope with the threats that are inherent to the cognitive nature of such environments, as previously discussed [17]. Such threats may potentially challenge the main goal of CR, which is the usage of the available radio spectrum space in a fair and optimal way, while preserving primary or incumbent transmitters from interferences. We proceed with a discussion on how such threats may be approached, with a particular focus on a fundamental mechanism of CR: the effective detection of primary user activity and spectrum opportunities.

1.4.1 Attacks against cooperative sensing

Spectrum sensing is a fundamental mechanism of CR networks and, in this context, one major problem to avoid is the designated hidden PU problem. This problem occurs when a SU cannot sense the activity of a PU it interferes with, i.e., when it is out of the coverage area of the PU or when sensing is affected by well-known adverse effects in wireless communications, in particular multipath fading and shadowing. For instance, in Figure 1 the PU base station is a hidden PU, in the perspective of the three nodes of the distributed CR network that are out of its coverage area, while having transmission ranges that overlap it. In practice, we must consider that sensing can also be erroneous due to inherent hardware imperfections, and consequently the usage of spectrum occupancy information obtained exclusively from local sensing might not achieve satisfactory results. In this context, cooperative or collaborative sensing is considered an effective means to increase the efficiency of PU detection in CR environments. However, it also creates new security vulnerabilities, as we proceed to discuss in greater detail.

1.4.1.1 Data fusion: a key enabler for cooperative sensing In collaborative sensing schemes, the final

decision regarding spectrum access is based on the fusion of sensing data from multiple SUs. In particular, the fusion process may be centrally achieved by a common data fusion center, or in alternative be implemented in a distributed manner, as illustrated in Figure 3. In the distributed approach, each SU acts as both a sensing and a fusion center, by collecting reports from its neighbors and performing data fusion and decisions individually. Distributed approaches are usually preferable, as a centralized fusion center in practice represents a single point of failure against the operability of the entire CR network. On the other hand, the required transmission of collaborative information may result in overhead. In their work about compressive spectrum sensing, Chen et al. [18] approach this problem by considering that the SUs only transmit part of the available sensing information as a strategy to reduce overhead. Lo and Akyildiz [19] also identify and address other possible overhead causes and effects that limit gains in collaborative sensing.

With the goal of reporting their sensing results, each SU in the context of a cooperative approach can either follow a hard-decision or a soft-decision approach. With hard-decision, each SU reports its decision in a binary form (i.e., channel is busy or idle), while with soft-decision

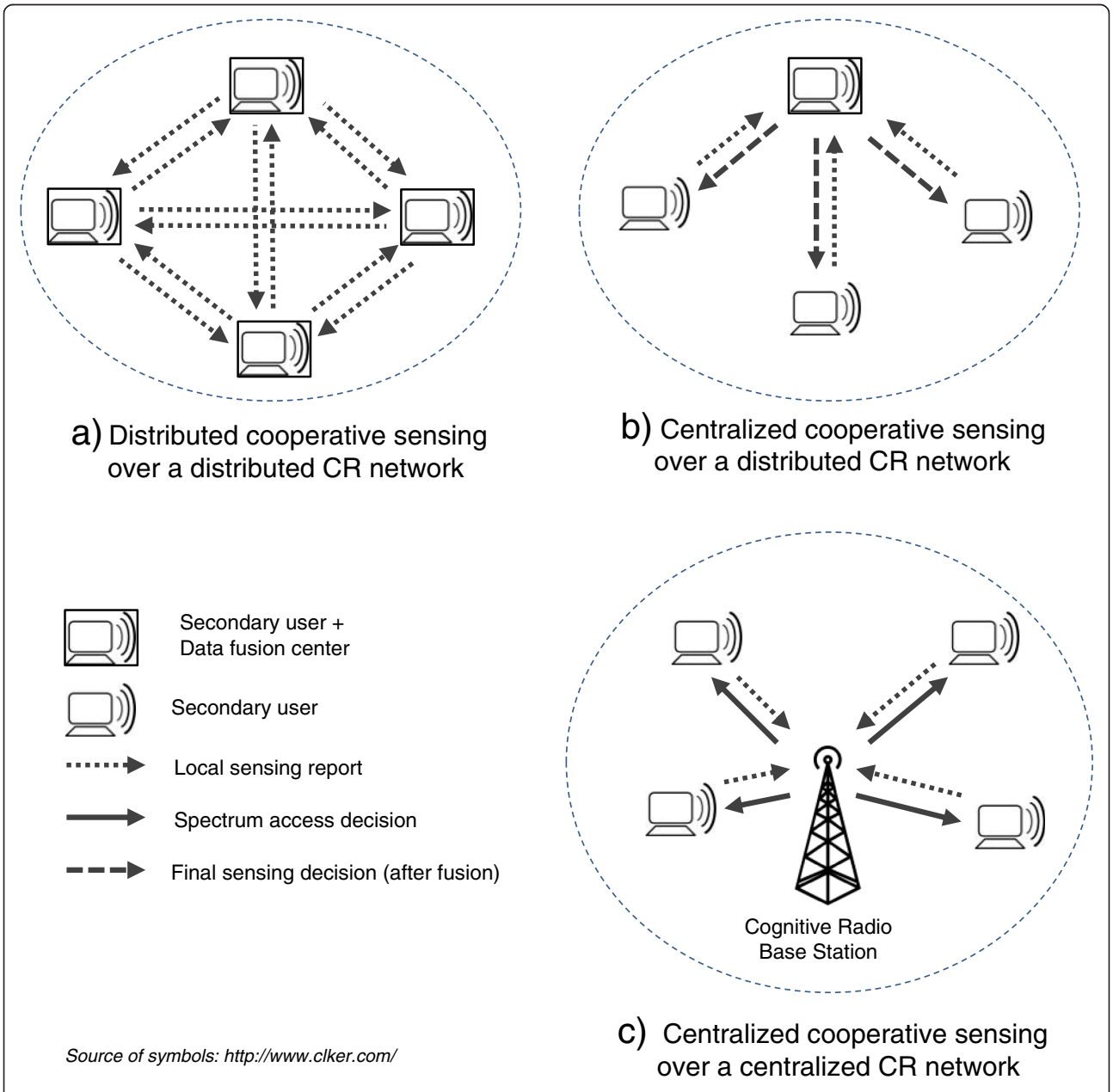

Figure 3 Cooperative sensing approaches in one-hop distributed and centralized CR scenarios.

