Location Privacy in Cognitive Radio Networks: A Survey

Article *in* IEEE Communications Surveys & Tutorials · April 2017

DOI: 10.1109/COMST.2017.2693965

1 author:

Mohamed Grissa
Oregon State University
7 PUBLICATIONS **16** CITATIONS

SEE PROFILE

Location Privacy in Cognitive Radio Networks: A Survey

Mohamed Grissa, Bechir Hamdaoui and Attila A. Yavuz
Oregon State University, Corvallis, OR 97331, grissam,hamdaoui,attila.yavuz@oregonstate.edu

***Abstract*—Cognitive radio networks (CRNs) have emerged as an essential technology to enable dynamic and opportunistic spectrum access which aims to exploit underutilized licensed channels to solve the spectrum scarcity problem. Despite the great benefits that CRNs offer in terms of their ability to improve spectrum utilization efficiency, they suffer from user location privacy issues. Knowing that their whereabouts may be exposed can discourage users from joining and participating in the CRNs, thereby potentially hindering the adoption and deployment of this technology in future generation networks. The location information leakage issue in the CRN context has recently started to gain attention from the research community due to its importance, and several research efforts have been made to tackle it. However, to the best of our knowledge, none of these works have tried to identify the vulnerabilities that are behind this issue or discuss the approaches that could be deployed to prevent it. In this paper, we try to fill this gap by providing a comprehensive survey that investigates the various location privacy risks and threats that may arise from the different components of this CRN technology, and explores the different privacy attacks and countermeasure solutions that have been proposed in the literature to cope with this location privacy issue. We also discuss some open research problems, related to this issue, that need to be overcome by the research community to take advantage of the benefits of this key CRN technology without having to sacrifice the users' privacy.**

***Keywords*—** Location privacy, cognitive radio networks, dynamic spectrum access, privacy preserving protocols.

I. Introduction

Cognitive radio networks (CRNs) have been widely adopted as an efficient way to improve the spectrum utilization efficiency and alleviate the spectrum scarcity crisis caused by the huge demand on radio frequency resources. This technology has several applications and is considered as one of the main enablers for 5G wireless networks to deal with its stringent spectrum requirement. This paradigm, first coined by Mitola [1], could be thought of as an intelligent wireless communication system that is aware of its surrounding and that can adapt dynamically to the changes in the RF environment. It enables *dynamic spectrum access* (DSA) and improves the spectrum utilization efficiency by allowing unlicensed/secondary users (SUs) to exploit unused spectrum bands of licensed/primary users (PUs). That is, SUs can opportunistically use unused spectrum bands (aka spectrum holes or white spaces), which are defined by FCC as the channels that are unused at a specific location and time [2], so long as doing so does not cause harmful interference to PUs.

A. The CRN location privacy problem

Despite its great potential for improving spectrum utilization efficiency, the CRN technology suffers from serious privacy and security risks. Although the survey covers location privacy issues arising at the various CRN components, for motivation purposes, we focus in this section on the *spectrum discovery component* only, in which white spaces are identified using either the *cooperative spectrum sensing* or the *database-driven spectrum access* functions.

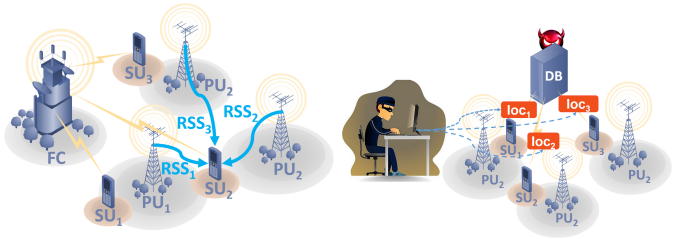
1) Cooperative spectrum sensing

In cooperative sensing, a central entity called Fusion Center (FC) orchestrates the sensing operations as follows: It selects one channel for sensing and, through a control channel, requests that each SU perform local sensing on that channel to detect the presence of PU signals and send its sensing report back to it. Fusion Center then combines the received sensing reports, makes a decision about the channel availability, and diffuses the decision back to the SUs. Here, a sensing report is essentially a sensed/measured quantity characterising some PU signal strength the SU observed on some PU channel, and what quantity the SU measures depends on the spectrum sensing method it uses (e.g., waveform [3], energy detection [4], cyclostationarity [5], etc.; see Section II-A1 for more details). For example, when using the energy detection method, the sensed quantity is the energy strength of the sensed PU signal, often referred to as **received signal strength** (RSS) [6].

In cooperative sensing, communications between SUs and Fusion Center could be done via one of the following: (i) direct, single-hop wireless links; (ii) multi-hop links (with first link being wireless); (iii) wired links (whether single or multiple hops). In the first and second types, location privacy information can be easily leaked by observing the wireless radio signals sent by SUs to Fusion Center. In this case, existing (mostly mature) location privacy preservation technologies (e.g., see [7], [8] for sensor, [9] for WiFi and [10] for cellular) can be applied here to protect the location privacy of SUs during cooperative sensing. In the third communication type when SUs communicate with Fusion Center via wired links, wireless signal-based localization techniques can no longer be used here to locate SUs.

However, unlike traditional wireless networks, in the case of cooperative sensing, preventing leakage of location information from wireless signals (e.g., by communicating via wired links) does not guarantee the preservation of SUs' location privacy. This is because location information can also be leaked from the sensing reports sent by SUs to the Fusion Center during cooperative sensing [11]. Recall that a sensing report is essentially the received signal strength (RSS) value of some PU signal that the SU observed on a specific PU channel. And it has been shown that these values are highly correlated to the physical location of the

reporting SU [11]. Now Fusion Center may know the actual physical locations of few PUs as well as the channels these PUs communicate on, and thus, by knowing the RSS values measured by an SU on each of these PU channels, Fusion Center can easily locate the SU. Some illustrative scenarios, showing how Fusion Center can easily infer the physical locations of SUs by simply looking at few sensing reports on different PU channels, are given in [11]. This is also illustrated in Figure 1(a).



(a) Cooperative sensing (b) DB-driven access

Figure 1: Location privacy issues during spectrum discovery

2) Database-driven access

In database-driven spectrum access, spectrum availability information is provided to SUs by querying a spectrum database, often maintained and controlled by a third party (e.g., Google, Spectrum Bridge, RadioSoft, etc.). Here, although SU queries' final destination is the database, which is often located far away from the SUs, location information can also be leaked from wireless radio signals if the SUs' first hop is a wireless link; e.g., a cellular base station or a WiFi access point. In this case, the aforementioned, existing location privacy preservation techniques that overcome wireless signal-based leakage can also be applied to protect SUs' location privacy. However, as illustrated in Figure 1(b), there is a more straightforward location privacy threat specific to the database-driven access method: In order for an SU to acquire spectrum availability information, it is required to query the database with its physical location, so that the database can inform it about spectrum availability in its vicinity. This explicit exposure of SUs' location information to third (commercial) parties raises serious privacy concerns and has some undesired consequences, as discussed next.

B. Why worry about location information privacy?

Most users will not be okay with having their whereabouts and private location information made public, especially in the presence of malicious entities that may be eager to exploit this information for malicious purposes and to gain more knowledge about other sensitive and private information. A survey conducted in 2015 by Pew Research found that "*Most Americans hold strong views about the importance of privacy in their everyday lives*", and that "*These feelings also extend to their wishes that they be able to maintain privacy in their homes, at work, during social gatherings, at times when they want to be alone and when they are moving around in public*"(Madden et al. [12]). This same survey also reports that "*90% say that controlling what information is collected about them is important*" and "*88% say it is important that they not have someone watch or listen to them without their permission*". For instance, with an operation as simple as a succession of database accesses, a database can easily monitor and track the SU's daily life activities and communications, allowing the database to learn various behavioral information about the user; e.g., where he/she goes for shopping, which social circles he/she attends, and where and when he/she eats. As spectrum databases are being managed by business entities, such a private information is at the risk of being sold and shared with other commercial entities. Indeed, a SU's fine-grained location information, when combined with other publicly available information, could easily be exploited to infer other personal information about an individual including his/her behavior, preferences, personal habits or even beliefs. For instance, an adversary can learn an individual's religious belief by observing that a he/she frequently visits places with religious affiliations. Location traces could also reveal some information about the health condition of a user if the adversary observes that the user regularly goes to a hospital for example. The frequency and duration of these visits can even reveal the seriousness of a user illness and even the type of illness if the location corresponds to that of a specialty clinic. The adversary could sell this health information to pharmaceutical advertisers without the user's consent. Moreover, malicious adversaries with criminal intent could use the location information to pose a threat to individuals' security and privacy; for instance, they can commit crimes of theft and burglary when users are absent.

We envision that the public's acceptance of the dynamic and opportunistic spectrum sharing paradigm will greatly depend on the robustness and trustworthiness of CRNs vis-a-vis of their ability to address these privacy concerns. It is, therefore, imperative that techniques and tools to be developed by the research community for CRNs be enabled with privacy preserving capabilities that protect the location privacy of SUs while allowing them to harness the benefits of the CRN paradigm without disrupting the functionalities that these techniques are designed for to promote *dynamic spectrum access*.

C. Location privacy protection: pros and cons

Ensuring that the location privacy information of SUs is protected has great benefits. First and most importantly, it promotes dynamic and opportunistic sharing of spectrum resources, thereby increasing spectrum utilization efficiency. Knowing that their location privacy is protected so that they do not have to worry about their whereabouts being tracked and their privacy being compromised, SUs will be encouraged to participate in the cooperative spectrum sensing process, and to query spectrum databases for spectrum availability. Ensuring location privacy protection can also be beneficial to PUs. For example, being concerned that their location privacy information may be leaked to spectrum databases, SUs may attempt to use PU channels without registering and querying spectrum databases for spectrum availability, thereby causing harmful interference to PUs.

Providing location privacy preservation guarantees cannot, however, be done without a cost. It does introduce additional communication, computation and storage overheads, which

TABLE I: Pros and cons of preserving the location privacy of SUs

	Pros	Cons
SU	- Encourages SUs to participate in the cooperative spectrum sensing process, and hence in accurately locating spectrum opportunities. - Discourages SUs from using spectrum opportunities without checking for availability first, either through spectrum databases or cooperative sensing, and thus prevents SUs from violating secondary spectrum access policies. - Promotes dynamic spectrum sharing, and thus increases spectrum utilization efficiency and helps address the spectrum supply shortage problem.	- Incurs additional SUs' communication, computation, and storage overheads; this can be problematic when SUs are resource-limited devices (e.g., IoT devices, sensors, etc.). - Introduces delay in the process of querying spectrum databases for spectrum availability information in the case of database-driven CRN approach. - Introduces delay when locating and deciding about spectrum availability through the cooperative spectrum sensing approach.
PU	- Protects PUs from harmful interference that might come from SUs not willing to check for spectrum availability (either via the cooperative spectrum sensing approach or database-driven access approach) before using PU channels.	- Outdated spectrum availability information due to the delays incurred as a result of protecting the location privacy may lead to the use of occupied PU channels by SUs, thereby causing interference to PUs.

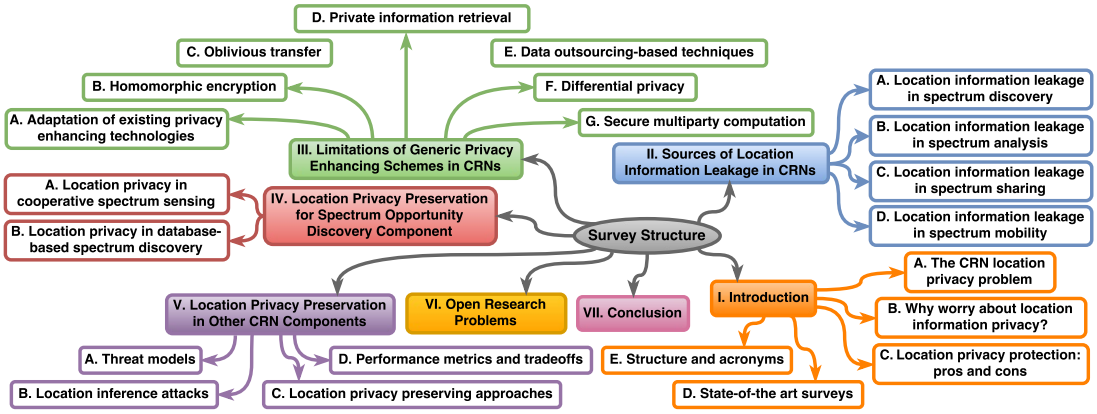


Figure 2: Survey structure

may, in turn, also introduce additional delay when it comes to learning about the availability status of some channel, and can, in the extreme case, make the spectrum availability information outdated, thus possibly resulting in using a channel that is not vacant. The pros and cons of providing location privacy protection are summarized in Table I.

D. State-of-the art surveys

There have been several existing works that investigate and address the various CRN vulnerabilities and security issues [13]–[17]. However, most of these survey works focus on security and privacy issues in general with little or no attention to the location privacy issue that we address in this survey. For instance, Mee et al. [15] present an extensive review on the use of reinforcement learning to achieve security enhancement in the context of CRNs while dealing with jamming and byzantine attacks. El-Hajj et al. [16] provide a per-layer classification of attacks targeting CRNs, and discuss existing countermeasure solutions that address these attacks. Sharma et al. [17] discuss security threats, attacks, and countermeasures in CRNs for both PUs and SUs with focus on the physical layer. There have also been few surveys that aimed at exploring location privacy issues, but they are generally not focusing on CRNs. For instance, Zhang et al. [18] present a high-level overview of fundamental approaches for user localization and privacy preservation but mainly in the context of location-based services (LBS). They also discuss this issue, but only briefly, in the context of indoor environments, wireless sensor networks, and cognitive radio networks. To the best of our knowledge, this is the first comprehensive survey that digs into the different privacy threats and attacks that target the location information of SUs at the different CRN components, along with the different techniques that have been proposed in the literature to mitigate and address these threats.

E. Structure and acronyms

This paper provides a comprehensive survey of the location privacy threats and vulnerabilities arising at the various components of CRNs, as well as the different techniques proposed in the literature to overcome these privacy issues. The general survey structure is depicted in Figure 2, and is as follows:

- Section II investigates the vulnerabilities and sources of location information leakage in CRNs, and provides insights on how these vulnerabilities could become potential threats to SUs' location privacy.
- Section III explores the privacy enhancing technologies (PETs) that are most relevant to CRNs. The goal is to show how these techniques, that are widely adopted in other contexts, could not be applied off-the-shelf as they are in the context of CRNs unless judiciously adapted to the unique requirements of CRNs.
- Sections IV and V discuss threats and attacks that have been identified in the literature with respect to the spectrum opportunity discovery component (Section IV), as

well as other CRN components (Section V). They also discuss their impacts on SUs' privacy, and investigate countermeasure solutions that have been proposed in the literature to deal with these attacks. These two sections also explore and present the different metrics used to assess and evaluate both the achievable performance and the privacy level of these proposed solutions.

- Section VI discusses unsolved research challenges pertaining to the location privacy in CRNs, with a special focus on the CR components that have received the least attention from the research community. It also discusses open research problems arising from alternative CRN architectures and from emerging CR-based technologies.
- Section VII concludes the survey.

For convenience, we summarize the used acronyms in Table II.

TABLE II: Acronyms

AoA	Angle of arrival
BS	Base station
CR	Cognitive radio
CRN	Cognitive radio network
DB	Spectrum database
DSA	Dynamic spectrum access
FC	Fusion center
FCC	Federal Communications Commission
GW	Gateway
MAC	Medium Access Control
MPC	Secure multiparty computation
MTP	Maximum transmit power
OPE	Order preserving encryption
$ORAM$	Oblivious random access memory
OT	Oblivious transfer
PET	Privacy enhancing technology
PIR	Private information retrieval
QoS	Quality of service
REM	Radio environment map
RSS	Received signal strength
$SINR$	Signal to interference-plus-noise ratio
SNR	Signal to noise ratio
SP	Service provider
SSE	Searchable symmetric encryption
SU	Secondary user
PU	Primary user
ToA	Time of arrival
$TDoA$	Time difference of arrival
WSN	Wireless sensor network

II. Sources of location information leakage in CRNs

CRNs need to perform a number of spectrum-aware operations to adapt to the dynamic spectrum environment. These operations form what is called a *cognition cycle* [1], [19]–[21], which mainly consists of four spectrum functions as shown in Figure 3: Spectrum opportunity discovery, spectrum analysis, spectrum sharing and spectrum mobility. Despite their merit in enhancing the spectrum utilization, CRNs may present some privacy risks to SUs especially in terms of their location privacy. In this section, we investigate the different aspects of the cognitive spectrum functions and we discuss the different threats that can compromise the location privacy of SUs in CRNs during the execution of these functions.

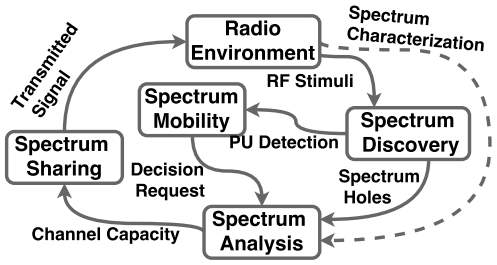


Figure 3: Cognitive radio cycle [20].

A. Location information leakage in spectrum discovery

This is considered to be one of the most important components of the cognition cycle, as it provides information about spectrum holes and PUs' presence. Mainly, there are two approaches to obtain this information: spectrum sensing, to be performed by SUs [22], and geolocation database. We first describe these two approaches, and then investigate the sources of location information leakage that they may have.

1) Spectrum sensing

Spectrum sensing enables SUs to be aware of their surroundings and to be able to identify spectrum holes in their vicinity so that they can exploit them opportunistically. It basically requires SUs to sense and detect primary signals without interfering with PU's transmissions [23], [24]. Spectrum sensing could be divided into two main functionalities, PU detection and cooperation, which are detailed next.

a) PU detection

The first step towards discovering spectrum opportunities is to detect PUs' signals. To do so, each SU needs to sense its local radio environment, as it is generally assumed not to have any prior knowledge about PUs' activities. We now present existing techniques that have been proposed in the literature to detect primary signals.

- *Energy detection [4]*: This is the simplest and the most popular approach for signal detection [25]. It is also considered as the optimal sensing approach when no information about the primary signal is available [26]. The presence or absence of a PU is decided by measuring PU signal's energy (aka the received signal strength (RSS)) on a target channel and comparing it against a detection energy threshold λ [6], [27].
- *Matched filter detection [28]*: It is considered as the optimal signal detection method [25], [29] as it maximizes the signal to noise ratio. It requires a full knowledge of PU's signal features such as modulation format, data rate, etc. It compares the known signal (aka template) with the input signal to detect the presence of the template signal in the unknown signal. The output of the matched filter is then compared to a predetermined threshold to decide on PU's presence or absence.
- *Cyclostationary detection [25], [30]*: PUs' transmitted signals are usually cyclostationary, i.e. their statistics exhibit periodicity [27]. Such a periodicity is usually introduced to the primary signals so that receivers can use it for timing and channel estimation purposes. But it can also be exploited for detecting PUs [21]. SUs can detect this periodicity in the modulated signals by

analyzing a spectral correlation function. This spectrum sensing technique is appealing because of its capability of differentiating the primary signal from noise and interference even in very low SNR environments [27].

- *Wavelet detection [3], [27]*: This method uses wavelet transform, an attractive mathematical tool used to investigate signal local regularity to analyze singularities and irregular structures in the power spectrum density caused by spectrum usage [21]. Wavelets are used for detecting edges, which are boundaries between spectrum holes and occupied bands, in the power spectral density (PSD) of a wideband channel.

Most of the above mentioned techniques are based on a set of measurements sampled at the Nyquist rate and can sense only one band at a time because of the hardware limitations [31]. In addition, sensing a wideband spectrum requires dividing it into narrow bands and making SU sense each band using multiple RF frontends simultaneously [31]. This may result in a very high processing time and hardware cost which makes these approaches not suitable for wideband sensing. Compressive sensing [32] is proposed to overcome these issues. In compressive sensing theory, a sparse signal can be acquired and compressed simultaneously in the same process with only the essential information at rates significantly lower than Nyquist rate. This means that the signal can be recovered from far fewer measurements and at a lower rate (below Nyquist rate) compared to that of traditional methods [31], [33]. As the wideband spectrum is inherently sparse due to its low spectrum utilization, compressive sensing becomes a promising approach to realize wideband spectrum sensing.

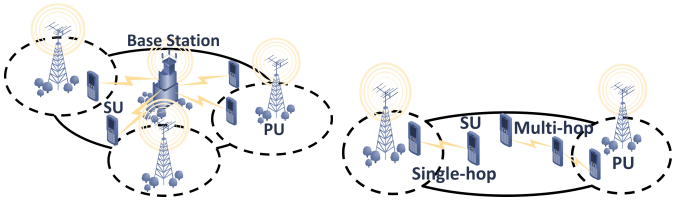
b) Cooperation

One widely adopted approach for improving spectrum sensing accuracy is cooperation, where SUs share their local sensing observations and collaboratively make spectrum availability decisions. These observations can be made using one of PU detection techniques discussed in Section II-A1a.

The idea behind cooperation is to exploit spatial diversity of spatially distributed SUs to cope with problems, like shadowing, multipath fading, and receiver uncertainty, that may impact individual local observations of SUs [22]. There have been many cooperative approaches proposed in the literature [25], [34]–[37], and cooperative spectrum sensing has been widely adopted in many cognitive radio standards, e.g. WhiteFi [38], IEEE 802.22 WRAN [39] and IEEE 802.11af [40]. The collaboration between SUs is usually performed through a control channel [29] and could be realized in two major ways: centralized and distributed [41].

In the centralized approach a central entity, referred to as *fusion center* (FC), orchestrates the cooperative sensing task among SUs through a control channel as shown in Figure 4(a). FC collects the local observations from SUs and combines them to determine PU's presence on a specific channel. In the distributed approach, SUs do not rely on FC for making channel availability decisions. They instead exchange sensing information among one another to come to a unified decision [41], [42] as shown in Figure 4(b)

Another promising approach for enabling effective cooperative spectrum sensing over a large geographic area is to exploit



(a) Centralized (b) Distributed

Figure 4: Cooperative spectrum sensing

the emerging *crowdsourcing* paradigm, in which spectrum service providers outsource spectrum sensing tasks to distributed mobile users [6], [43]–[46]. Crowdsourcing is formally defined as the act of taking a job traditionally performed by a designated agent and outsourcing it to an undefined, generally large group of people in the form of an open call. This concept has been adopted in many contexts [47], and has been first applied to CRNs by Fatemiah et al. [43].

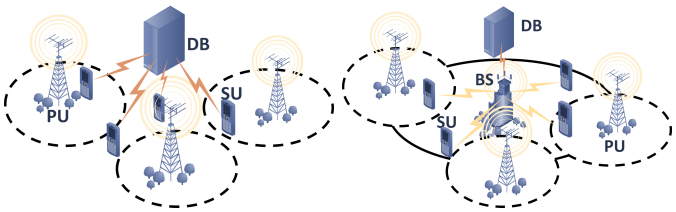
The use of crowdsourcing for enabling spectrum sensing is motivated by several facts and trends. First, according to a recent Cisco report [48], the number of mobile-connected devices is expected to hit 11.6 billion. This huge number guarantees sufficient geographic coverage, especially in highly populated regions such as metropolitan areas [44] where *dynamic spectrum access (DSA)* systems are expected to play important roles [46]. Moreover, future mobile devices are widely expected to be able to perform spectrum sensing tasks given the expected pervasiveness of DSA future wireless systems [44], [49]. Finally, mobile devices are increasingly equipped with more powerful communication and computation resources, and are enabled with self-localization capabilities, making mobile crowdsourcing even more appealing and attractive [46].

The cooperative spectrum sensing process is usually performed by a specified set of nodes that are considered to be trustworthy [43]. Crowdsourcing-based cooperative spectrum sensing, on the other hand, is to be realized by gathering and combining sensing reports from a large group of nodes that could be unreliable, untrustworthy, or even malicious [43], thereby giving rise to new challenges.

Another important challenge that arises from SUs' cooperation nature is how to combine the various SUs' sensing results or observations for hypothesis testing to decide on the presence of primary signals in an accurate manner. This process consists of sending the sensing results to FC or to the neighboring SUs, depending on the topology, to make spectrum availability decisions. It is referred to as data fusion and can be done in one of two ways: soft combining and hard combining [50]. In soft combining, local sensing reports, measured locally by SUs from their received signals, are combined together to compute some statistics using combining rules such as square law combining (SLC), maximal ratio combining (MRC) and selection combining (SC) [50]. In hard combining, SUs make decisions about the availability of the spectrum locally, and share their one-bit decision (i.e., available or not available) outputs to make a voting decision about spectrum availability [50].

2) Geolocation database

This is another approach for spectrum opportunity discovery that was recommended recently by FCC [51]. A typical database-driven CRN [52], [53] consists of a geolocation database (DB) containing spectrum availability information, a set of SUs and a set of PUs as shown in Figure 5(a). To learn about spectrum opportunities in its vicinity, a SU is not required to detect the primary signal by itself anymore. Instead, it needs to query DB by including its exact location in the query. DB then replies with a set of available channels in SU's location and with the appropriate transmission parameters (e.g. transmit power) for each channel to avoid interfering with the incumbents. Afterwards, depending on the situation, SU may optionally inform DB of its choice and registers the channel it is planning to operate on during what is referred to as notification or commitment phase [54], [55]. DB keeps track of this information to have more visibility over the CRN and make its decision adaptively which allows it to reduce interference among SUs. SUs may be able to communicate directly with DB as in Figure 5(a) or via a fixed base station that relays their queries to DB as in Figure 5(b).



(a) without BS (b) with BS

Figure 5: Spectrum database-based CRN topologies

3) Sources of location information leakage

In this Section, we investigate the different vulnerabilities in the spectrum opportunities discovery phase and the potential threats that could exploit them in order to localize SUs. We first begin by exploring the sources of leakage in the cooperative spectrum sensing approach, and then we explore those in the database-based approach.

a) Cooperative spectrum sensing

In the cooperative spectrum sensing approach, SUs need to communicate with other entities in the CRN to exchange and share their observations of the spectrum. This collaboration may lead to a significant leakage of information regarding the location of the collaborating SUs. In the following, we investigate and discuss the different vulnerabilities that arise from the cooperation process.

Wireless signal: This is the most obvious and direct source of leakage in wireless networks in general and in CRNs in particular. The wireless medium and its inherent open and broadcast nature in CRNs makes it much easier for an attacker to compromise a SU's privacy and more specifically its location [56], [57]. Despite the many efforts to protect the private location information at the system level, mainly using encrypted signal transmissions, the signal itself can still be used to potentially localize a SU. Classic approaches for localization are usually based on a small set of measurements on the wireless signals, that include time-based ranging, received signal strength (RSS) and angle of arrival (AoA) [56].

- Time-based ranging: This is used to estimate the distance between two communicating nodes by measuring the signal propagation delay, known also as time-of-flight, $\tau_F = d/c$, where d is the actual distance between the nodes and c is the propagation speed ($c \simeq 3.10^8 m/s$) [57]. This can be accomplished using either time-of-arrival (ToA) or time difference-of-arrival ($TDoA$). If at time t_1 the victim node sends a packet that contains the timestamp t_1 to a semi-honest or malicious node that receives it at time t_2, then the latter node can estimate the distance that separates it from the victim node based on $\tau_F = t_1 - t_2$. This technique is known as ToA ranging [56], [57]. ToA needs at least three measurements of distance to localize the target via triangulation [58], which means that a malicious entity cannot localize precisely a target SU unless it is mobile or it collaborates with two other malicious entities. $TDoA$, on the other hand, does not rely on the absolute distance between a pair of nodes but rather on the measurement of the difference in time between signals arriving at two base nodes.
- Received signal strength (RSS)-based ranging: In theory, the energy of a radio signal decreases with the square of the distance from the signal's source. As a result, a node listening to a radio transmission should be able to use the strength of the received signal to estimate its distance from the transmitter [59]. More details about the practicality of RSS-based ranging technique and its feasibility given various factors could be found in [60].
- Angle of arrival (AoA)-based ranging: AoA could be defined as the angle between the propagation direction of an incident wave and some reference direction known as orientation [61]. The estimation of AoA could be done using directive antennas or using an array of uniformly separated receivers [62]. The relative angle could then be used to derive the distance between the two communicating nodes [59].

Observations: The spectrum sensing measurements and observations that SUs share to identify spectrum holes may be another source of location information leakage in CRNs. In the case of soft combining rule where SUs have to share their raw measurements, SUs may see their location information exposed. Indeed, it has been shown in [6], [11] that the sensing reports containing RSS measurements on PUs' signal, are highly correlated to SUs' physical location. The RSS measurements could be used to localize SUs with respect to PUs whose channels are sensed through these measurements. Note that this RSS is different from the RSS that we discussed previously for wireless signal which are obtained through a direct communication through the wireless medium between the adversary and the target victim. If the CRN uses a hard combining rule for the cooperative sensing, SUs need just to share their binary decision values. This can still leak some information about SUs' location as it can tell whether a SU belongs to the coverage area of a PU especially if the activity of PU is known by the attacker.

Identity: One cannot talk about a location information leakage if the identity of the target victim is not revealed. Therefore, the identity of the user could also be considered as a source of location information leakage in the way that an attacker can match this identity to a specific location. In other words, if an attacker learns that a SU is located at a specific location but at the same time fails to identify who it is, the location privacy of SU cannot be considered as compromised. So, as long as a SU is anonymous, its location privacy is preserved. In some cases, identity could also give an idea about the location of a SU if combined with publicly known information of this specific SU. Take the example of a user whose identity is revealed. Based on this information, an adversary can learn the profession of this user, for instance a doctor that works at a specific hospital. This allows an attacker to estimate the position of the target SU with high probability especially during regular working hours. This shows that the identity could be associated with a specific location of a SU.

Radio hop count: The sensing information needs to be delivered to the appropriate nodes for the final decision, especially in multi-hop CRNs which requires deploying efficient routing protocols. These routing protocols usually rely on hop count information [63], [64], and such information turns out to be another potential source of location information leakage [59]. Many approaches are proposed in the literature, especially in the context of wireless sensor networks, to estimate node position based on the number of hops between pairs of nodes [65], [66].

Clustered network: SUs may need to form or join different clusters during the spectrum sensing phase in order to improve the overall sensing performance and overhead. Different approaches are proposed in the literature for cluster formation in CRNs based on several criteria and metrics including geographical location, channel availability, signal strength and channel quality [67]. This clustering could leak information about SUs' location especially if the clustering criteria is based on the positions of SUs or on some information correlated to this position. Chang et al. [68] show that the clustering information along with some knowledge of the position of some anchor nodes in wireless sensor networks can lead to localizing the remaining nodes in the network. The same idea could be exploited in the context of CRNs in case, for example, that some SUs are compromised and their location is known to the adversary. In that case, the adversary can localize the remaining SUs. Moreover, if the clusters are also overlapping, this could further facilitate localization as shown by Youssef et al. in [69].

Signal-to-noise ratio (SNR): SUs may need to share their measured SNRs, with respect to the channels of interest, with other SUs to cooperate in forming coalitions and selecting the decision making nodes in ad hoc CRNs [70]. The average SNR of PU's received signal measured at $SU\ i$ is given by:

$$\overline{SNR}_{i,PU} = \frac{P_{PU} \cdot \kappa}{d^{\alpha}_{PU,i} \cdot \sigma^2} \tag{1}$$

with P_{PU} is the transmission power of PU, σ^2 denotes the Gaussian noise variance, κ is a path loss constant, α is the path loss exponent and $d_{PU,i}$ is the distance between PU and $SU\ i$ [71]. As Equation (1) shows, the SNR value measured by a SU depends on the distance that separates it from the corresponding PU. This could present a source of location information leakage as this information could be exploited to localize SU especially when it has to share its SNR with other SUs in the same coalition [72].