they report the sensed energy levels. In terms of sensing performance, Wang et al. [20] discuss that hard-decision performs almost the same as soft-decision when cooperative users face independent fading (e.g., when the SUs are not nearby each other). Additionally, we may note that hard-decision reduces the overhead in reporting sensing results [21]. Concerning soft-decision, Clouquer et al. [22] conclude that it is superior to hard-decision when fault-tolerance is not required or when sensors are highly reliable and fault-free.

Various approaches have been proposed regarding the fusion of sensing outputs in CR environments. Three common fusion approaches are implemented in the form of the OR-rule, the AND-rule, and the voting-rule. The OR-rule considers that PU activity is present if detected by at least one sensor, while the AND-rule requires that all participating sensors detect activity from the PU. With the voting-rule, a PU is declared to be present if more than a given fraction of the sensors are able to detect its activity [15]. In general terms, the OR-rule is the most commonly used approach, especially when a hard-decision approach is followed. In particular, Clouquer et al. [22] consider that this rule achieves the best performance in the presence of a hard decision. However, when the OR-rule is applied, the potential impact of the false spectrum access denial problem (i.e., when access is denied despite the SU being out of the region of potential interference) increases as the number of CRs increases [23].

Nasipuri and Li [24] propose a hard-decision process in which the decisions are performed by comparing the number of positive local decisions against a threshold (e.g., it results in the OR-rule if the threshold is equal to one). Other approaches are also possible, for example, the average fusion rule computes the average of the sensing outputs and compares it against a given threshold [22]. Malady and Silva [23] propose a centralized soft-decision approach employing a rule that computes a weighted sum of the signal strengths reported by the sensing SUs, again with the channel being considered busy if the computed value is greater than a particular threshold. Fatemieh, Chandra, and Gunter [25] discuss that the usage of a statistical median provides results that are more robust to excessively high or low reports by malicious or deeply faded nodes than when using a mean value. In their proposal, they jointly employ both estimators in order to achieve a mix of accuracy (mean) and robustness (median) in the decision process.

1.4.1.2 Security issues in the context of cooperative sensing As the final decision in collaborative sensing results from the combination of multiple sensing results, new opportunities emerge for attackers that are able to send manipulated sensing data. This is a major concern and one of the most fundamental security challenges that must be addressed before considering any collaborative sensing proposal to be feasible in practical terms and, in consequence, to fully achieve the benefits of CR [26]. Furthermore, as a SU might use experience learned from past to reason new behaviors and to anticipate future actions, non-detected attackers or faulty nodes may cause an impact on behavior on a long-term basis [27]. Despite this, the security aspects of spectrum sensing have in general received very little attention from research [28,29]. As previously discussed, in this context, one must also consider the likelihood of well-behaved SUs occasionally sending wrong sensing reports due to the uncertainty of the sensing environment and also to hardware imperfections. We note that cooperation in CR environments is not limited to the sharing of sensing reports. For example, it may involve the exchange of statistical data for cooperative learning. Therefore, the remainder of our discussion and the content of Figure 3 can be generalized to the exchange and fusion of generic data.

In general terms, reliable inputs (or inputs from reliable SUs) must be appropriately filtered and accepted prior to the execution of the fusion and decision processes. One of the possible strategies may consist in the utilization of a combination of mutual authentication, data integrity protection, and data encryption in order to restrict data inputs only to those from trustworthy users and consequently prevent illegitimate manipulation of data [16]. The work of Rifà-Pous and Garrigues [30] and also the IEEE 802.22 standard apply in this context. For example, IEEE 802.22 defines the secure control and management protocol (SCMP), a security mechanism derived from IEEE 802.16, providing authentication, authorization, message integrity, confidentiality, and privacy. SCMP guarantees that only authorized devices can access the network and that a device generating spurious data can be unauthorized by the base station. Additionally, if a geo-location database and localization techniques are used, it is also possible to compare the estimated position of an authenticated transmitter and its *a priori* known location. Rifà-Pous and Garrigues [30] propose a centralized solution that enables a fusion center to validate the identity of the SUs and authenticate their sensing reports and is appropriate for large CR networks. This solution uses cryptographic signatures based on simple hash functions and symmetric keys and requires the fusion center and the SUs to hold valid certificates.

For the detection of spurious sensing data, the most commonly used approach is outlier detection [26], also designated as anomaly or deviation detection. In a given set of values, an outlier corresponds to data that appears to be inconsistent with the remaining values. One of the main difficulties in outlier detection consists in preventing normal data from being erroneously classified as an

outlier. There are simple and straightforward outlier detection techniques that may be employed during the fusion process, for example, ignoring extremely low or high sensing reports, or the m largest and m smallest reported values. However, with such solutions, meaningful values may be dropped and, consequently, accuracy reduced. Choosing the threshold value (i.e., the value for m or the predefined high and low levels) is not a trivial task. Ideally, it should be dynamically learned and adjusted without any *a priori* knowledge [31]. The work of Chen, Song, and Xin [32] is an example of a solution that uses more complex statistics for detecting spurious sensing data in cooperative sensing. However, in this work the authors assume that the locations of PUs are known to all SUs and that each SU is also location-aware, aspects which might limit the practicality of this proposal.