The vulnerabilities and sources of leakage that we have raised previously could lead to serious location privacy risks for SUs if exploited by malicious entities in the CRN. This leakage could happen in the following scenarios:

- **Cooperation and sharing observations:** In order to participate in the cooperation for spectrum sensing, SUs need to share their observations of the spectrum either with other SUs or with a central entity. Despite the fact that sharing this information considerably improves the spectrum sensing performance, it exposes, however, individual SUs observations to other entities in the network. This becomes problematic if, during the sharing process, an external or internal malicious entity to the network gains access to these observations. This is due to the fact that these observations could be exploited to compromise SUs' location privacy as discussed earlier.
- **Dynamism:** Due to the dynamic nature of CRNs, SUs can leave or join the collaborative spectrum sensing task at anytime, making privacy-preserving aggregation techniques designed for static networks to hide individual observations of SUs unsuitable for CRNs. Indeed, this might allow a malicious entity that is collecting aggregated observations from SUs to estimate individual observations of leaving or joining SUs which, as discussed previously, is a source of location information leakage.
- **Node failure:** The location privacy issue here is very similar to the situation of network dynamism. Indeed, if, for some reason, some SUs cannot sense the spectrum or fail to share their sensing reports during the cooperation process, the individual observations of these SUs could be estimated. Again, these individual observations could be exploited by an adversary for localization purposes.
- **User selection:** User selection is an important step in cooperative spectrum sensing, which aims to optimally select the cooperating SUs that lead to the maximization of the cooperative gain and the minimization of the cooperation overhead. SUs are selected such that all the sensing reports are informative and not correlated while saving energy by avoiding unnecessary sensing operations [41]. This selection could be done through a clustering approach that divides SUs into different clusters. Malady et al. [73] propose several approaches for grouping SUs into clusters in distributed CRNs to keep bandwidth and power requirements manageable. Their methods are based on different criteria including SUs' positions with respect to a given reference or to PU if PU's position is known. In [74], Ding et al. propose a decentralized clustering-based user selection algorithm that relies on unsupervised learning to group SUs with best detection performance together to lead the sensing process. As discussed previously, the clustering

information could be exploited to localize SUs during the cooperative spectrum sensing process. Another way for selecting SUs for spectrum sensing, which has just started to gain some interest in the context of CRNs, is *crowdsourcing* as we have explained earlier. Crowdsourcing may, however, give rise to some privacy risks, especially in terms of location privacy as shown by Jin et al. [46]. The selection process in this case relies on an open call, made by FC, for users in order to contribute to the sensing at a specific location. This makes it easy for FC to associate users with the location of interest.

b) Geolocation database

With this architecture, SUs are not anymore required to perform spectrum sensing to learn about spectrum opportunities. Instead, they only need to query a geolocation spectrum database to get the list of available channels in their vicinity. This brings new privacy challenges that are completely different from the ones that emerge from the cooperation in spectrum sensing. In the following, we investigate the different sources of location information leakage that may arise from this specific CRN architecture.

Query: This is the most implicit source of location information, as every SU needs to include its precise location every time it queries DB for available channels. This information is usually sent in a plaintext form, allowing eavesdroppers to retrieve it. And even if the communication channel between SUs and DB is authenticated; i.e. it eliminates the risk of an eavesdropper, there is still the risk of having a malicious DB.

List of available channels in the query's response: This information could also be used by an adversary to narrow down the locations where a target SU might possibly be. Indeed, knowing which channels are available for a certain SU allows a malicious entity to attribute this SU to multiple PUs coverage areas especially if the adversary, DB for example, is aware of these PUs' activities and status.

Maximum transmit power (MTP): The MTP over a specific spectrum band is included in DB's response to SU, and is assigned to it based on its distance from its corresponding PU. It is usually calculated as follows

$$P = \begin{cases} 0, & d \leq r_0 \\ h(d - r_0), & d > r_0 \end{cases} \tag{2}$$

where d is the distance between the querying SU and its closest PU, r_0 is the protected contour radius of the channel of interest and $h(.)$ is a continuous, monotonically increasing function. As shown in Equation (2), MTP is highly correlated to the distance of SU from PU. In situations where PUs' positions are publicly known, an attacker could exploit MTP values that SUs receive from DB to infer SUs' locations.

These vulnerabilities and sources of leakage could become actual threats when exploited solely or combined together, and can occur in the following scenarios:

- **Querying DB:** When a SU interacts with DB to learn about spectrum availability, its location can easily be revealed as it is included in the query. Even if, somehow, a privacy-preserving scheme is implemented to make DB unable to retrieve SU's location information from its query but at the same time can still provide it with the spectrum availability information at its vicinity, an adversary can still localize SU by exploiting the information included in DB's response as we discuss next.
- **DB's response:** DB's response to a SU's query includes information like the list of available channels, and the maximum transmit power over each of those channels. This information could be used as explained earlier by a malicious DB or an external adversary to infer the location of a target SU.
- **Commitment phase:** Some implementations of the database-based CRNs require that a SU, upon receiving the response from DB, informs DB about the channel that it chooses to operate on. This will make SU's usage information available at least to DB. Hence, SUs in database-based CRNs will be prone to attacks that could exploit the vulnerabilities arising from spectrum utilization information as we explain in Section II-D2.

B. Location information leakage in spectrum analysis

This is an important step in the cognition cycle as it allows to analyze the information obtained from spectrum sensing to gain knowledge about spectrum holes (e.g. interference estimation, and duration of availability). Spectrum analysis usually consists of two major components: spectrum characterization, and reconfiguration. In this section, we explain each of these two components and discuss their sources of location information leakage.

1) Spectrum characterization

Available spectrum bands may have different channel characteristics that vary over time. In order to determine the most suitable spectrum band, one needs to characterize these channels. Such a characterization requires the monitoring and observation of the RF environment, as well as the monitoring and awareness of PUs activities in these channels [75].

a) RF environment characterization

This process estimates some of the following key parameters to characterize the different spectrum bands.

- *Interference:* It is crucial to estimate and model the interference caused by SUs at the primary receiver to derive the permissible power of a SU and ensure coexistence between SUs and PUs. Rabbachin et al. [76] propose a statistical model for aggregate interference generated by SUs in a limited or finite region by taking into consideration the shape of the region and the position of PU. The interference signal at PU generated by the i^{th} SU is modeled as [76]:

$$I_i = \sqrt{P_I} R_i^{-b} X_i \tag{3}$$

  where P_I is the interference power at the near-far region limit; R_i is the distance between the i^{th} SU and PU; and X_i is the per-dimension fading channel path gain of the channel from the i^{th} SU to PU.
- *Path loss:* This is closely related to distance and frequency. Path loss increases as the operating frequency increases, resulting in a decrease in the transmission range. Increasing the transmission power may be used

to compensate for the increased path loss, and hence for the decrease in transmission range. But this may increase interference at other SUs and PUs. According to [77], the average path loss of a channel could be expressed using a path loss exponent α. This exponent measures the rate at which the RSS decreases with distance, and its value depends on the specific propagation environment [78]. It is also considered as a key parameter in the distance estimation based localization algorithms, where distance is estimated from the RSS [79].

- *Channel switching delay:* This is basically the delay introduced by switching from one channel to another. In CRNs, the channel switching could be triggered by several events, such as the detection of PUs, the return of PUs to their channels, and/or the degradation of received QoS in the current channel, as we discuss in Section II-D.
- *Channel holding time:* It is the expected duration SUs can occupy a licensed channel before getting interrupted.
- *Channel error rate:* This is defined as the rate of data elements incorrectly received from the total number of data elements sent during a time interval. This rate may vary depending on the modulation scheme and the interference level of the channel [75].

b) PU activity modeling

As spectrum availability depends not only on the RF environment characteristics but also on the activities of PUs, it is crucial that PU activities are taken into account when characterizing the spectrum bands. This is essentially done by accounting for how long and how often PUs appear on their licensed spectrum bands. Existing approaches adopted for modeling this activity mainly rely on measured data obtained from the numerous spectrum measurement campaigns that have been conducted worldwide to quantify and study the PU spectrum utilization and assess the current status of the spectrum [80]–[82]. These measurements are also performed to improve the accuracy of spectrum databases. Many of these works consider only simple but important statistics of the spectrum occupancy, such as the maximum or the minimum and the average of power levels, the spectrum occupancy, and the duty cycle [80]. These statistics are simple and reliable, but provide an incomplete model of the PUs' activities. Other approaches consider more advanced statistical models, such as probability function models (e.g. CDF and PDF), Markov chains and linear regressions. These measurement-based modeling methods describe the statistical behaviors of the spectrum occupancy as a whole, but do not give the actual state of the spectrum occupancy, i.e. whether a channel is busy or available.

Some other significant research models the PU activity as a Poisson process with exponentially distributed inter-arrivals [81], [83]. However, such approaches fail to capture the short-term temporal fluctuations or variations exhibited by the PU activity, and do not consider correlations and similarities within the monitored data [81].

There are also approaches that try to predict future PU activities and thus locate future spectrum opportunities by using learning techniques and by exploiting the history of spectrum band usage [75], [81]. However, the prediction may go wrong resulting in harmful interference to PUs.

c) Sources of location information leakage

As mentioned earlier, spectrum characterization consists of building knowledge about the radio environment and PU activities. This knowledge, however, could be exploited (maliciously or un-maliciously) to leak location information of SUs, as discussed next.

Interference: As shown in Equation (3), the interference is highly correlated to the distance that separates SU from a PU. An adversary that has access to the characteristics of the interference caused by SUs can exploit this information to estimate the distance that separates SU from a PU.

Radio environment map (REM): This is a widely used method to characterize the spectrum. It is an integrated database that could be deployed in CRNs to store information about the radio environment's interference, signal properties, geographical features, spectral regulations, locations and activities of radios, policies of SUs and/or service providers, and past experiences [84], [85]. The main functionality of a REM is the construction of dynamic interference map for each frequency at each location of interest. This could be done in two different ways, either via field measurements or via propagation modeling. In the first approach, a REM collects spectrum measurements from nodes with spectrum sensing capabilities. These nodes could be actual SUs or dedicated spectrum sensors [86]. Since it is impractical to have measurements all the time at all possible locations, REM fuses the collected measurements to estimate the interference level at locations with no measurement data by means of spatial and temporal interpolation [86]. The field measurement approach is believed to provide the highest location accuracy but not without a price. Its price lies in the need to perform drive tests whenever changes occur in the radio environment to keep the REM up to date. The second approach, propagation modeling, relies on mathematical models for radio propagation prediction, which allow easy, fast and inexpensive updating for the REM. Indeed, whenever there is a change in the radio environment, we only need to rerun the propagation models with the new parameters to update the REM [56].

This is different from the spectrum geolocation database in that REM generates spectrum map by processing the data collected from multiple sources with its cognitive engine, and therefore can easily adapt to dynamic operating environments whereas DB stores quasi-static information. REM introduces environment awareness that would be harder to acquire by individual CR capabilities via extensive spectrum analysis. Hence, REM can also be seen as the network support turning simple nodes into intelligent ones [86].

This radio map, when it is in the hands of some malicious entity in the network, could be exploited to localize a querying SU that sends its measurement to the REM manager in order to learn about spectrum availability. One way to exploit this information is based on fingerprinting localization technique which basically estimates the target position by simply finding the best-matched pattern or fingerprint for the measurement provided by SU within a certain map [56]. Machine learning techniques could be used to build the radio

signal map during the training phase and then to compare the online measured RSS to the preconstructed map during the localization phase [56]. Obviously the map that could be used for the localization is the REM itself. As the REM could be used in a distributed or a centralized manner, either a malicious BS or a malicious SU could exploit it to localize a target SU.

2) Reconfiguration

After the channel of choice has been characterized, SU's transceiver parameters have to be reconfigured to adapt to channel conditions and satisfy the QoS requirements and regulatory policies. These parameters include:

- Transmission power: Controlling this parameter aims to achieve several objectives that include minimizing energy usage, reducing co-channel interference, etc. [87], [88].
- Operating frequency: This parameter represents the capability of SUs to reconfigure their central frequency in response to variations in the RF environment.
- Channel bandwidth: This refers to the width of the spectrum over which a SU operates. It is essential for SUs to have variable channel adaptation capabilities to be able to operate in heterogeneous networks.
- Communication technology: This allows interoperability between different communication technologies such as GSM, LTE, etc.

Sources of location information leakage: Some of the reconfigurable parameters that we have listed could leak some information about SUs' location especially if these parameters are controlled in a shared way.

- *Power control*: This process may present a threat to SUs' location privacy. Most of the existing approaches for power control rely on the *signal-to-noise ratio* (SNR) or the *signal-to-interference-plus-noise ratio* ($SINR$) metric when solving the power control problem [88]–[91]. For example, Hoven et al. [88] use local SNRs of primary signals measured by SUs as a metric to design an effective power control rule. Other works use $SINR$ as a constraint or a requirement to minimize the total transmission power of the CRN as in [89] and maximize the spectrum utilization of the CRN as in [92]. Yang et al. [93] model this problem as a game with $SINR$-based utility function. Power control might become threatening to the privacy of SUs as information like SNR and $SINR$ is usually correlated to the distance that separates a SU from a PU. This is problematic especially when the power control process is intended to achieve a system-level goal like minimizing the total transmission power [89] or maximizing the overall spectrum utilization [92] of CRNs. In that case, power control will have to be performed jointly between SUs in a centralized [89], [94] or distributed [89], [92]–[94] way, thereby exposing local SNR and $SINR$ values, for example, to other CRN entities or intruders, putting SUs' location information at risk.

C. Location information leakage in spectrum sharing

Multiple SUs may try to access the same spectrum bands at the same time, thus necessitating multiple-access coordination mechanisms that allow multiple SUs to share the same spectrum [95]. Spectrum sharing consists then of enabling coexistence of multiple SUs while avoiding interference (among SUs themselves as well as between SUs and PUs) and maintaining some target QoS levels. Broadly speaking, this functionality is composed of three elements: resource allocation, spectrum access and spectrum trading.

1) Resource allocation

Enabling dynamic spectrum sharing is crucial to the success of CRNs. It allows users to select, use, and share spectrum bands adaptively with the aim of maximizing the overall spectrum utilization efficiency while not causing harmful interference to legacy users [87], [96]–[99]. In this section, we discuss two resource allocation functions: *spectrum selection and assignment* and *power control and beamforming*.

a) Spectrum selection and assignment

Once the spectrum holes are analyzed and characterized, the most suitable channel is selected based on QoS requirements of SUs, as well the characteristics of the channels [87], [98], [100]. Several criteria may be taken into account while assigning spectrum bands to SUs. These include minimizing interference to PUs, maximizing overall spectrum efficiency, maximizing SUs' throughput, minimizing network delay, and increasing network connectivity, just to name a few [87], [101]. Spectrum assignment could be done in a centralized or a distributed way, and there have been many proposed approaches, both centralized and distributed, that address the spectrum assignment and selection problem in CRNs [87], [96], [102]–[107]. Generally speaking, these approaches are mainly based on one of the four mature concepts: graph theory, game theory, learning and adaptation, and optimization theory. Next, we explore these four concepts and investigate the sources of location information leakage that may arise from using them.

i) Graph theory: Graph theory has been extensively used to address the spectrum assignment problem especially when the structure of the CRN is assumed to be known a priori [87]. Here the network is modeled as a graph, where the vertices usually represent SUs and the edges model the connection between these SUs. To solve the graph-based spectrum assignment problem, network conflict graphs and graph coloring are widely used [87].

- Network conflict graph: This models and captures the interference among SUs caused by concurrent transmissions of nearby SUs communicating on the same or neighboring channels [87]. The vertices of the graph represent the communication links among SUs, whereas the edges represent the pairs of links whose concurrent communications interfere with one another when assigned the same or adjacent spectrum bands [87], [98], [108]. Conflict graphs are mostly used in centralized topologies, where a central entity (BS or FC) constructs the graph and uses it to assign channels among SUs.
- Graph coloring: In this approach, the CRN is mapped to a graph that could be either unidirectional or bidirectional depending on the algorithm's characteristics. The vertices in this graph represent SUs that need to share the spectrum, and the edges model the interference between

SUs. PUs could also be included in the graph with pre-assigned colors. The spectrum assignment problem using graph coloring is equivalent to coloring each vertex (or edge) using different colors from a specific set of colors, each often representing an available spectrum band [87], [98], [109]. The goal is to improve spectrum efficiency by increasing frequency reuse while meeting interference constraints by ensuring that two connected vertices (SUs) cannot be assigned the same color, i.e. the same band.

Sources of location information leakage: We identify two main sources of leakage that arise from graph-based approaches during the spectrum selection process: the topology and the connectivity information.

- *Topology:* The topology of the network that could be learned via the graph-based spectrum assignment techniques could be explored to infer SUs' location. In fact, some works have already used this information to localize nodes in wireless sensor networks [110], [111].
- *Connectivity:* This information basically tells which nodes are located within each other's transmission range (i.e., connected to one another). Many approaches have used this information for positioning purposes [112]–[115] and some of them can be used to localize target nodes even from connectivity information among the nodes themselves only [112], [113].

ii) Game theory: Game theory has also been extensively used to solve the spectrum assignment problem in CRNs [96], [104], [116]. A game could be seen as a way of interaction between multiple players competing with each other while trying to adjust their strategies to optimize their utilities [21]. Game theory is suitable for the spectrum assignment problem in CRNs as the spectrum allocation decision of one SU has a direct impact on the performance of other neighboring SUs [87].

Spectrum selection games in CRNs usually consist of three components: The players which represent SUs and may include PUs, the action space and the utility function(s). The players have a set of functions representing available frequency bands. The action space is the Cartesian product of the sets of actions of all players. Each player has a utility function that is used to translate the action space into the real world needs, e.g. the frequency bands that meet SU's requirements [87]. The goal of the game is to maximize each SU's utility function. This takes into consideration the impact of each SU's decisions on the other players. For games with specific characteristics, there is always a steady state solution (i.e., a Nash equilibrium), and any unilateral change of a player leads to a lower utility for that specific player [87], [116].

Sources of location information leakage: Games may require that SUs share their channel selection decisions among one another. This information, just like the case of spectrum availability, could be used for SU localization. In fact, this information reveals the list of channels that a SU may be interested in using; i.e. the list of available channels in its vicinity. Sharing this list with other SUs may put into risk SU's own privacy, as this information could be used by an adversary to estimate its position especially if this adversary has a global knowledge of the CRN.

iii) Learning and adaptation: CRNs employ software-defined radios, which are capable of executing complex computational tasks through a specialized software module called the cognitive engine [105], [117]. This engine has learning capabilities that allow SUs to make spectrum selection decisions and perform tasks in a distributed manner by only relying on what SUs learn from the environment [105], [118]. This is usually done by means of machine learning techniques, which have recently attracted significant attention in the context of CRNs [119]–[121]. For example, in [122], the authors propose a cognitive engine based on artificial neural network (ANN) that learns how environmental measurements and the status of the network affect the CRN performance on different channels. Based on this, the cognitive engine can dynamically select the best channel, expected to yield the best performance for SUs. Li et al. [123] use a multi-agent Q-learning approach, a model-free type of reinforcement learning, to address the problem of channel selection in multi-user and multi-channel CRNs. Each SU considers both the channel and the other SUs as its environment, updates its Q values continuously, and uses the Q-table to select the best channel. NoroozOliaee et al. [119], [124] derive new private objective functions suitable for supporting elastic traffic that can be used by learning algorithms to enable cognitive users to locate and exploit unused spectrum opportunities in a distributed manner while maximizing their received throughput. These same authors also derive learning-based objective functions for the inelastic traffic model with non-cooperative [125], [126] and cooperative [127], [128] users. Yau et al. [129] propose a context-aware and intelligent dynamic channel selection scheme that enables SUs to adaptively select channels for data transmission to enhance QoS.

Sources of location information leakage: The learning process may also lead to some location information leakage. This is mainly due to:

- *Environmental measurements:* In centralized CRNs, the learning agent, usually FC, needs to collect environmental measurements during the training phase [122] to be able to select the best channels for secondary transmissions. In the case of distributed CRNs, the learning process involves multiple agents, which often need to exchange measurement information among themselves. As we have shown previously, this information, when shared among the different CRN entities, may reveal significant information about SUs' location.
- *Activity prediction:* Prediction strategies through machine learning techniques could also be used to predict both PU and SU activities based on past measurements and experience [130], [131]. This can allow a malicious entity to predict which channels a SU might be using in the future. Combining this information with the learned activity model of PUs and their coverage areas, it becomes possible to predict a SU's location, just as explained in Section II-D2.

iv) Optimization theory: Optimization techniques (e.g., convex optimization, linear programming, non-linear programming, etc.) have also been widely used to solve the spec-

trum assignment problem in CRNs. For instance, Tan et al. [107] formulate the channel assignment problem as an integer optimization with the aim to maximize throughput, and propose two greedy non-overlapping and overlapping channel assignment algorithms to solve it. Bkassini et al. [132] model the channel assignment problem as a weighted bipartite graph, where PUs and SUs constitute the two disjoint sets of vertices in the bipartite graph. The authors use the well-known Hungarian method [133] to solve this problem in polynomial time. Ding et al. [134] formulate the joint spectrum and power allocation problem as a convex optimization problem, and propose a distributed algorithm to solve it. Ben Ghorbel et al. [135], [136] propose two-phase optimization heuristics also for joint allocation of the spectrum and power resources. Their proposed heuristics split the spectrum and power allocation problem into two sub-problems, and solve each of them separately. The spectrum allocation problem is solved during the first phase using learning, whereas the power allocation is formulated as a real optimization problem and solved, during the second phase, by traditional optimization solvers. Salameh et al. [137] formulate the joint rate/power control and channel assignment as a mixed-integer program with the aim to maximize the sum-rate achieved by all contending SUs over all available spectrum opportunities. Due to the NP-hardness nature of this problem, they transform it into a binary linear programming problem which they solve in polynomial time. In [138], the authors formulate the joint QoS-aware admission control, channel assignment, and power allocation as a non-linear NP-hard optimization problem. In [139] the channel assignment problem is expressed as an Integer Linear Programming (ILP) problem. These approaches rely on heuristics to solve the spectrum assignment due to the complexity of the formulated optimization problems.

b) Power control and beamforming

Power control and beamforming are effective methods for mitigating co-channel interference and thus boosting the system capacity. The challenge with power control and beamforming in CRNs lies in making sure that SUs' transmissions do not cause the received interference at PUs to exceed a tolerable limit. In light of this, a number of beamforming and power allocation techniques have been proposed for CRNs with various objectives, such as capacity maximization [140] and transmit power minimization.

For instance, Le et al. [141] propose to formulate the joint rate and power allocation problems for the secondary links as optimization problems with both QoS and interference constraints under low network load conditions. This work relies on two popular fairness criteria, namely, the max-min and the proportional fairness criteria. Kim et al. [142] develop joint admission control and rate/power allocation methods subject to QoS and minimum rate requirements as well as maximum transmit power and fairness constraints for SUs in MIMO ad hoc CRNs.

Zhang et al. [140] consider beamforming and power allocation jointly for SIMO-MAC, and formulate it as two optimization problems: sum-rate maximization and $SINR$ balancing. These problems are solved using a water-filling based algorithm and constraint decoupling techniques. The goal is to obtain the suboptimal power allocation strategy and to maximize the minimal ratio of the achievable $SINR$s relative to the target $SINR$s of the users in the system under a sum-power constraint. Zheng et al. [143] propose beamforming designs for a multi-antenna CRN, with the aim of allowing multiple SU transmissions concurrently with the PU presence, to achieve also $SINR$ balancing subject to the constraints of the total SUs transmit power and the received interference power at the PUs. This is achieved by optimizing the beamforming vectors at the SU transmitter based on imperfect channel state information (CSI).

2) Spectrum access

Spectrum access of CRNs is responsible for the sharing of the spectrum among SUs by handling medium contention, interference avoidance, multi-user coexistence, etc. [144].

a) Access paradigms

There are three spectrum access paradigms in CRNs:

Spectrum underlay: This paradigm mandates that SUs can transmit concurrently with PUs only if doing so generates an amount of interference at the primary receivers that is below some acceptable threshold [142], [145].

Spectrum overlay: Spectrum overlay paradigm also allows concurrent primary and secondary transmissions. But SUs are assumed to have knowledge about certain primary transmission parameters to avoid interference with the primary transmissions. The enabling premise for overlay systems is that SUs are allowed to use the spectrum for their own transmissions as long as they are willing to use some of their power to relay some of PUs' transmissions [146].

Spectrum interweave: This paradigm is based on the opportunistic spectrum access idea, which has been one of the main drivers for cognitive radio access. Different from the two previous paradigms, this paradigm does not allow simultaneous secondary and primary transmissions on the same frequency band. Instead, it allows SUs to access and use the licensed spectrum only when the spectrum is vacant [145].

b) Spectrum access techniques

Many MAC protocols have been proposed to coordinate SUs to access and share the available channels and to avoid (or reduce) collisions among users [140]. Such a coordinated access could be performed in a distributed or a centralized way [144]. These protocols can either be cooperative [147], [148] in that they require coordination among SUs to enable efficient sharing of spectrum and thus improve spectrum utilization, or contention-based [149], [150] in that no coordination is required among users. In contention-based protocols, cognitive senders and receivers exchange their sensing results through handshaking mechanisms to negotiate which channel they will use for their communications [144]. Tan et al. [107] propose an overlapping channel assignment algorithm and design a MAC protocol to resolve the access contention problem when multiple SUs attempt to exploit the same available channel. Salameh et al [151] propose a contention-based protocol that tries to satisfy QoS constraints by limiting the number of used channels per SU.

In coordination-based protocols, each SU shares its channel usage information with its neighbors to increase sensing

reliability, and to improve overall system performance [144]. For instance, Hamdaoui et al. [148] propose a coordination-based MAC protocol that adaptively and dynamically seeks and exploits opportunities in both licensed and unlicensed spectra and along both the time and the frequency domains. Zhao et al. [152] propose a heterogeneous distributed MAC protocol that permits distributed coordination of local clusters in a multi-hop CRN through a local common channel.

c) Sources of location information leakage

The sharing of information during this coordination process, though needed for enabling efficient multiple access, could expose the location information of SUs to one another.

Sensing outcomes: Contention-based MAC protocols may require SUs to share their sensing outcomes with one another to negotiate their access to the spectrum. However, as we have shown in Section II-A3a, these sensing outcomes can potentially leak SUs' location information.

Channel usage information: Channel usage information, when shared among SUs as in coordination-based MAC protocols, is shown to leak details about their location; this will be discussed later in Section II-D2.

3) Spectrum trading

Spectrum trading could be seen as the economic aspect of spectrum sharing [153]. It aims to maximize the revenue of the spectrum owners, i.e. PUs, while maximizing the satisfaction of SUs [154] that compete for gaining access to the spectrum. Spectrum trading can be done between PUs and SUs or among SUs only [153]. It relies mainly on two concepts: Auction theory and market theory. Next, we highlight these two concepts and investigate their sources of leakage.

a) Auction

A typical dynamic spectrum auction has three main phases: 1) *Spectrum discovery phase:* SUs obtain spectrum availability information through one of the spectrum opportunity discovery approaches, explained in Section II-A, and determine the bid price for each available channel based on its quality. 2) *Bidding phase:* each SU submits its bids and its location along with its ID to the auctioneer. 3) Channel assignment: once the auctioneer collects all the bids from SUs, it distributes channels among them and charges the winners accordingly [155]. This is suitable for situations when the price of the spectrum is undetermined and depends on SU's requirements [154]. Auction-based spectrum sharing for CRNs has been studied intensively in literature (e.g., [156]–[158]).

b) Market theory

Monopoly Market: This is the simplest market structure as there is only one seller, i.e. PU, in the system. Based on SUs' demand, the seller can optimize the trading process to obtain the highest profit [153], [159], [160].

Oligopoly Market: This is a type of market that lies between full competition and no competition (or monopoly) and is defined as a market with only a small number of firms and with substantial barriers to entry in economics [21]. These firms or primary service providers compete with each other independently to achieve the highest profit by controlling the quantity or the price of the supplied commodity which is the spectrum resource in this case. Unlike the monopoly case, in oligopoly, there are multiple firms that provide the same service, making it necessary for firms to consider each other's strategy [153]. The most basic form of oligopoly is duopoly, where only two sellers exist in the market [159], [160].

Market-equilibrium: In this spectrum trading model, the primary service provider or spectrum seller is assumed to be not aware of other service providers, which could be due to the lack of any centralized controller or information exchange among each other. This makes the spectrum seller naively set the price according to the spectrum demand of SUs. This price reflects the willingness of the spectrum seller to sell its spectrum which is generally determined by the supply function. On the other hand, the willingness of a SU to buy spectrum is determined by the demand function [116]. Market-equilibrium aims at giving a price for which spectrum supply from a primary service provider is equal to spectrum demand from SUs [21]. This price achieves two goals: the spectrum supply of the primary service provider meets all spectrum demand of SUs, and the spectrum market does not have an excess in the supply [116].

c) Sources of location information leakage

Spectrum trading may also introduce some sources of location information leakage as we discuss next.

Location information: During the bidding phase of spectrum auction, SUs may need to submit their locations to the auctioneer as suggested in [155]. This is clearly an obvious source of location information leakage as it exposes the location information of SUs to the auctioneer and to an external adversary that may be eavesdropping the communications of SUs during the auction process.

Bid channels: SUs here need to submit their bids for their channels of interest to the auctioneer (or spectrum broker) . An adversary aiming to infer a SU's location can deduce, from the list of channels SU bids for, that SU is located somewhere where these channels are available. Simple intersection of the availability areas of these channels can easily locate SU [155].

Bid prices: For each channel available for auction, a SU can first evaluate its quality and, depending on the channel's quality, establish a price for it. It then submits its bid for the channel to the broker. These prices are shown to be a potential source of SUs' location information leakage [155].

D. Location information leakage in spectrum mobility

SUs communicating on a licensed spectrum band may need to vacate their current band at any time, for instance, due to the return of PUs to their licensed band. When this happens, SUs need to find and switch their ongoing communications to another vacant band to avoid the disruption of their ongoing transmissions. This is known as *spectrum mobility* or *spectrum handoff* [161]. There are several events that could trigger spectrum handoff in CRNs, and next, we list some of them:

- *PU's return:* Whenever a PU returns to its channel, SU is forced to vacate it and switch to another available one, if any. This initiates the handoff process. Finding a new available channel often requires SU to perform spectrum sensing, making handoff more challenging [162].

- *SU's mobility:* Because spectrum availability is location dependent, moving while having an ongoing communication may trigger spectrum handoff, as current channel may no longer be available in SU's new location [163].
- *Quality degradation:* Spectrum handoff could be triggered by the degradation of the channel quality. It can be triggered when, for example, the QoS level received by SU goes below a certain threshold, forcing it to find and switch to another channel.