Several authors consider in their proposals that the number of malicious and faulty nodes cannot be greater than the number of properly behaving and honest working nodes. For instance, Min, Shin, and Hu [33] assume in their work that at least two thirds of the nodes are well behaving. On the contrary, Wang and Chen [34] propose a data fusion scheme for centralized CR networks that tolerates a high percentage of malicious SUs. This strength results from allowing the data fusion center to also sense the spectrum and use its own outcomes to assess the honesty of the SUs. In order to consider statistical, sporadic, and transient phenomena (e.g., false alarm probabilities), recent historical values may also be considered. For example, the proposal in the work of Li and Han [35] aims at finding the outlier users that are far from most SUs in the history space in terms of the reported values.

It must be noted that spectrum status is usually assumed to be correlated for SUs in close proximity and, in this context, spatial correlation can also be explored. A SU is thus very likely to have an erroneous sensing decision if most nearby SUs have the opposite decision (i.e., it is an outlier), as discussed by Zhang, Meratnia, and Havinga [31]. Therefore, the distinction between genuine and spurious data is based on the assumption that faulty or falsified reports are likely to be unrelated with neighboring data (i.e., spatially unrelated), while accurate sensing reports from neighboring sensors are likely to be (spatially) correlated [31]. This results in the commonly used nearest neighbor-based approaches or distance-based clustering approaches (i.e., sensors in close proximity are grouped into clusters). For instance, Min, Shin, and Hu [33] propose a collaborative sensing protocol in which sensors in close proximity are grouped in a cluster, with the purpose of safeguarding collaborative sensing. The sensors report their energy-detector's output along with their location information to the fusion center at the end of each sensing period. This work thus considers the spatial correlation in received signal strengths among nearby sensors. Chen, Song, Xin, and Alam [36] follow a similar approach, as they also explore spatial correlation of received signal strengths among nearby SUs, with the purpose of detecting malicious SUs in cooperative spectrum sensing. This proposal also includes a neighborhood majority-voting rule.

The work of Nasipuri and Li [24] is another example that can be mentioned in this context, and its proposed fusion rule includes a clustering metric. In this proposal, location information from collaborative sensors is employed in order to determine the proximity of sensors that have similar observations. The proposal of Chen et al. [29] also considers geographical information, as it is based on a spatial correlation technique. Defining which SUs are in close proximity remains a challenging issue in the context of the successful exploration of spatial correlation and requires appropriate geo-location techniques [37].

The detection of outliers can also be a means to dynamically determine the reputation levels of the SUs, i.e., for drawing conclusions about the quality of the information they report. As indicated in Table 2, this approach enables the use of trust-based security schemes that may, for instance, attribute more relevance to the reports of more trustworthy SUs (e.g., through a weighted mean-based fusion scheme in which different weights are adaptively assigned to the SUs according to their reputation levels) [6,29,33,38] or ignore the sensing reports from SUs with reputation values under a defined threshold [21,34,39,40]. Globally, when a SU reports sensing data not tagged as an outlier, its reputation is increased. In the opposite scenario, when a SU frequently sends reports inconsistent with the final decision [38], its reputation value is decreased. Through this reinforcement-based approach, past reports are therefore considered for the computation of decisions. Examples of schemes following this approach may be found in the collaborative sensing solutions proposed by Wang et al. [20], Wang and Chen [34], and by Zeng, Paweczak, and Cabric [21]. In the former, the nodes are classified either as honest or as malicious, with all nodes initially assumed to be honest. The later proposal describes a similar dynamic reputation-based approach, in which the SUs can be in three possible states: discarded, pending, and reliable. Initially, only a predefined set of trusted nodes is considered reliable. Concerning the proposal of Wang and Chen [34], which also consists in a trust-based data fusion scheme, it targets centralized CR networks and aims at tolerating a high percentage of malicious SUs. We note that some authors consider that the soft-decision approach presents more potential to support the implementation of reputation-based security

solutions [21]. We cannot also ignore the possibility of an attacker being intelligent enough in order to know the internal workings of the fusion rule. In this scenario, the attacker could adapt and start behaving honestly anytime its reputation level drops below a defined threshold [6,32]. Tingting and Feng [41] describe an attacker of this type as a hidden malicious user.

An alternative approach is to assume that nodes from a given set are reliable (e.g., access points, base stations, or specific SUs) [5,21]. Such an assumption may provide an increase in the performance of collaborative sensing, for example, by initially considering only reports from reliable nodes. Yang et al. [37] propose a sensing service model that employs dedicated wireless spectrum sensing networks providing spectrum sensing as a service, which include a large number of low-cost, well-designed, and carefully controlled sensors. Zhang, Meratnia, and Havinga [31] state that the existing outlier detection techniques do not consider node mobility or dynamically changing topologies and, as such, should be based on decentralized approaches (i.e., performed locally such as in distributed cooperative sensing) in order to keep the communication overhead, memory, and computational costs low, while enhancing scalability. The same authors also state that the outlier detection operations must be performed online and without any *a priori* information, given that it may be difficult to pre-classify normal and abnormal sensing data in distributed CR environments in terms of PU activity.

1.4.2 Primary user emulation in CR environments

Primary user emulation attacks in CR environments aim at forcing SUs to avoid using specific frequency bands and, therefore, may cause the same adverse effect as always reporting a channel to be busy with cooperative sensing schemes, as described in Table 2. This threat is materialized through the transmission of fake PU signals and does not necessarily require the attackers to participate in any underlying cooperative scheme. Thus, a PU emulation attacker does not aim at causing interference to PUs and, according to Araujo et al. [42], PU emulation is the most studied attack against CR.