1) Spectrum handoff strategies

Based on the handoff triggering timing, spectrum handoff techniques could be classified into four categories or strategies: Non-handoff strategy, reactive handoff strategy, proactive handoff strategy, and hybrid handoff strategy [164], [165]. We first explore these different strategies, then we investigate their sources of location information leakage.

a) Non-handoff strategy

In this strategy, when one of the triggering events for handoff occurs, SUs stop transmitting over the current channel and choose not to switch to another channel. Instead they remain idle until the channel becomes available again [166], as introduced in the non-hopping mode of the IEEE 802.22 WRAN standard [167]. How good this handoff strategy is depends on the activities and loads of PUs. It causes very little to no PU interference but the waiting latency to resume secondary transmission could be unpredictably very large, as it depends on when PU leaves the spectrum. This strategy is best suited for systems with short PU transmissions [164].

b) Pure reactive handoff strategy

In this strategy, the target channel selection and the handoff are performed reactively after a spectrum handoff triggering event occurs [165], [168]. Here, SUs need to perform spectrum sensing in order to find the target backup channel to which communication is to be transferred. Several reactive handoff strategy-based approaches are proposed in the literature [169], [170]. In general, this strategy has less handoff latency than that of the non-handoff strategy, but has larger latency when compared to the proactive spectrum handoff strategy [164], [165] (described next). The handoff performance of this strategy depends on the accuracy and speed of the spectrum sensing process in identifying a vacant target channel.

c) Pure proactive handoff strategy

In this approach, the handoff and the target channel selection are performed proactively before a spectrum handoff triggering event takes place [171], [172]. SUs do so by periodically observing all channels to obtain spectrum usage statistics which allow them to determine the candidate channels for spectrum handoff [168]. The selection of the target free channel for future spectrum handoff is usually made based on PU traffic characteristics [165], where SUs can predict PU arrivals in the target spectrum band in advance. Hence, the handoff latency is reduced considerably when compared to the reactive spectrum handoff strategy, which requires taking action after the handoff triggering event takes place. However, if the prediction of PU traffic is inaccurate or if the target backup channel is obsolete, for instance due to being occupied by other SUs at handoff time, this could lead to poor handoff performance [164]. This makes this strategy best suited to networks with well-modeled PU traffic characteristics.

d) Hybrid handoff strategy

This approach combines proactive spectrum sensing with reactive spectrum handoff as suggested by Christian et al. [164]. It performs proactive spectrum sensing to decide on the backup target channel in advance and before the handoff is triggered, and makes a reactive handoff decision after the triggering event takes place. Thus, it reduces the handoff latency when compared to the reactive handoff strategy. This hybrid approach could be seen as a tradeoff between reactive and proactive handoff strategies.

2) Sources of location information leakage

Spectrum mobility can also leak some location information about SUs, as highlighted next:

Handoff: Recall that a SU utilizing a PU channel is forced to vacate the channel (and possibly switch to another) when PU returns to and claims its channel. PU (and easily other entities) knows, in this situation, that SU is located within its coverage area. Handoff can thus lead to leakage of location information of SU performing handoff.

Spectrum utilization information: A SU's spectrum usage history (e.g., sequence of channels SU has used over some period of time) could easily be used to localize SU (or to track it if it is moving). Recall that when a SU is communicating over a PU channel, it means that SU is outside the coverage areas of all ON PUs associated with that channel, or inside the area of an OFF PU. Now, for instance, by tracking which channels SU has used over a period of time and by knowing when and which PUs are OFF/ON during that time period, an adversary can easily narrow down the area where SU is located at by intersecting the areas associated with PUs [54]. Spectrum utilization history information could then be a significant source of location information leakage.

Sensing reports: Before handoff, a SU may need to sense the spectrum to identify a new target channel (using one of PU detection techniques identified in Section II-A1a). If cooperation is further required to select the appropriate channel for handoff, SUs will have to share their sensing reports, which can compromise their location privacy.

Location privacy-preserving protocols should therefore be designed with the objective of hiding information that can leak SU's location during the handoff process and also reducing, as much as possible, the occurrences of handoff events.

E. Summary

In this section, we identified the sources of location privacy leakage emerging from the different components of CRNs, namely, spectrum discovery, spectrum analysis, spectrum sharing, and spectrum mobility. We highlighted the different functionalities of each of these components, and discussed how some of these functionalities can present some vulnerabilities that could be exploited to localize SUs. In the next section, we will go over a family of renowned privacy enhancing technologies and generic crypto schemes that we believe are the most relevant to CRNs. We will also discuss to which extent

these technologies could be applied to design location privacy-preserving protocols that could prevent attacks exploiting the identified vulnerabilities.

III. Limitations of generic privacy enhancing technologies in CRNs

Location privacy preservation is a mature technology for many wireless systems, such as sensor [7], vehicular [173], [174], WiFi [9], cellular [10], and others [175]. Depending on the wireless system and application at hand, location information can be leaked through various means, ranging from wireless signal localization [7], [9] to traffic monitoring and analysis [8]. For instance, in sensor networks, location information can be inferred by monitoring packet reception times [8] or analyzing packet traffic [176], [177] of source nodes. Countermeasure solutions for these attacks have also been proposed, ranging from introducing randomness to multi-hop path selection [178], [179] to making the source nodes move randomly [8] to confuse the attackers. Unlike other wireless systems, location privacy preservation that addresses vulnerabilities in CRNs has not, however, received much attention, though several works related to spectrum sensing [11], [54], [55], [72], [180]–[182], spectrum auction bids [155], [183], subscriber identification [184], and database-driven DSA [54], [55], [180]–[182], [185] have been proposed.

A. Adaptation of existing privacy enhancing technologies

Direct adaptation of existing Privacy Enhancing Technologies (PETs), such as Searchable Encryption (SE) (e.g., [186]–[190]) and Oblivious Random Access Memory (ORAM) (e.g., [191] [192], [193]), which enable a client to outsource its data to a database in an encrypted form so it can perform search queries on it, cannot, for example, be used as they are in database-driven DSA to enable private spectrum information retrieval. There have also been proposed cryptographic techniques that enable generic (e.g., Fully Homomorphic Encryption (FHE) [194]–[196]) or specific (e.g., functional encryption [197], [198]) data processing over encrypted data, and these existing PETs cannot be directly adapted either to fit the CRN context, so that SUs' location privacy is preserved while still querying the spectrum database for availability information in an effective manner. Architectural differences and performance requirements of CRNs make direct adaptation extremely ineffective. Privacy-preserving search/access techniques, such as SE or ORAM, are specifically designed for a data outsourcing model [189], [190], [199], in which a client encrypts *its own data* with *its private key* and then outsources it to the database. However, in database-driven DSA, a third party owns and manages the spectrum database. Therefore, it is impractical for database owners to generate a searchable encrypted copy of the database for each single user (note that the initialization phase of these PETs are highly costly [187], [193]). Existing, fully generic techniques such as FHE [194], [195]) are, on the other hand, extremely costly and therefore impractical for CRNs.

That is said, there have been several attempts that aimed to adapt existing PETs to fit the CRN context. In the case of database-driven DSA for example, the proposed techniques that aim to protect the location information of SUs when they are querying databases for spectrum availability information rely on either k-*anonymity* [200], [201] or PIR (*private information retrieval*) [202], [203]. k-*anonymity* approaches (e.g., [55]) essentially rely on a third party, known as the anonymizer, to ensure that the probability of identifying the location of a querying user remains under $1/k$, where k is the size of the anonymity set to be received by the untrusted database (alternatively, the anonymity set can be constructed distributedly instead of relying on a third party). k-*anonymity* approaches are known to suffer from one major problem: they cannot achieve high location privacy without incurring substantial communication/computation overhead (e.g., higher privacy means higher k). They often compromise the location privacy at the benefit of lowering the incurred overhead, or vice-versa [204]. PIR-based approaches [54], [180], [181], on the other hand, offer much better privacy than k-anonymity approaches, but also incur substantial overhead, thus limiting their practical use for CRNs [205]. Proposed approaches relying on these technologies will be discussed in more details in later sections.

In what follows from this section, we take a closer look at some of the most known and generic PETs and discuss why they cannot be used off-the-shelf as they are in the context of CRNs to protect SUs from location inference attacks that exploit the vulnerabilities identified in Section II. These techniques, include *homomorphic encryption*, *oblivious transfer*, *private information retrieval*, *data outsourcing-based techniques*, *differential privacy*, and *secure multiparty computation*.

B. Homomorphic encryption

Homomorphic encryption is a special form of encryption that allows computations to be performed on ciphertexts. It generates an encrypted result whose decryption matches the result of operations performed on the plaintexts. There are two kinds of homomorphic encryption: full and partial.

1) Fully homomorphic encryption

This is a special type of homomorphic encryption which allows the computation of arbitrary functions on encrypted data without decrypting it. This concept was first introduced by Gentry [206] and is based on the properties of ideal lattices. Theoretically speaking, this is a very powerful concept as it permits the construction of a program that performs all kind of operations on the ciphertexts. Since such a program does not need to decrypt its inputs, it can be run by an untrusted party without revealing its inputs and internal state, making it an attractive tool for preserving privacy.

This might seem applicable in the context of CRN to hide, for example, the observations of SUs (proven to leak information about SUs location as discussed in Section II-A3a) during the spectrum sensing phase and share them with FC (or other SUs) without worrying about SU's location privacy. The main issue, however, with this type of encryption is that it involves high computation and requires large storage, making it unpractical. Another major issue with this encryption is

that the search time resulting from using fully homomorphic encryption is linear in the length of the dataset. This again makes it unpractical, especially for applications with large datasets like spectrum geolocation databases.

2) Partially homomorphic encryption

A partially homomorphic cryptosystem is an encryption scheme that, unlike fully homomorphic encryption, can only perform either multiplication or addition on the ciphertexts, but not both. Several cryptosystems with homomorphic propoerties were proposed in the literature. Paillier cryptosystem [207] is one of the most famous additive homomorphic schemes. Examples of multiplicative homomorphic cryptosystems include El Gamal [208] and RSA [209]. Thanks to their homomorphic properties, these schemes could be used in situations that require performing some basic operations on sensitive data while hiding user inputs (like when reporting sensing information).

Partially homomorphic encryption is more practical than the fully homomorphic one; however, for them to provide high security level, they incur large communication and computational overhead. This makes it unpractical to use especially for large CRNs if not used judiciously.

C. Oblivious transfer

Oblivious transfer (OT) is a privacy enhancing protocol that enables a sender to transfer one of many pieces of data to a receiver, while keeping the sender oblivious as to which piece has been sent and while making sure that the receiver receives only one message. The simplest flavour of this protocol, 1-out-of-2, was first introduced by Rabin [210] and was later generalized to 1-out-of-n and k-out-of-n cases. In the 1-out-of-n case, as explained in Figure 6, the sender has n messages and the receiver has an index i. The receiver wants to learn the i^{th} message without the sender learning i. On the other hand, the sender wants that the receiver only learns one message among the n messages. This could be thought of as a suitable approach to use for extracting spectrum availability information from the spectrum DB. This approach, however, incurs very large communication and computational overheads which makes it unpractical in a delay sensitive problem like spectrum availability discovery.

Figure 6: Oblivious transfer for the case 1-out-of-n

D. Private information retrieval (PIR)

This concept was first introduced by Chor et al. [202]. It allows users to privately retrieve records from a database while preventing the latter from learning which records are being retrieved. This could be thought of as a weaker version of 1-out-of-n OT which further requires that the receiver does not learn anything about the other entries in the database.

PIR approaches could be classified into two categories: Information-theoretic PIR and computational PIR. In information-theoretic setting, the reconstruction of the client's query is impossible no matter how much computation the adversary would perform. A trivial PIR approach could be to download the entire database. This would offer an information-theoretic privacy, i.e. unbreakable privacy, but on the other hand involves enormous communication overhead. Any information-theoretical PIR solution has a communication overhead of at least the size of the database as proven by Chor [202]. Fortunately, this applies only to the case where the database is stored only on a single server. One way to get around this extensive overhead is by assuming that the database is replicated in several servers that do not communicate with each other. This way, a non-trivial theoretic PIR solution that has communication overhead smaller than the database size turns out to be feasible. An information-theoretic approach in this model means that an individual database server cannot learn which element was retrieved by the user, no matter how much computation it may perform as long as it does not collude with the other servers [211]. Several approaches proposed in the literature considerably reduce the communication overhead of information theoretic PIR (e.g. [212] where the communication cost is $\mathcal{O}(n^{1/2k-1})$ with k is the number of database servers).

On the other hand, in computational PIR approaches, the security is based on hard-to-solve well-known cryptographic problems, e.g. discrete logarithm or factorization [213]. This makes them secure against computationally bounded adversaries. But an adversary with sufficient computational resources can learn the client's query by breaking the underlying security system. Some computational PIR approaches are able to provide poly-logarithmic communication complexity [211]. Gentry et al. [214] propose the most communication efficient PIR that has a constant communication overhead.

Even though research on PIR is making progress in terms of reducing the overhead, PIR approaches still suffer from large overhead that limits their practicality and impedes their off-the-shelf use without adaptation in the context of CRNs.

E. Data outsourcing-based techniques

These techniques are designed for applications that require secure data outsourcing, where a client's sensitive data is outsourced to a third-party storage provider, e.g. the cloud. Existing access control solutions focus mainly on preserving confidentiality of stored data from unauthorized access and the storage provider. Next, we discuss two well known data outsourcing based PETs: *searchable symmetric encryption (SSE)* and *oblivious random access memory ($ORAM$)*.

1) Searchable symmetric encryption (SSE)

Searchable symmetric encryption is a PET that is largely deployed to privately outsource one's data to another party while maintaining the ability to selectively search over it [215]. This means that a client needs to outsource its data to a database/server in an encrypted form to be able to later perform private search queries on it as shown in Figure 7. Despite its efficiency and the high level of privacy that SSE provides, it cannot be applied to database-based CRNs simply because in SSE, the data has to be outsourced by the client, whereas in

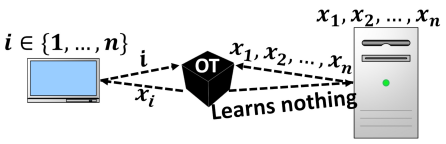


Figure 7: Searchable symmetric encryption

database based CRNs, the data about spectrum availability is generated and provided by the service operator that manages the spectrum database. This means that SUs have no control over this data and, thus, they cannot encrypt it and outsource it to DB as required by SSE.

2) Oblivious random access memory ($ORAM$)

Encrypting its outsourced data is not sufficient for a user to protect the confidentiality of his/her data content as his/her access pattern to the data remains unprotected which may reveal the user's private information. $ORAM$ is introduced by Goldreich et al. [216] to not only preserve data confidentiality but also to hide a user's access pattern to its outsourced data blocks. Traditionally, $ORAM$ has been designed to arrange the data such that the user never touches the same piece twice, without an intermediate shuffle. This erases the correlation between block locations and obfuscates the memory accesses of data, so that access patterns do not leak information about the stored data. Just like SSE, $ORAM$ can only fit to the problem of data outsourcing which is not suitable to the context of CRNs for the same reasons discussed for SSE.

F. Differential privacy

This is a recent privacy concept tailored to the statistical disclosure control problem which is defined as follows: how to release statistical information about a set of people without compromising the privacy of any individual [217]. Its goal is to assure a good statistical accuracy while preserving individual's privacy. It is a well established definition guaranteeing that queries to a database do not reveal too much information about specific individuals who have contributed to the database as suggested in [218]. The formal definition of this concept could be found in [219]. The basic idea behind it is that for two almost identical input data sets, the outputs of the mechanism that provides differential privacy are almost identical. More precisely, it requires that the probability that a query returns a value v when applied to a database $\mathcal{D}$, compared to the probability to report the same value when applied to an adjacent database $\mathcal{D}'$ (i.e. $\mathcal{D}$, $\mathcal{D}'$ differ in at most 1 entry) should be within a bound of $\exp^{\epsilon}$ for some privacy level ϵ. Since differential privacy is a probabilistic concept, any differentially private mechanism is necessarily random. A typical way to achieve this notion is to add controlled random noise, drawn from a Laplace distribution for instance, to the query output. One benefit of this concept is that a mechanism can be shown to be differentially private independently from any side information that the adversary might have.

However, standard differential privacy techniques usually perform poorly in situations where participants contribute various time-series data that could be aggregated and mined for useful information, due to noise [220]. Examples of time-series data may include users' current locations, weather information or information obtained from other participatory sensing applications like spectrum sensing in CRNs [220]. Moreover, the nature of differential privacy concept makes it poorly suitable for applications that involve a single user, such as spectrum database-based opportunities discovery, where the location of a single user has to be hidden. Thus, it requires that any change in a user's location have negligible effect on the published output of the query, which makes it impossible to communicate any useful information to the service provider [221]. Despite this, some approaches try to adapt this concept to the context of CRNs as we show in Sections IV & V.