Various approaches may be followed to achieve PU detection, namely energy detection, feature detection, and matched filtering [4]. The detection of PU activity through energy detection is the mostly used approach, namely due to its simplicity of implementation and because it does not require any *a priori* information about each PU transmission characteristics [4,20,43]. This detection scheme checks the received power against a given threshold and does not investigate any particular characteristic of the signals. However, energy detection also facilitates attacks from non-sophisticated adversaries, given the simplicity of generating a signal with a particular energy level in the same frequency as the PU. In fact, it is the most susceptible detection scheme to PU emulation attacks [43]. The employment of more advanced spectrum sensing methods also does not provide effective protection against security attacks, as they simply require more sophisticated attackers.

We must also consider the possibility of attackers being able to predict which channels will be used by the SUs and emulate PU activity on those specific channels, increasing significantly the effectiveness of the attacks [44]. In fact, a PU emulation attack can result in a DoS attack to a legitimate SU when the attacker has enough intelligence to transmit a fake signal on the selected channel any time that SU performs sensing [45]. We note that it is not reasonable or efficient for an attacker to emulate PU activity continuously due to energy concerns [46]. Therefore, an attacker should have sensing and learning capabilities similarly to the SUs. Naqvi, Murtaza, and Aslam [45] define a smart PU emulation attacker as one that emulates PU activity exclusively during sensing times in the CR network. A greedy attacker uses the channel after it was sensed as busy by the legitimate SUs it successfully fooled, while a malicious attacker remains silent. Haghighat and Sadough [46] define a smart attacker as an attacker that only transmits fake signals during the absence of PU activity. In their work, they also show that a smart attacker produces the same level of disruption as when transmitting continuously, although at the expense of less energy spent. In their work, Yu et al. [47] state that a successful PU emulation attack requires the attackers to be able to track and learn the characteristics of primary signals and avoid interfering with the primary network. In this context, features and approaches other than spectrum sensing are required to identify PU emulation attacks, as we proceed to discuss.

1.4.2.1 Location- and distance-based approaches Most existing proposals address the detection of PU emulation attacks by estimation of the location of the transmitters and comparing it with the *a priori* known locations of the legitimate PUs, as in IEEE 802.22 through the access to geo-location databases [5,6,43,44,48,49]. If the estimated location of an emitter deviates from the known locations of the PUs, then the likelihood of this being a PU emulation attacker increases. Therefore, it is usual to assume that each SU is equipped with a positioning device enabling self-positioning capabilities [41,43,49], in particular using Global Position System (GPS) for absolute location information (i.e., defining the position in a system of coordinates) [14,50]. However, GPS presents various limitations, as it may not be available for all nodes in the network, is not appropriate for indoor usage, is inefficient in terms of power consumption, and may represent

an additional cost not always supportable [51,52]. Despite such difficulties, Celbi and Arslan [14] state that location awareness is an essential characteristic of SUs and that they should be able to realize seamless positioning and interoperability between different positioning systems.

Having the locations of the legitimate PUs known to all the SUs is a linear task in the absence of PU mobility, such as with television towers or cellular base stations, and considering that geo-location databases are available. However, such requirements may be either challenging or impossible in many CR scenarios. Idoudi, Daimi, and Saed [53] state that existing solutions against PU emulation attacks do not handle PU and SU mobility appropriately. For example, Yuan et al. [44] only consider the possibility of television transmitters in their proposal, i.e., PUs with fixed and known PU locations. The cooperative solution that is proposed by León, Hernández-Serrano, and Soriano [54], which specifically targets centralized IEEE 802.22 networks, is based on the same assumption and thus cannot cope with the emulation of PUs that have unknown locations (e.g., wireless microphones), despite its ability to precisely determine the locations of received signals. Blesa et al. [55] state that countermeasures based on geo-location are not appropriate for scenarios with mobile PUs and SUs, and, according to Araujo et al. [42], mobile attackers can take advantage of their mobility in order to remain undetected. We note that Peng, Zeng, and Zeng [56] propose what they argue to be the first PU emulation detection solution considering mobile attackers. Xin and Song [5] present a PU emulation attack detection scheme, designated as Signal Activity Pattern Acquisition and Reconstruction System (SPARS), which does not use any *a priori* knowledge of PUs. They argue that, in contrast with existing solutions on PU emulation detection, SPARS can be applied to all types of PUs.

The accurate determination of the location of the transmitter of a given signal in relative terms (i.e., when compared to the position of the receiving SU) is in general a challenging task. Several practical mechanisms have been proposed for wireless nodes to perform direct distance measurements [57], and the most common current approach is to derive the distance between the transmitter and the receiver based on the signal strengths (RSS) of the received signals [37]. This computation requires knowledge about the emitter's transmission power, the usage of an accurate propagation model, and a statistical model of phenomena such as background noise [22]. We may however consider such methods to be limited in terms of accuracy, as the measured values can fluctuate even in small areas due to numerous adverse factors, such as fading or the presence of obstacles [50]. Other approaches are possible for automated distance determination, such as having the nodes equipped with arrays of directional antennas that enable determining the angles of arrival (AoA) of the received signals using trigonometric techniques [57]. When compared to the usage of RSS, this approach has the advantage of not requiring any *a priori* knowledge about the transmission power used by the transmitter, being more precise, and enabling the determination of relative positions instead of merely the distances to PUs. In particular, if a node is equipped with a minimum of two antennas, the location of the emitter of a signal can be computed by the cross point of two lines with the corresponding incoming angles. Nevertheless, we may observe that RSS is still the prime candidate for range measurements, mainly due to its simplicity and low cost.

The estimation of the distances to the transmitters of the received signals using RSS values is employed by most of the existing proposals addressing the detection of PU emulation attacks [56]. However, as the transmission power of attackers is not known by the SUs and can vary over time if they have power control capabilities, estimating the distance to the sources of the signals requires additional features. A possible approach consists in deploying an additional network of sensors to cooperatively determine the locations of the transmitters and, therefore, of the potential PU emulation attackers, such as in the proposal of Chen, Park, and Reed [48]. In this context, Jin, Anand, and Subbalakshmi [43] also discuss that most existing proposals assume this type of approach for the localization of malicious nodes.

The proposal of Yuan et al. [44], designated as belief propagation, is also based on RSS and on the comparison of the location of suspect attackers with the *a priori* known locations of the legitimate PUs. However, Yuan et al. [44] propose an alternative solution that intends to detect PU emulation attacks regardless of the locations and transmission powers of the attackers. This proposal avoids the utilization of an additional sensor network and of expensive hardware, does not require estimating the exact location of PU emulation suspects, and assumes a simple energy detection approach. As the SUs have no idea about the transmission power of the potential attacker and the distance to it, a cooperative scheme enables each SU to compare the distribution of the observed RSS values in order to estimate the locations of the suspect transmitters and build a belief about a particular sender being an attacker or not. These beliefs are iteratively exchanged and updated among the various SUs. After convergence, if the mean of the final beliefs is below a defined threshold, the source of the signal is considered to be an attacker. In this case, all the SUs are informed about the characteristics of the PU emulation attacker and ignore its activity. Despite the interest of belief propagation approaches, we also observe that they usually lack validation in real implementation scenarios, and that may be costly from the point of view of the

number of observations that a secondary user may be required to perform.

The proposal of Jin, Anand, and Subbalakshmi [43] is another example that assumes neither advanced features from the SUs nor the usage of sensor nodes dedicated to assist in determining the source locations of the received signals. As in various existing proposals, this work considers that energy detection is used and that the locations of the PUs are known to all the SUs. On the contrary of Yuan et al. [44], in this proposal there is no cooperation between the SUs and, therefore, no propagation of local beliefs concerning PU emulation attacks. Jin, Anand, and Subbalakshmi [43] propose the utilization and combination of two hypothesis tests in order for each SU to detect PU emulation attacks. A Neyman-Pearson composite hypothesis test [43] enables a secondary user to distinguish between a legitimate PU and an attacker, considering some constraints on the miss probability of a positive detection. An alternative approach is also discussed, based on the usage of a Wald's sequential probability test enabling a secondary user to set thresholds for both false alarm and miss probabilities, possibly at the cost of more radio observations required to arrive at a decision.

1.4.2.2 Cryptographic approaches Regarding PU detection, it is important to note that other methods not based on any *a priori* knowledge on the location of PUs can be developed, in particular by integrating security-related data with signals from primary users. Possible directions consist in including cryptographic signatures within such signals, or using integrity and authentication mechanisms for communications between primary and secondary CR users. In the context of practical CR applications, such approaches must guarantee compatibility with regulatory decisions such as those from the Federal Communications Commission (FCC), which states that the utilization of available spectrum by SUs should be possible without requiring any modification to the incumbent users and their signals. Therefore, PU authentication is a challenging issue and existing proposals are subject to practical limitations [53]. Kim, Chung, and Choo [58] discuss that this restriction limits the accuracy of secure distributed spectrum sensing schemes in CR networks. For example, the proposal of Borle, Chen, and Du [59] employs a physical layer authentication scheme based on cryptographic signatures to address PU emulation attacks. The proposed scheme is transparent to the primary receivers but inevitably requires some level of modification to the primary transmitters. The PU emulation attack defense solution that Alahmadi et al. [60] propose targets digital television networks and also requires modifying the primary transmitters, such that they generate reference signals encrypted through the Advanced Encryption Standard (AES) algorithm. The authors state that their approach only requires equipping the primary transmitters with a commercially available AES chip, while we note that the SUs and the PUs must also have a shared secret, so further work in the context of key management should be addressed.

In the context of the cryptographic approaches, Liu, Ning, and Dai [61] propose the integration of signatures with RSS information by employing a helper node that is physically close to the PU, in order to enable the SUs to verify transmissions from the PU and decide on its legitimacy. This proposal integrates cryptographic signatures and wireless link signatures derived from physical radio channel characteristics (such as channel impulse responses). A SU may thus verify the signatures carried by the helper node's signals and thus obtain the helper node's (authenticated) link signatures from which it may derive the legitimacy of the primary node's transmissions. We may again consider that the limitation of this approach may be in the cost of the usage and deployment of dedicated helper nodes, particularly considering that its physical proximity to a PU is an important requirement of the effectiveness of this approach.

We finally note that detecting PU emulation must not be considered to be an end by itself. Countermeasure solutions must be developed in order to invalidate the effects and goals of such attacks and preferentially to prevent their occurrence by building security at the foundations of CR environments. This is probably the most challenging and unexplored issue in this context. Nevertheless, most existing works on PU emulation attack only target its detection [45]. Actually, the foundations of the CR paradigm inherently enable the SUs to circumvent PU emulation attacks even when they are not detected. That is, with CR, a SU determines which channels are busy and selects one of them if any exists. Upon the detection of activity on a channel being used for secondary transmission, either it is a primary or fake signal, the secondary transmitter must go through a spectrum handoff process (i.e., transmission is interrupted and resumed on a new channel) [47]. Therefore, according to Xin and Song [5], it is not really relevant for a SU to determine if a busy channel results from legitimate PU traffic or any emulation attack, since it reacts similarly. Xin and Song [5] also state that when an attacker realistically mimics the activity pattern of the PUs, the resulting interference is tolerable by the CR network. That is, CR has been designed to cope with a mild disruption from PUs and, therefore, they can tolerate PU emulation attacks that cause similar types of disruption. However, we note that this CR native feature is not effective when a PU emulation attack is performed by an intelligent attacker that has knowledge about the internals of the CR networks, i.e., that can guess the next channel to be selected by a SU, or when the attack is

launched on different channels simultaneously by coordinated malicious nodes [5,53]. Under such circumstances, service disruption of SUs due to busy channels considerably increases and might result in DoS when the affected SUs fail in finding a vacant channel [47,53].