G. Secure multiparty computation (MPC)

The concept of secure multiparty computation (MPC) originates from the works of Yao [222] and Goldreich et al. [223]. It allows a group of n mutually distrusting parties $P_1, ..., P_n$, holding private inputs $x_1, ..., x_n$ to securely compute a joint function $f(x_1, ..., x_n) = (y_1, ..., y_n)$ on these inputs [224]. The goal is to make each party P_i learn only y_i but nothing else. This could be achieved through an interactive protocol, executed between these parties, whose execution should be equivalent to having a trusted party that privately receives x_is from P_is, computes f and returns y_is to P_is. This protocol should be able to give the correct result to honest parties even if some parties are dishonest.

In a CRN context, this could be an attractive tool to provide privacy for any task that involves some computation between several entities. For instance, this could be used in distributed cooperative spectrum sensing during the spectrum discovery phase to allow SUs to collaborate in order to compute statistics over the sensing reports while preserving the privacy of their reports and thus their location. Another potential use of MPC could be during the coalition formation process, again in the spectrum discovery phase, to prevent leaking SNR values that can compromise SUs' location as explained in Section II-A3a. MPC could also be used in game theoretical approaches during the spectrum sharing phase to prevent the leakage that can arise from the local decisions shared between different SUs during the game. Furthermore, this could be an attractive tool also to protect the bids of SUs during the auction process that is performed to ensure spectrum sharing among SUs. As explained in Section II-C3c, the auction process may leak some information about SUs' location which makes it natural to consider leveraging sealed bids or relying on a trusted party for the auction. Ideally, an MPC protocol should be equivalent to a trusted third party; hence, MPC could play this role and replace an untrusted auctioneer as suggested in [224].

It is obvious that the potential applications of MPC are multifold due to its flexibility to emulate multiple scenarios. However, the bottleneck is its extensive computational and communication overhead, which makes its deployment difficult in practical situations, and more precisely in the context of CRNs, at least for the time being.

H. Summary

In this section, we explored a family of renowned PETs and generic crypto schemes that we believe are the most

relevant to CRNs. We highlighted the benefits and limitations of applying these schemes to CRN off-the-shelf as they are. In the following section, we will present and discuss location privacy preservation approaches proposed for protecting location privacy during the spectrum opportunity discovery process. We will explore the different threat models, location inference attacks, and location privacy preserving techniques that are specific to this spectrum discovery component.

IV. Location privacy preservation for spectrum opportunity discovery component

In this section, we investigate the different approaches proposed in the literature to deal with the location privacy issue in CRNs during the spectrum opportunity discovery phase. First, we discuss the challenges that face designing SU's location privacy preserving protocols in both cooperative spectrum sensing and geolocation database-based approaches. Then, we list the different threat models that need to be considered in these two approaches. After that, we detail existing and potential attacks that could be performed by malicious entities to localize SUs by exploiting the vulnerabilities that we identified in Section II-A. Subsequently, we describe existing solutions that are proposed to cope with these attacks and preserve SUs' location privacy. Finally, we explain the performance metrics that are or could be used to assess the performance and reliability of location privacy preserving protocols in CRNs, and present tradeoffs that are considered when designing these protocols.

A. Location privacy in cooperative spectrum sensing

As discussed in Section II-A3a, the cooperation among SUs during the sensing process gives rise to several vulnerabilities that could be exploited to compromise SUs' location privacy. Thus, location privacy preservation protocols for cooperative sensing need to be designed with several goals in mind:

- *Hide sensing information.* As explained in Section II-A3a, SUs' sensing reports may leak information about their locations [225]. Hence, one main goal of these protocols is to hide sensing reports by concealing the observed sensing information from decision makers or any potential external attackers that might eavesdrop SU's communications [11], [226]–[229].
- *Achieve accurate spectrum availability information.* Protocols need to preserve the location privacy of SUs, but without compromising their ability to still provide accurate spectrum availability information. Achieving this design goal is very challenging, due to its conflicting nature: hiding information for the privacy protection purpose may limit the ability to provide accurate spectrum availability information.
- *Optimize resource usage.* An important limitation that needs to be accounted for when designing privacy preserving protocols is SUs' resource capability. It is then important to design protocols that require minimum computation and storage resources and incur limited communication overheads. This, for instance, implies that expensive cryptographic approaches are to be avoided.
- *Hide SNR values.* Another goal that needs be aimed at is to hide the SNR values that SUs might need to exchange to form coalitions, for example. As explained in Section II-A3a, SNR may leak significant information about SUs' location, and thus a reliable location privacy preserving scheme needs to conceal these values without hindering the CRN operations relying on them.

1) Threat models

Several threat models are considered in the literature to study and address SUs' location privacy issue in cooperative spectrum sensing:

- *Dolev–Yao threat model.* In this model the adversary, usually an intruder, can overhear, intercept, and synthesize any message that is exchanged between SUs and FC or even between SUs themselves during the cooperative spectrum sensing process. The adversary is only limited by the constraints of the cryptographic methods used [230]. This model is considered in [53], [228], [229]
- *Semi-honest or honest-but-curious threat model.* This means that the adversary, that could be a FC [11], [226], [228], [229], a SU [228], [229] or an additional entity as in [229], follows the sensing protocol honestly without changing any of its parameters. However, it shows some interest in learning the location information of target SUs by exploiting their sensing reports.
- *Malicious threat model.* Entities in the CRN may be malicious, meaning that FC, SU or any other entity involved in the cooperative spectrum sensing process can change their parameters and lead several attacks to localize a target SU.
- *Non-collusion threat model.* FC, SUs and any other entities in the CRN do not collude to infer target SUs' location [228], [229]. This means that these entities do not share what they learned about target SUs' location during the cooperative spectrum sensing process.
- *Collusion threat model.* FC or some SUs may collude with other SUs or entities and work together to infer target SUs' location [11], [227] by exploiting their sensing reports and communication signals.

2) Location inference attacks

Location inference attacks exploit the vulnerabilities and the sources of leakage that we explained in Section II-A3a to localize SUs. These attacks could be performed by an internal entity (e.g. another SU or FC) or an external attacker that does not belong to the CRN. These attacks can be classified into two categories, based on the information used for localization: Geometric localization and fingerprinting.

a) Geometric localization based attacks

These attacks exploit channel parameter measurements including RSS, SNR, AoA, ToA and $TDoA$ to localize a target SU. RSS, SNR and ToA could be used to get the range information, as explained in Section II-A3a, which is essential for the trilateration localization technique [56], [72]. Trilateration is a very simple and intuitive approach that computes the position of a target node by finding the intersection of three circles that model the range with respect to at least three anchor nodes as depicted in Figure 8.

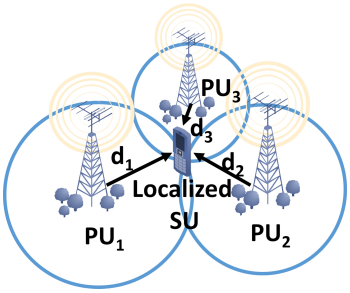


Figure 8: Localization of an SU via Trilateration using the ranges d_1, d_2 and d_3 corresponding to PU_1, PU_2 and PU_3 respectively.

In the context of CRN, the anchor nodes could be three PUs whose locations, depending on the situation, could be publicly known. Thus, an attacker that has access to the RSSs that a SU measures with respect to three channels could exploit this knowledge to localize SU using trilateration. SNR could also be used in a similar way, as reported in [72], for ad hoc CRNs. The attack can occur during the process of forming coalitions and choosing coalition heads as these operations require exchanging SNR information between SUs. Another attack scenario could involve multiple attackers or colluding nodes that belong to the CRN and that have a direct communication with the target node.

Triangulation is also another technique that exploits channel parameter measurements for localization purposes. It uses angles instead of distances and requires at least two reference nodes to localize the target node [231]. The two reference nodes measure the AoA of the signal coming from the target node. The position of the target node is the intersection of the two lines along the angles from each reference node as in Figure 9. As this attack requires a direct communication between the victim and the attackers, this implies that the attackers, which are also the reference nodes in this case, belong to the CRN, e.g. two colluding malicious SUs.

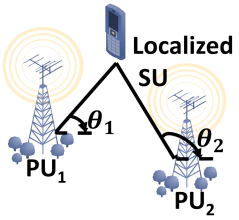


Figure 9: Localization of an SU via Triangulation using the angles of arrivals, AoAs, θ_1 and θ_2 of the SU's signal measured respectively at PU_1 and PU_2

Geometric localization attacks may be performed in CRNs that deploy crowdsourcing (explained in Section II-A1b) for spectrum sensing. For instance, Jin et al. [46] propose an attack scenario that targets the location privacy of participants in the crowdsourcing process. They consider a special setting where these participants compete to perform spectrum sensing tasks at specific locations via a reverse combinatorial auction operation [232]. During this auction, participants send their bids, corresponding to their claimed cost of performing the sensing tasks. This cost, as modeled by the authors, involves the round trip distance that a participant needs to travel to perform the sensing tasks and return back to its current location, called base location, which is the target of the proposed attack. This attack exploits the geometric relationship between users bids and the distance they travel to perform the sensing.

b) Fingerprinting based attacks

These attacks are more suitable in situations where the geometric relationships between SUs' positions and measurements cannot be established. It estimates the victim's location by finding the best matched fingerprint for the corresponding measurement within a pre-built RF map. It consists mainly of two phases: An off-line or training phase and an on-line or test phase. In the off-line phase, the RF map is generated. This map could be the REM (discussed in Section II-B1c) if the attacker is FC or a SU that has access to it, or it could be a map that an external attacker has built by itself. Figure 10 shows a simplified example of how this kind of localization works.

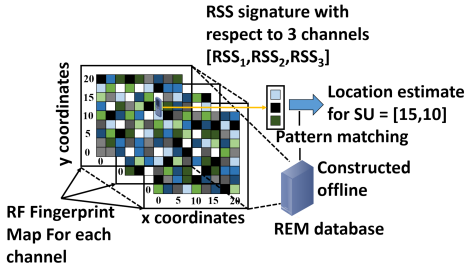


Figure 10: Localization of an SU via Fingerprinting using its RSS signature $[RSS_1, RSS_2, RSS_3]$ with respect to 3 channels and the REM database.

Li et al. [11] consider two attacks that rely on this principle to localize a SU based on its RSS measurements that it shares with FC in a centralized CRN. They assume that an attacker constructs a signal propagation model by collecting all the sensing reports transmitted within the network [11]. The attacker uses machine learning techniques, for example k-means classifier as in [11], to partition the RSS data into multiple sets corresponding to various locations. The first attack, called *single report location privacy (SRLP)* Attack, involves an external attacker that eavesdrops SUs' communications or an internal attacker that could be an untrusted FC or a compromised SU. Under this attack, the attacker exploits individual RSS measurements of SUs to localize them by computing the distance between each sensing report and the centroids of each cluster in the signal propagation model that is built beforehand by the attacker. The second attack that they propose is called *differential location privacy (*DLP*)* attack which estimates the sensing report of a SU during the aggregation process performed by FC. In this attack, the attacker compares the changes of the aggregation results after a SU joins or leaves the CRN and then it infers its location by finding to which cluster the estimated report belongs to, just like in the *SRLP* attack.

It is worth mentioning, however, that even though fingerprinting could be attractive for leading location inference attacks, it is not necessarily practical unless the attacker is

TABLE III: Location privacy preserving schemes in cooperative spectrum sensing

Countermeasures	Attacks Considered	Techniques	Pros	Cons
Li et al. [11]	- Location inference from sensing reports (e.g. RSS)	- Privacy preserving aggregation with encryption - Dummy report injection	- Relatively efficient against differential privacy attacks	- Very high computational and communication overhead - No fault tolerance - Has a little negative effect on the sensing performance
Grissa et al. [228]	- Location inference from sensing reports (e.g. RSS)	- Private comparisons using Yao's millionaires protocol - Order preserving encryption	- Low communication overhead - High location privacy	- Relatively high computational overhead
Mao et al. [226]	- Location inference from sensing reports (e.g. RSS)	- *El Gamal* cryptosystem	- Considers both semi-honest and malicious adversaries	- High communication overhead - Prone to *DLP* attack
Wang et al. [227]	- Location inference from sensing reports (e.g. RSS) - Collusion between service providers - Collusion between service providers and SUs	- Cloaking of sensing reports - Dimension reduction of sensing data through non-invertible projection	- Considers multiple malicious service providers - Considers collusion between some entities - Provides differential privacy	- Privacy level decreases with the decrease of service providers - Privacy level decreases with the increase of SUs - Some information distortion during the cloaking process
Kasiri et al. [72]	- Location inference from SNR during coalition formation	- Anonymization of SNRs	- Takes into account SUs' mobility	- Privacy level decreases as the number of sensed channels increases - Providing high location privacy degrades sensing performance
Grissa et al. [229]	- Location inference from sensing reports (e.g. RSS)	- Additional entity in the network - Order preserving encryption	- Very low communication & computational overhead - High location privacy	- Additional entity that needs to be managed by a third party for non-collusion
Jin et al. [46]	- Location inference from sensing cost during reverse auction - Location inference from auction result - Location inference from changes in auction participation	- Exponential mechanism for differential privacy	- Offers differential location privacy	- The lower the social cost the higher the location information leakage

very powerful with lots of resources. This is due to the fact that the construction of accurate radio maps and fingerprints requires considerable off-line effort and may give rise to several challenges. These include, but are not limited to, the huge number of measurements that need to be taken and also the need to regularly update the radio map due to the inherent time varying nature of wireless channels and networks [56].

3) Location privacy preserving approaches

As explained in Section II-A1b, SUs in cooperative spectrum sensing CRNs need, first, to share their observations either with FC (in centralized CRNs) or with other SUs (in distributed CRNs). These local observations are then combined to make a cooperative spectrum availability decision. These observations could be statistics computed over the signal or just local binary decisions made by each SU individually. Both cases present some privacy risks to SUs as discussed in Section II. Thus, research efforts should focus on hiding SUs' observations from the other entities in the network. Most of the existent works that we discuss in this Section consider the location inference attack from the sensing reports that SUs share. We summarize these works in Table III and we discuss them in more details in the following.

Li et al. [11] introduce an approach that uses secret sharing and the privacy preserving aggregation process proposed in [233] to conceal the content of the sensing reports. This scheme uses also dummy report injections to replace the report of a leaving SU in order to cope with the differential location privacy attack (explained in Section IV-A2b) and prevent a malicious FC from estimating the sensing report of the leaving SU. Moreover, this scheme can bear collusion attacks involving FC and some compromised SUs. Despite its merits, it has several limitations: (i) FC needs to collect all the sensing reports in order to be able to decode the aggregated result. Obviously, this could not be fault tolerant, since some reports may be missing due, for example, to the unreliable nature of wireless channels. (ii) It cannot handle network dynamism if multiple SUs join or leave the network simultaneously, as it can only deal with the event of one SU leaving or joining the network at a time. (iii) The pairwise secret sharing requirement, that this scheme has, incurs extra communication overhead and delay. (iv) The underlying encryption scheme requires solving the discrete logarithm problem [213] for the decryption, which is extremely costly and is only possible for very small plaintext space.

Grissa et al. [42], [228] propose a location privacy preserving protocol that aims to hide SU's sensing reports (specifically RSS) from FC and the sensing threshold used for the decision from SUs. This prevents FC from trying to localize SUs using their sensing reports and, at the same time, prevents malicious SUs from using the sensing threshold to manipulate their measurements and impact FC's decision. This scheme relies on *order preserving encryption* [234] to make SUs encrypt their sensing reports and allow FC to learn only the relative order of these reports. Using this order

and following a binary search-like technique, FC executes at most $\log\ n$ private comparisons between SUs' RSSs and FC's sensing threshold using *yao's millionaire* protocol [235]. The order learned by FC aims to make the number of private comparisons logarithmic in the number of SUs. This is shown to provide high location privacy to SUs while enabling an efficient sensing performance. However, even though this approach has a low communication overhead and a logarithmic computational overhead as a function of the number of SUs, the computation incurred is still relatively high. This is due to the use of the expensive *yao's millionaire* protocol [235] that, itself, relies on expensive homomorphic encryption.