Concerning smart PU emulation attacks [45,46], malicious attackers remain silent during secondary transmission slots in order to save energy, and greedy attackers use the channel if it is effectively vacant (i.e., without PU traffic). Based on this assumption, Naqvi, Murtaza, and Aslam [45] propose a strategy that enables detecting and mitigating malicious PU emulation attacks. Their solution is based on allowing the SUs to perform sensing at random intervals other than the regular ones, i.e., when the attacker is supposedly quiet. That is, a SU senses the intended channel out of the sensing periods expected by the attacker and uses the remaining time slot to transmit data if the channel is actually vacant. According to Naqvi, Murtaza, and Aslam [45], their proposal is the only one that, beyond identifying PU emulation attacks, also provides countermeasures against this type of threat. Yu et al. [47] suggest that the utilization of a guard channel is a simple but effective solution to mitigate the effect of PU emulation attacks in CR networks. They also propose a defense strategy that includes reserving a portion of channels for spectrum handoff in order to reduce the resulting rate of secondary service disruption.

2 Conclusions

Cognitive radio is a highly multidisciplinary area currently attracting numerous research efforts, which provides a large number of challenges regarding security and accurate sensing [62]. As previously discussed, this survey is focused particularly on security in the context of primary user detection, particularly in what concerns two major types of attacks: primary user emulation and spectrum sensing data falsification. The importance of such attacks is also related to the fact that they may in fact compromise the feasibility of CR solutions and applications. As in other communication approaches, we may expect security to represent a fundamental enabling factor of future CR applications.

As discussed throughout the survey, in practical terms, improvements and new solutions are required to properly address the described security threats. Despite the usefulness and interest of most of the proposals previously discussed, many of them are not practical from a deployment point of view. For instance, many current proposals require the deployment of additional sensors (helping devices) or the comparison of observations against characteristics known *a priori*, particularly the locations of the PUs. The cost of such solutions, the unavailability of location information, or the lack of accuracy of the positioning mechanisms may complicate the design and effectiveness of new security approaches. Also, the assumption about the primary users' locations being known *a priori* may be both simplistic and unrealistic. In our point of view, these are the main issues still open regarding the identification of attacks against the detection of PU activity, one major open issue regarding security in CR environments.

Recent technologies such as IEEE 802.16 Worldwide Interoperability for Microwave Access (WIMAX) are expected to contribute to increase the number of mobile primary users in a near future, and in consequence mobility and variable topologies will be a reality in many environments. In consequence, advanced security solutions not assuming *a priori* knowledge of the location of the PUs must be investigated and properly evaluated in real deployment environments. On the other hand, in scenarios where such information may be available, security may benefit from the utilization of cost-effective and accurate positioning techniques.

In terms of security, distributed CR networks may provide a better approach than centralized approaches, despite complicating the design of appropriate mechanisms. By allocating spectrum and security decisions to several SUs, the risk of DoS attacks against a single point of failure (i.e., the central entity) is eliminated. In this context, clustering schemes may be an intermediate alternative, with each cluster having its own central entity (i.e., decision and fusion center) and the SUs being able to elect another central entity or migrate to another cluster in case of failure or attack.

Future developments on security for CR network environments may also involve standardization efforts in the context of normalization entities workforces, such as the European Telecommunications Standards Institute (ETSI) Reconfigurable Radio Systems (RRS) Technical Committee (TC). This TC is currently active in the standardization of CR systems and also in the addressing of security threats [62]. In the same context as IEEE 802.22, the European Computer Manufacturers Association (ECMA)-392 workgroup aims at designing mechanisms to enable wireless devices to exploit the white spaces in the television frequency bands. Soto and Nogueira [17] state that, despite recently proposed protocols, architectures, and standards already including security (e.g., see IEEE 802.11 SCMP in Section 1.4), they use conventional techniques that are not sufficient to prevent CR networks from the attacks described in this survey. We also believe that reviewing existing limitations in normalization activities, such as FCC specifying that no modifications are allowed on primary networks, can contribute to make identifying PU emulation attacks less challenging, even when PUs are mobile and not known *a priori*.

As for the current Internet architecture and communications technologies, we may expect research and standardization work to provide equally important contributions in the addressing of security in future open CR environments. Overall, primary user detection will subsist as a fundamental network operation, and security will certainly be required to provide appropriate protection against the usage of spurious information, which can otherwise compromise the applicability of CR.

Competing interests
The authors declare that they have no competing interests.

Acknowledgements
The authors would like to acknowledge the support of project Intelligent Computing in the Internet of Services (iCIS; reference CENTRO-07-0224-FEDER-002003).

Author details
[1]Instituto Politécnico de Coimbra, ISEC, DEIS, Rua Pedro Nunes - Quinta da Nora, 3030-199 Coimbra, Portugal. [2]DEI-UC - Department of Informatics Engineering, University of Coimbra, Pólo II - Pinhal de Marrocos, 3030-290 Coimbra, Portugal. [3]CISUC - Centre for Informatics and Systems of the University of Coimbra, Pólo II - Pinhal de Marrocos, 3030-290 Coimbra, Portugal.