Some approaches consider an intermediate node or entity to help addressing the location privacy issue, e.g. [226], [229]. Mao et al. [226] provide an approach that requires SUs to encrypt their RSS values using a derivative of *El Gamal* [208] encryption scheme. In their approach, one of SUs is picked to play the role of a helper to FC. First, the *Helper* and FC collaborate to construct a public/secret key pair and each of them keeps a part of the secret key for itself. Then, FC and *Helper* share the public key with SUs. Subsequently, SUs send their RSSs encrypted using this public key to the *Helper* that permutes them, decrypts them with the secret part that it has, and then sends them to FC which decrypts them using its part of the key. Once decrypted, FC aggregates the RSS values to make a final decision. The authors consider a semi-honest threat model for FC and Helper and a restricted malicious model where only SUs are malicious. However, even though this approach guarantees that individual sensing reports cannot be revealed neither to FC nor to the Helper, it incurs high communication overhead. In order to provide high enough security level, the keys of El Gamal cryptosystem, and hence the size of the ciphertexts, need to be very large. This makes the communication cost very high, especially when the number of SUs is large. Moreover, as FC can learn aggregated sensing reports of SUs, this scheme is still prone to the *DLP* attack explained in Section IV-A2b.

Grissa et al. [42], [229] propose another approach that relies also on *order preserving encryption (OPE)* and on deploying an additional node, referred to as *gateway (GW)*. GW is deployed to perform private comparisons between SUs' sensing reports and the decision criteria or threshold of FC. This is done by making each SU encrypt its RSS, using OPE and a unique secret key shared with FC, and send it to GW. FC also sends n encryptions of its sensing threshold, using OPE and the n keys established with SUs, and sends them to GW. On top of the OPE encryption, each entity communicating with GW encrypts its data with a key uniquely established with GW to secure the communication. GW removes the second layer encryption and compares each OPE encrypted RSS to its corresponding OPE encrypted sensing threshold (the one that FC has constructed with the same secret key). The main advantage of this approach is its high efficiency in terms of communication and computational complexity due to its reliance on symmetric encryption only. The high efficiency benefits of this technique comes, however, at the cost of needing an additional architectural entity, GW, that has to be managed by a third party to avoid collusion with SUs or FC and to provide the claimed privacy guarantees.

Other approaches consider a different CRN scenario that consists of multiple service providers (SPs) that may exchange sensing data among themselves as in [227]. Wang et al. [227] propose a framework that aims to preserve SUs' privacy in collaborative spectrum sensing from malicious SPs. It assumes that the only trustworthy SP for a SU is the one serving it. The remaining SPs and SUs may collude to infer private information about a target SU, including its location. To preserve SUs' privacy, this framework hides individual sensing data of SUs by making each SP transform sensing reports of corresponding SUs into cloaks. To find the optimal cloaking strategy, each SP projects its original sensing data to a single-dimensional space, with minimal data distortion [227], using a privacy-preserving non-invertible projection and shares statistical information of the projected data with one SP picked as a leader. The leader uses this information to decide about the optimal cloaking strategies and shares it with the other SPs. The authors rely on dynamic programming to obtain the optimal cloaking strategy that minimizes information distortion and that is obtained through collaboration between SPs. This scheme considers collusion between different malicious entities and provides *differential privacy* to SUs. However, its privacy level decreases with the decrease of the number of SPs and the increase of the number of SUs. It also introduces some distortion to the sensing information which may impact the sensing accuracy.

Some works try also to address the location privacy issue in distributed cooperative sensing. For example, Kasiri et al. [72] address this issue in multi-channel cognitive radio *MANET*s. They propose a scheme that relies on the notion of anonymization to prevent location information leakage from SNR values that are exchanged between SUs for coalition formation purposes. Anonymization is achieved by means of random manipulation and distortion of the exchanged SNRs, which can leak information about the location of SUs as shown in Section II-A3a. Each SU creates an anonymization area with respect to each sensed channel. However, a major limitation of this scheme is that the more channels sensed by a SU the more likely it is to be located as the adversary can intersect the anonymization areas to narrow down SU's location. Another limitation is that it cannot achieve high location privacy without degrading the sensing performance of the CRN. Indeed, the authors present a tradeoff between privacy and performance as both cannot be maximized together.

Some works try also to preserve the location privacy of users that participate in the crowdsourcing process, which is used to recruit distributed mobile users to sense a given channel around specific locations. For instance, Jin et al. [46] formulate participants selection process as a reverse auction problem where participants compete to perform spectrum sensing tasks in return for rewards. Each participant's true cost for performing the sensing tasks is closely related to its current location as explained in Section IV-A2. The authors rely on the exponential mechanism to protect the location information and prevent the attack that they have identified (explained in Section IV-A2). Users are selected iteratively for each sensing sub-task following the exponential mechanism to

guarantee differential privacy for their bids, and consequently differential location privacy. While protecting location privacy, this approach aims to minimize the social cost that represents the sum of the real costs of users completing all the sensing tasks. However, minimizing this cost deteriorates the location privacy level, which is the main limitation of this approach.

4) Performance metrics and tradeoffs

a) Performance metrics

Computational complexity: This is an important metric as SUs are usually resource constrained. Thus, it is paramount to consider this when designing a location privacy preserving scheme for CRNs. This metric usually accounts for the overhead resulting from the various operations required by the scheme (e.g., cryptographic operations) and incurred by all different entities involved in the privacy preserving protocol, and could be measured separately for each entity or as a whole for the entire system. Computational complexity has a direct impact on the delay that a SU may experience before getting the decision about the spectrum availability. Computational complexity is considered in most of the research works that address the location privacy issue in cooperative spectrum sensing in CRN, e.g. [11], [72], [226], [228], [229].

Communication overhead: Communication overhead is another important metric that needs to be considered. Location privacy preserving schemes must not overwhelm the network by incurring high communication overhead that may lead to the degradation of the overall system performance, especially provided that bandwidth and/or energy resources are often limited. Encryption, which most proposed solutions rely on to ensure privacy, tends to incur, depending on the size of ciphertexts, heavy communication overheads. Another factor that also tends to contribute to this overhead is the number of SUs involved in the cooperative sensing task.

Spectrum availability accuracy: It is important to protect SUs' location privacy, but while making sure that doing so does not interfere with the cooperative sensing task. Therefore, another important metric is the ability of these privacy preserving schemes to perform the sensing task accurately. This is quantified, for example in [72], using the detection probability to capture the impact of the privacy preserving scheme on detecting PUs presence.

Location privacy level: As the ultimate goal of any location privacy preserving protocol is to preserve the location privacy of SUs, it is then paramount to have a metric that can be used to assess and quantify the privacy level. There are several metrics that could be used for capturing this:

- *Anonymity level*: This measures the level of anonymity provided by the cloaking algorithm and usually refers to the size of the area to which a SU generalizes its location to achieve anonymity. One way to quantify this is by computing a relative measure normalized by the anonymity level required by a SU. Kasiri et al. [72] rely on a similar approach and define the location privacy level of a specific SU as the ratio between the anonymized area with respect to all PUs and the maximum anonymized area of that SU. The privacy level for the whole network is obtained by computing the average of the location privacy levels over all SUs.
- *Entropy*: This shows how uniform the probability of locating a SU at a specific position is and it is used to measure the uncertainty level that an adversary has [236]. Li et al. [11] have used this concept to quantify the location privacy level of their schemes. The area covered by the CRN is divided into sub-regions, forming a set $\mathcal{G} = \{g_1, g_2, \cdots, g_m\}$. The uncertainty of the adversary, and thus the location privacy level of a SU i involved in the cooperative spectrum sensing, is then defined as:
$$\mathcal{A}(i) = -\sum_{b=1}^{m} p_{i|b} \log(p_{i|b}) \tag{4}$$
where $p_{i|b}$ is the probability that SU i is located in sub-region g_b. The location privacy level for the overall system is then given by $\mathcal{A} = \sum_{i=1}^{n} \mathcal{A}(i)$, where n is the number of SUs. If an attacker can uniquely infer that SU i is located at sub-region g_b, then $p_{i|b} = 1$, i.e. $\mathcal{A}(i) = 0$. On the other hand, if the attacker is unable to tell which sub-region SU is located in, which means SU could be located at any region with equal probability $p_{i|b} = 1/m$, then the privacy level for SU i would be $\mathcal{A}(i) = \log m$, which is the maximum privacy level it can get when participating in the cooperative sensing.
- *ϵ-differential privacy*: This concept is based on the differential privacy concept (discussed in Section III). A mechanism $\mathcal{M}$ is said to provide ϵ-differential privacy for a SU i if for any two sets of sensing reports, $R = [r_1, \cdots, r_i, \cdots, r_n]$ and $R' = [r_1, \cdots, r'_i, \cdots, r_n]$, that differ only on i's sensing report, we have:
$$|\ln \frac{Pr[\mathcal{M}(R) = \mathcal{O}]}{Pr[\mathcal{M}(R') = \mathcal{O}]}| \leq \epsilon \tag{5}$$
for all $\mathcal{O} \in Range(\mathcal{M})$ with $Range(\mathcal{M})$ is the set of all possible outputs of $\mathcal{M}$ [227] . The privacy level is controlled by the parameter ϵ with higher privacy is ensured by lower ϵ values. Very low values of ϵ ensure that $Pr[\mathcal{M}(R) = \mathcal{O}]$ and $Pr[\mathcal{M}(R') = \mathcal{O}]$ are roughly the same, meaning that the output $\mathcal{O}$ is not sensitive to the changes of any single SU's sensing reports.

Location privacy could also be quantified using the concepts of *inaccuracy* and *incorrectness* introduced by Shokri et al. [236]. These concepts could be redefined to fit the context of location privacy in CRNs as done in [237]. First, let Θ denote the observed sensory information that could be used to localize a SU, and x and x_c represent the location estimated by the attacker and the actual SU's location, respectively. Let also $p(x|\Theta)$ be the probability distribution of all possible values of the target SU's location given the observed information. Essentially, this probability models the adversary's extracted information from its observations.

- *Inaccuracy*: This is the discrepancy between the posterior distributions $p(x|\Theta)$ and $\hat{p}(x|\Theta)$ which basically quantifies the difference between SU's real location distribution and the adversary's estimated location distribution.
- *Incorrectness*: This is the distance (or expected distance) between the true SU's location and that inferred by the

attacker. This metric is shown in [236] to be the most appropriate for quantifying location privacy. The expected distance, which is the adversary's expected estimation error, can be written as $\sum_x \hat{p}(x|\Theta)\|x - x_c\|$, where $\|\cdot\|$ is a distance, e.g. euclidean, between x and x_c.

b) Performance tradeoffs

Several performance tradeoffs could be made when designing location privacy preserving schemes for cooperative spectrum sensing:

Scheme overhead vs. hardware cost: Scheme overhead in terms of communication, computation, and/or energy could be reduced at the cost of additional architectural components. For example, Grissa et al. [229] introduce and rely on an extra network entity to reduce both communication and computational overheads while also improving privacy. This reduction in overhead is achieved by means of this new entity, introduced to carry out the private comparisons between SUs and FC without disclosing RSS values. Without such an entity, these comparisons would have been very expensive, resulting in an excessive scheme overhead.

Privacy level vs. scheme overhead: Achieving higher location privacy at the cost of deploying more expensive cryptosystems with higher communication and/or computation overhead is another tradeoff researchers often make. For example, the works in [11], [226], [228] make such tradoffs in order to improve the location privacy of their schemes.

Privacy level vs. sensing accuracy: Higher location privacy can also be obtained at the cost of willing to degrade the sensing performance of the CRN. For example, such a tradeoff is made in the approach proposed by Kasiri et al. [72], where the anonymization area, capturing the privacy level, is increased but at the cost of decreasing the average detection probability, representing the CRN sensing performance.

B. Location privacy in database-based spectrum discovery

Here, the location privacy issue is completely different from that of the cooperative sensing-based CRNs. In fact, as explained in Section II-A2, each SU is now required to send its exact location to DB in order to learn about spectrum opportunities in its vicinity. This makes preserving the location privacy of SUs more challenging, since an adversary does not need to perform any extra computation to estimate the position, and the location information here could be easily extracted from the query itself. Thus, location information preserving schemes for database-based CRNs need to be designed with two conflicting goals: i) hiding or not including SU's location information in the query to be sent to DB, and ii) in response to a SU's query, DB needs to inform SU about spectrum availability in SU's vicinity. The second goal above somehow entails that DB needs to know where SU is located at, and thus, meeting these two conflicting requirements is very challenging. As we will see later, this cannot be achieved without making some performance tradeoffs.

1) Threat models

Several threat models are considered in the literature to study and address SUs' location privacy issue in database-driven CRNs:

- *Dolev–Yao threat model*: The adversary, usually an intruder, can overhear, intercept, and synthesize any message exchanged between SUs and DB. More specifically the adversary can learn the location of an SU from the query that the latter sends to DB to learn spectrum opportunities. The adversary here is only limited by the constraints of the used cryptographic schemes [230]. This model has been considered in several works [54], [238].
- *Semi-honest* or *honest-but-curious threat model*: The adversary, usually DB, follows the sensing protocol honestly without changing any of its parameters, but shows some interest in learning the location of target SUs [54], [55], [181], [182]. This means that it responds to SUs queries with correct spectrum availability information, but at the same time tries to learn their whereabouts.
- *Malicious-entity threat model*: DB, or an intermediate BS, may be malicious, i.e. they can change protocol parameters to localize a target SU that is querying DB. In some situations, the malicious entity could even be a sophisticated adversary that has considerable resources and has access to information from DB [239].

2) Location inference attacks

The most straightforward and basic attack is based on SU's query content. A SU needs to include its exact location in its query to DB. This makes it vulnerable to an intruder, that can learn its location by eavesdropping its queries, or even to DB that has access to these queries. Typically, DB's response to a SU's query contains spectrum availability information; e.g., the list of available channels in SU's vicinity and the maximum allowed transmit powers in each of these available channels. An adversary that has access to this information could localize a target SU by overlapping the availability areas of the different channels available at SU's location as explained in Section II-A3b. This kind of attack assumes that the adversary has knowledge about the RF environment covered by DB as well as the activity and coverage of PUs. The adversary can also exploit the fact that the allowable secondary transmit powers are highly correlated to the relative distance between a SU and a PU as discussed in Section II-A3b. This has been exploited by Zhang et al. [55] to identify a unified attack framework to localize both SUs and PUs based on the MTP function introduced in [237]. The MTP calculated by DB is divided into several levels based on the distance between SU and PU. Specifically, when this distance is less than a certain protection radius, SU is not permitted to transmit on PU's channel. Beyond the protection radius, SU can transmit at an increased power level as its distance from PU increases until it reaches the maximum allowed transmit power as regulated by FCC.

3) Location privacy preserving approaches

We summarize the approaches that are proposed in the literature to cope with the location privacy issue in database-based spectrum discovery in Table IV and we discuss them in more details in the following. Generally speaking, most existing techniques attempt to protect SUs' location privacy by adopting one of two techniques/concepts: *k-anonymity* [240] or PIR (*private information retrieval*) [202].

As discussed in Section III, *k-anonymity*-based approaches try to ensure that the probability of identifying the location of a querying SU remains under $1/k$, where k is the size of the anonymity set to be received by the untrusted DB. *k-anonymity*-based approaches are known to suffer from one major problem: they cannot achieve high location privacy without incurring substantial communication/computation overhead. Furthermore, it has been shown in a recent study led by Sprint and Technicolor [241] that anonymization based techniques are not efficient in providing location privacy guarantees, and may even leak some location information.