Received: 16 December 2014 Accepted: 19 March 2015
Published online: 11 April 2015

References
1. IF Akyildiz, WY Lee, MC Vuran, S Mohanty, NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. Comput. Netw. **50**(13), 2127–2159 (2006)
2. J Mitola, G Maguire, Cognitive radio: making software radios more personal. IEEE Personal Commun. **6**(4), 13–18 (1999)
3. L Lu, X Zhou, U Onunkwo, GY Li, Ten years of research in spectrum sensing and sharing in cognitive radio. EURASIP J. Wirel. Commun. Netw. **2012**(1), 1–16 (2012)
4. J Marinho, E Monteiro, Cognitive radio: survey on communication protocols, spectrum decision issues, and future research directions. Wireless Net. **18**(2), 147–164 (2012)
5. C Xin, M Song, Detection of PUE attacks in cognitive radio networks based on signal activity pattern. IEEE Transact. Mobile Comput. **13**(5), 1022–1034 (2014)
6. A Fragkiadakis, E Tragos, I Askoxylakis, A survey on security threats and detection techniques in cognitive radio networks. IEEE Commun. Surveys Tutorials **15**(1), 428–445 (2013)
7. A Attar, H Tang, AV Vasilakos, FR Yu, VCM Leung, A survey of security challenges in cognitive radio networks: solutions and future research directions. Proceedings IEEE **100**(12), 3172–3186 (2012)
8. G Baldini, T Sturman, AR Biswas, R Leschhorn, G Godor, M Street, Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead. IEEE Commun. Surveys Tutorials **14**(2), 355–379 (2012)
9. AC Sumathi, R Vidhyapriya, *Security in Cognitive Radio Networks - A Survey. 12th International Conference on Intelligent Systems Design and Applications, ISDA 2012*, 2012, pp. 114–118
10. W El-hajj, H Safa, M Guizani, Survey of security issues in cognitive radio networks. J. Internet Tech. **12**(2), 181–198 (2011)
11. O León, J Hernández-Serrano, M Soriano, Securing cognitive radio networks. Int. J. Commun. Systems **23**(5), 633–652 (2010)
12. IEEE 802.22 WRAN WG Website. http://www.ieee802.org/22/. Accessed 31 July 2012.
13. P Ren, Y Wang, Q Du, J Xu, A survey on dynamic spectrum access protocols for distributed cognitive wireless networks. EURASIP J. Wirel. Commun. Netw. **2012**(60), 1–21 (2012)
14. H Celebi, H Arslan, Utilization of location information in cognitive wireless networks. IEEE Wireless Commun. **14**(4), 6–13 (2007)
15. AN Mody, R Reddy, T Kiernan, TX Brown, *Security in Cognitive Radio Networks: An Example Using the Commercial IEEE 802.22 Standard. IEEE Military Communications Conference, MILCOM 2009*, 2009, pp. 1–7
16. TC Clancy, N Goergen, *Security in Cognitive Radio Networks: Threats and Mitigation. IEEE 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2008*, 2008, pp. 1–8
17. J Soto, M Nogueira, A framework for resilient and secure spectrum sensing on cognitive radio networks. Comput. Netw. **79**, 313–322 (2015)
18. J Chen, L Jiao, J Wu, X Wang, Compressive spectrum sensing in the cognitive radio networks by exploiting the sparsity of active radios. Wireless Net **19**(5), 661–671 (2013)
19. B Lo, I Akyildiz, Reinforcement learning for cooperative sensing gain in cognitive radio ad hoc networks. Wireless Net **19**(6), 1237–1250 (2013)
20. W Wang, H Li, Y Sun, Z Han, Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks. EURASIP J. Adv. Sig. Pr. **2010**, 1–15 (2010)
21. K Zeng, P Paweczak, D Cabric, Reputation-based cooperative spectrum sensing with trusted nodes assistance. IEEE Commun. Letters **14**(3), 226–228 (2010)
22. T Clouqueur, P Ramanathan, KK Saluja, KC Wang, *Value-fusion versus decision-fusion for fault-tolerance in collaborative target detection in sensor networks. Proceedings of the Fourth International Conference on Information Fusion*, 2001, pp. 25–30
23. AC Malady, C Silva, Clustering methods for distributed spectrum sensing in cognitive radio systems. IEEE Military Commun. Conference MILCOM **2008**, 1–5 (2008)
24. A Nasipuri, K Li, *Collaborative Detection of Spatially Correlated Signals in Sensor Networks. Proceedings of the 2005 International Conference on Telecommunication Systems Modeling and Analysis*, 2005, pp. 17–20
25. O Fatemieh, R Chandra, CA Gunter, *Secure Collaborative Sensing for Crowd Sourcing Spectrum Data in White Space Networks. IEEE Symposium on New Frontiers in Dynamic Spectrum*, 2010, pp. 1–12
26. B Khaleghi, A Khamis, FO Karray, SN Razavi, Multisensor data fusion: a review of the state-of-the-art. Info Fusion **14**(1), 28–44 (2013)
27. JL Burbank, *Security in cognitive radio networks, The required evolution in approaches to wireless network security. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2008*, 2008
28. R Chen, JM Park, YT Hou, JH Reed, Toward secure distributed spectrum sensing in cognitive radio networks. IEEE Commun. Magazine **46**(4), 50–55 (2008)
29. CY Chen, YH Chou, HC Chao, CH Lo, Secure centralized spectrum sensing for cognitive radio networks. Wireless Net **18**(6), 667–677 (2012)
30. H Rifà-Pous, C Garrigues, Authenticating hard decision sensing reports in cognitive radio networks. Comput. Netw. **56**(2), 566–576 (2012)
31. Y Zhang, N Meratnia, P Havinga, Outlier detection techniques for wireless sensor networks: a survey. IEEE Commun. Surveys Tutorials **12**(2), 159–170 (2010)
32. C Chen, M Song, CS Xin, CoPD: a conjugate prior based detection scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks. Wireless Net **20**(8), 2521–2528 (2014)
33. AW Min, KG Shin, X Hu, *Attack-tolerant distributed sensing for dynamic spectrum access networks. 17th IEEE International Conference on Network Protocols, ICNP 2009*, 2009, p. 294
34. J Wang, IR Chen, *Trust-based data fusion mechanism design in cognitive radio networks. 2014 IEEE Conference on Communications and Network Security, CNS*, 2014, pp. 53–59
35. H Li, Z Han, *Catching Attacker(s) for Collaborative Spectrum Sensing in Cognitive Radio Systems: An Abnormality Detection Approach* (Spectrum, IEEE Symposium on New Frontiers in Dynamic, 2010), pp. 1–12
36. C Chen, M Song, C Xin, M Alam, *A robust malicious user detection scheme in cooperative spectrum sensing. 2012 IEEE Global Communications Conference, GLOBECOM*, 2012, pp. 4856–4861
37. Y Yang, Y Liu, Q Zhang, L Ni, *Cooperative boundary detection for spectrum sensing using dedicated wireless sensor networks. IEEE International Conference on Computer Communications, INFOCOM*, 2010, pp. 1–9
38. M Atakli, H Hu, Y Chen, WS Ku, Z Su, *Malicious node detection in wireless sensor networks using weighted trust evaluation. Proceedings of the 2008 Spring Simulation Multiconference*, 2008, p. 836
39. T Suen, A Yasinsac, *Peer identification in wireless and sensor networks using signal properties. IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, 2005
40. J Li, Z Feng, Z Wei, Z Feng, P Zhang, Security management based on trust determination in cognitive radio networks. EURASIP J. Adv. Sig. Pr **2014**(1), 1–16 (2014)
41. L Tingting, S Feng, Research on hidden malicious user detection problem. Sec. Commun. Net. **7**(6), 958–963 (2014)

42. A Araujo, J Blesa, E Romero, D Villanueva, *Security in cognitive wireless sensor networks. Challenges and open problems. EURASIP Journal on Wireless Communications and Networking 2012*, 2012
43. Z Jin, S Anand, KP Subbalakshmi, Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing mobile computing and communications. ACM SIGMOBILE Mobile Comput. Commun. Rev **13**(2), 74–85 (2009)
44. Z Yuan, D Niyato, H Li, JB Song, Z Han, Defeating primary user emulation attacks using belief propagation in cognitive radio networks. IEEE J. Selec. Areas Commun **30**(10), 1850–1860 (2012)
45. B Naqvi, S Murtaza, B Aslam, *A mitigation strategy against malicious primary user emulation attack in cognitive radio networks. 2014 IEEE International Conference on Emerging Technologies, ICET*, 2014, pp. 112–117
46. M Haghighat, SMS Sadough, *Smart primary user emulation in cognitive radio networks: defence strategies against radio aware attacks and robust spectrum sensing. Transactions on Emerging Telecommunications Technologies 2014*, 2014. doi:10.1002/ett.2848
47. R Yu, Y Zhang, Y Liu, S Gjessing, M Guizani, Securing cognitive radio networks against primary user emulation attacks. arXiv preprint arXiv **1308**, 6216 (2013)
48. R Chen, JM Park, JH Reed, Defense against primary user emulation attacks in cognitive radio networks. IEEE J. Selec. Areas Com **26**(1), 25–37 (2008)
49. R Chen, JM Park, *Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks. 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, SDR '06*, 2006, pp. 110–119
50. D Niculescu, Positioning in ad hoc sensor networks. IEEE Net **18**(4), 24–29 (2004)
51. F Franceschini, M Galetto, D Maisano, L Mastrogiacomo, A review of localization algorithms for distributed wireless sensor networks in manufacturing. Int. J. Comput. Integ. Manufac **22**(7), 698–716 (2009)
52. B Xiao, H Chen, S Zhou, *A walking beacon-assisted localization in wireless sensor networks. IEEE International Conference on Communications, ICC'07*, 2007, pp. 3070–3075
53. H Idoudi, K Daimi, M Saed, *Security Challenges in Cognitive Radio Networks. Proceedings of the World Congress on Engineering*, 2014
54. O León, J Hernández-Serrano, M Soriano, Cooperative detection of primary user emulation attacks in CRNs. Comput. Netw. **56**(14), 3374–3384 (2012)
55. J Blesa, E Romero, A Rozas, A Araujo, PUE attack detection in CWSNs using anomaly detection techniques. EURASIP J. Wireless Com. Net. **2013**(1), 1–13 (2013)
56. P Kai, Z Fanzi, Z Qingguang, *A New Method to Detect Primary User Emulation Attacks in Cognitive Radio Networks. 3rd International Conference on Computer Science and Service System, CSSS 2014*, 2014, pp. 674–677
57. C Savarese, JM Rabaey, J Beutel, *Location in distributed ad-hoc wireless sensor networks. IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP'01*, 2001, pp. 2037–2040
58. M Kim, MY Chung, H Choo, VeriEST: verification via primary user emulation signal-based test for secure distributed spectrum sensing in cognitive radio networks. Sec. Com. Net **5**(7), 776–788 (2012)
59. KM Borle, B Chen, W Du, *A physical layer authentication scheme for countering primary user emulation attack* (IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP, 2013), pp. 2935–2939
60. A Alahmadi, M Abdelhakim, J Ren, T Li, Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. IEEE Transac. Info. Forensics Sec **9**(5), 772–781 (2014)
61. Y Liu, P Ning, H Dai, *Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptography and Wireless Link Signatures. 2010 IEEE Symposium on Security and Privacy*, 2010, pp. 286–301
62. VT Nguyen, F Villain, YL Guillou, Cognitive radio RF: overview and challenges. VLSI Design **2012**, 1–13 (2012). doi:10.1155/2012/716476