For instance, Zhang et al [55] rely on the *k-anonymity* concept to provide a location privacy preserving mechanism to protect the location privacy of both PUs and SUs. The proposed scheme requires that each SU queries DB by sending a square cloak region that includes its actual location instead of just sending this location. SU keeps querying DB using the same cloak region to avoid further location information leakage. This scheme requires a tradeoff between high location privacy and spectrum utility, which means that achieving a high location privacy level results in a decrease in spectrum utility. This limits the applicability of this kind of approaches as they impact the main goal of CRNs which is optimizing spectrum utilization efficiency. As discussed earlier, a good approach should provide location privacy to SUs but without hindering the functioning of CRNs.

k-anonymity is also used by Li et al. [182] to protect SUs' location privacy during the commitment phase in which SUs have to register the channels that they are planning to use as explained in Section II-A3b. In this approach, SUs first send their channel requests to the BS that they are associated with, using pseudonyms that are randomly generated by a certification authority. BS, then, queries DB on behalf of the querying SUs using their pseudonyms. After that, DB performs hash matching of SUs' pseudonyms with a hash matrix provided by the certification authority to verify SUs' pseudonyms. Subsequently, DB assigns a set of channels to BS based on the latter's location. BS then allocates the channels to its SUs using a coloring model to prevent interference between them. Finally, BS registers the used channel of each SU in DB by including dummy information to provide *k-anonymity* to the utilization information. This is done by registering more channels than the number of SUs' requests to confuse attackers and prevent them from using the utilization information to localize SUs. Using BS to register the used channels helps cutting off the relation between the registered channels and SUs' identities, which makes it harder for DB to associate this information to corresponding SUs and, hence, localize them. Thus, the proposed scheme can decrease the probability of localizing SUs. However, it requires that BS is trustworthy or it would not be able to protect SUs' location. This assumption is not usually realistic as it is hard to guarantee trustworthiness in practice. It suffers from the fact that the probability of localizing SUs increases as the number of switching events increases or as the number of BSs decreases.

PIR-based approaches [54], [180], [181], on the other hand, offer much better privacy than *k-anonymity*-based approaches, but incur substantial computation and communication overhead, thus limiting their practical use for CRNs [205], unless used judiciously as discussed in Section III. For instance, Gao et al. [54] propose a PIR-based location information preserving scheme by adopting the PIR protocol of Trostle et al. [242]. Instead of sending its location, SU hides its coordinates within other locations and transforms this information in such a way that SU is the only one that can revert it. Upon receiving the blinded query, DB multiplies it with the spectrum availability information matrix and sends the outcome back to SU. SU will be able to only retrieve the availability information in its location using the secure parameters that it used to transform the original query. SU is the only one who knows the blinding factors and the transformation used to transform the original query. Hence, only SU can recover the spectrum availability information from the result sent by DB. However, this approach suffers from large computational overhead which is due to the use of the PIR protocol, known to be expensive to execute as we highlighted earlier.

Grissa et al. [53] propose an approach that offers an unconditional privacy to SUs within the DB's coverage area. This approach uses set membership data structure, more precisely *cuckoo filter* [243], to send a compressed version of DB to SU. In this scheme, SU only sends its characteristics, but not its location, to DB, which it uses to adapt the content of the *cuckoo filter*. After receiving the filter, SU constructs a query that includes its location and a combination of other parameters (e.g. band frequency, transmission power level, etc) and queries the filter to check whether it contains the constructed query. If it is the case, SU can deduce that the channel is available and can use it by following the parameters specified in the query. Otherwise, SU concludes that the specified combination does not exist in DB and keeps querying the filter with different combinations until it finds one or reaches the filter's capacity. Obviously, the main advantage of this scheme is that it provides optimal location privacy to SUs as opposed to the other approaches. However, it incurs a relatively large communication overhead especially when the size of DB is huge. The authors try to address this issue by proposing to sacrifice one of SU's coordinates to considerably reduce the size of the filter while providing reasonable privacy. This is not needed when the size of DB is not large.

Troja et al. [180] propose another PIR-based approach to protect the location privacy of mobile SUs. The PIR mechanism used in this work allows a SU to learn spectrum availability in multiple-cell block containing its current cell. As they move, SUs gradually develop a trajectory-specific spectrum knowledge cache, via a series of PIR queries. SUs within communication range of each other form groups and interact in a peer-to-peer (P2P) manner to privately exchange their anonymized cached channel availability information. This reduces considerably the number of PIR queries as less SUs need to query DB since they could learn opportunities from SUs within their group. However, this still incurs large communication cost and relatively high computational overhead, especially when the group size is relatively large.

Troja et al. [181] propose another PIR-based privacy-preserving protocol that relies on the Hilbert space filling curve which is a continuous fractal that maps space from *2-D* to

TABLE IV: Location privacy preserving schemes in database-driven spectrum opportunities discovery

Countermeasures	Attacks Considered	Techniques	Pros	Cons
Zhang et al. [55]	- Location inference from maximum transmission power - Location inference from channel switch	- Cloaking the query of SU within a square region based on *k-anonymity*	- Provides location privacy for both SUs and PUs	- High location privacy degrades spectrum utility
Li et al. [182]	- Location inference from spectrum utilization information	- Intermediate base stations to forward SUs' queries to DB - Intermediate base stations for spectrum allocation - *k-anonymity* for registering used channels	- Adversaries cannot link usage information to SUs - Decreases SUs' geolocation probability	- The probability of geolocating SUs increases with the number of available channels. - The probability of geolocating SUs increases with the number of switching events
Gao et al. [54]	- Location inference from query - Location inference from spectrum utilization information	- Query blinding via PIR - Spectrum mobility reduction	- Low communication overhead - Reduces the localization probability of SUs	- High computational overhead
Grissa et al. [53]	- Location inference from query	- Sending portion of DB to SU using cuckoo filter	- Very low computational overhead - Provides ideal location privacy	- Large communication overhead if DB is huge
Troja et al. [180]	- Location inference from query	- Collaboration between SUs - *private information retrieval*	- Minimal number of PIR queries via collaboration between SUs - Takes into account SU's mobility	- Large communication overhead - Relatively high computational overhead
Troja et al. [181]	- Location inference from query	- Hilbert space filling curve indexing of DB - *private information retrieval*	- Takes into account SU's mobility - Minimal number of PIR queries via trajectory prediction	- Relatively high computational overhead
Zhang et al. [239]	- Location inference from query	- Random obfuscation using Laplacian noise	- Provides differential location privacy for both SUs and PUs	- Increasing the location privacy level decreases the utility of both PUs and SUs

1-D [244]. DB is indexed based on this curve to address SUs' mobility which allows neighboring cells to be stored in consecutive locations in DB. DB is split into multiple disjoint segments which enables SU to retrieve channel availability information for a large number of consecutive cells surrounding SU's location with a single PIR query. SUs use trajectory information, known a priori or generated on the fly via a prediction mechanism, to minimize the number of future PIR queries as a SU can obtain availability information for current and future positions in just one query. Despite its merit in providing location privacy to mobile SUs with efficient communication overhead, this approach incurs relatively large computational overhead. The main advantages of this scheme are that it considers mobile SUs and exploits trajectory information to reduce the number of PIR queries to DB in order to reduce overhead. However, it still suffers from one of the well known limitations of PIR-based approaches, i.e. the high computational overhead, despite its nice effort in reducing the number of required queries.

Other approaches try to adapt the *differential privacy* concept, explained in Section III, and apply it in the context of database-driven CRNs. For instance, Zhang et al. [239] propose an approach to protect bilateral location privacy of both PUs and SUs. SUs obfuscate their location using a two dimensional *Laplacian* distribution noise satisfying the ϵ-*geo-indistinguishability* mechanism, derived from *differential privacy*, introduced in [221]. The obfuscation depends on the privacy preserving level that is decided by both SUs and PUs by solving an optimization problem that maximizes their bilateral utility. SU sends its obfuscated location along with the privacy level which represents the maximum distance that separates the sent location from the actual location. Based on these parameters, DB decides about the transmit power and radius or distance from PU that SU cannot exceed. The main advantage of this approach is that it provides differential location privacy for both PUs and SUs while allowing them to adjust their privacy level to maximize their utility. However, as this approach aims to maximize both the utility and privacy level, which are always conflicting, increasing the privacy level of both PUs and SUs often results in decreasing their utility, and striking a balance is challenging.

4) Performance metrics and tradeoffs

a) Performance metrics

Computational complexity: Making sure that these schemes do not require heavy computation at both ends, SU and DB, is crucial to the design of such schemes. This is important merely because these SU devices, again, are usually resource constrained (in both energy and CPU), and the applications running on them may not tolerate delays. In addition, it is highly desirable not to overwhelm DB by involving it in heavy computations, which can lead to congestion. Several works (e.g., [53], [54], [180], [181]) use this as a metric for assessing the effectiveness of their proposed approaches. For example, Troja et al. [181] captures the computation overhead by measuring the average cumulative response time that their proposed scheme leads to. This time includes the query generation time at SU, the processing time at DB, the network transfer time, and the resulting extraction time at SU.

Communication overhead: Another crucial performance metric is to assess how much network data the proposed scheme generates. This assesses whether adding a privacy preserving scheme would inundate the network and degrade its performance. Indeed, a large communication overhead may introduce a considerable delay that may leave the spectrum availability outdated and cause interference to PUs if SUs decide to use channels based on this outdated information.

Location privacy level: In addition to the privacy concepts

already discussed in Section IV-A4a, the following can be used to assess the privacy level of any given scheme.

- *Localization probability:* This is basically the probability that a SU is geolocated successfully by an attacker under a given scheme. It may be influenced by different parameters, e.g. the number of channel switching events, the number of BSs in the network, etc. Some approaches like [182] have considered this metric to evaluate their approach's privacy level.
- *Size of possible location set:* This measures the granularity of the location that an attacker can infer about a SU. A privacy preserving scheme fails completely to protect the location of a SU if the size of this set is equal to 1, which means that the attacker has succeeded to determine the exact cell in which SU is located [54].

b) Performance tradeoffs

Location privacy vs. spectrum utilization: This tradeoff consists on sacrificing some utility to provide high location privacy guarantees. This means that seeking a higher privacy level will necessary reduce the utility in question. For instance, Zhang et al. [55] make a tradeoff between the location privacy of both SUs and PUs, and spectrum utilization. SUs and PUs can adjust their privacy levels to maximize their utilities. In this case, increasing the location privacy level would decrease the spectrum utilization and vice versa.

False positive rate vs ideal privacy: Some approaches, like [53], use set membership data structures to construct a compact representation of DB and make SUs query it for spectrum availability. However, this kind of data structures, despite its efficiency in compacting large sets of data, could introduce some false positives when it is queried. This means that the result of query may reveal that a channel is available while in reality it is not. Some data structures, like the *cuckoo filter* used in [53], give the possibility to control this rate. Minimizing this rate will, however, increase the communication overhead. So the tradeoff here is to allow some false positives in the filter to guarantee ideal privacy to SUs.

C. Summary

In this section, we discussed the location privacy issues in the spectrum opportunity discovery component for both cooperative spectrum sensing-based and database-driven spectrum discovery. We detailed the different threat models and attacks that target the location information of SUs. We then presented the different approaches that are proposed in the literature to deal with these issues. Finally, we explained the different performance metrics that are or could be used to assess the efficiency and the privacy level of location privacy preserving protocols in CRNs. In the following section, we will follow the same structure and reasoning to discuss the location privacy issues in the remaining CRN components.

V. Location privacy preservation in other CRN components

In this Section, we investigate SUs' location privacy issue in the remaining CRN components of the cognition cycle. Unlike the spectrum opportunity discovery component, much less attention has been given by the research community to the location privacy issue in these components. The design goals of privacy preserving schemes for each of these components are then to address the sources of location information leakages discussed in Section II-B (spectrum analysis), Section II-C (spectrum sharing), and Section II-D (spectrum mobility).

A. Threat models

The same threat models that we have discussed previously in the spectrum opportunity discovery phase apply to the remaining components of the cognition cycle. Thus, we skip these threat models here and we refer the reader to Sections IV-A (cooperative spectrum sensing) and IV-B (database-based spectrum opportunity discovery) for more details.

B. Location inference attacks

Some of these attacks may target SU's location during the dynamic spectrum auction process. For instance, Liu et al. [155] identify an attack that exploits two sources of leakage, highlighted in Section II-C3c: bid channels and bid prices. The first attack uses bid channels (i.e. channels that are bid for by a SU). As explained earlier, a SU bids only for channels that are available for it, i.e. SU belongs to the complement area of each corresponding PU's coverage. Hence, a malicious auctioneer can use the SU's available set of channels, obtained from the SU's bids, to decrease its possible location range by intersecting the complements of the corresponding PU's coverage areas as shown in Figure 11. The second attack exploits the bid

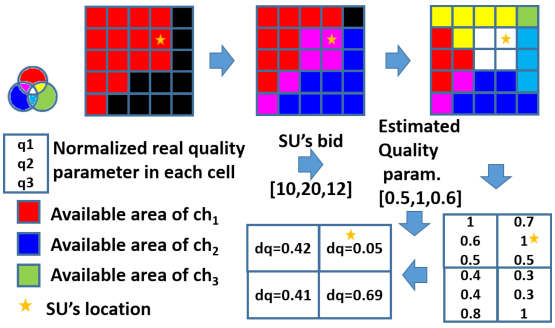


Figure 11: An example of the attacks identified in [155] which first estimate the position of an SU to be in the intersection of the available areas of channels 1, 2 and 3. Then, the attacker further narrows down the estimated area by picking the cell having the smallest distance between the exact channels' qualities and those estimated from bid prices.

prices, which depend on the quality and characteristics of the spectrum known to be highly correlated to SU's location. It could be used after the first attack to further narrow down the possible location area of the target SU. A higher bid price means that the SU perceives a high spectrum quality, and hence, the auctioneer can estimate the channel quality perceived by a SU from the SUs' bid price information. Since an attacker can easily have (or can reasonably be assumed to have) access to the statistics of channels' qualities in each cell, it can then compute the distance between these exact channels' qualities and those estimated from bid prices. The cell with

the minimum distance corresponds then to SU's location with high probability, as depicted in Figure 11.

Other attacks may exploit the spectrum utilization information to localize SUs as explained in Section II-D. Gao et al. [54], for example, identify an attack that infers SUs' location in database-driven CRNs by exploiting the channels' utilization information. The first component of the proposed attack arises from the fact that a SU cannot access a PU channel if the PU is present, and hence, if a SU is active in the presence of a PU, then the SU must be outside the PU's coverage area. This gives the attacker a clue that the SU is located at the complement of the PU's coverage area. If the CRN covered area is modeled as a grid, as shown in Figure 12, the adversary keeps incrementing a score, initially initialized to 0, for each cell that belongs to an available area of a specific channel. The location of the target SU will be the cell with the maximum score, which represents the area where all available areas of the channels overlap as illustrated in Figure 12. The second component of the proposed attack

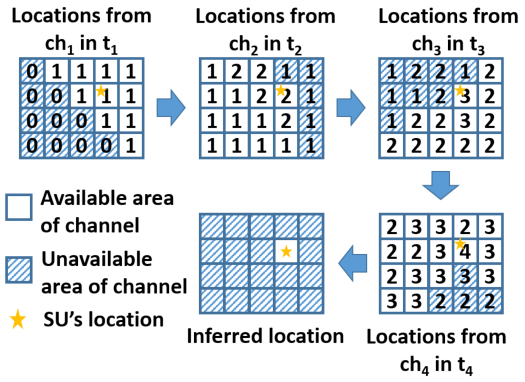


Figure 12: An example of the attack identified in [54] which uses the complement of the coverage area of each transmitting PU to gradually localize an SU by incrementing a score for each cell situated outside the coverage area of each PU. The inferred location willl be the cell with the highest score.

relies on the fact/event that a SU plans to switch from some channel chn_{k_1} to another channel chn_{k_2} when PU_{k_1} returns to its channel. In this situation there are two possible scenarios: First, when PU_{k_2} is also present and is using its channel chn_{k_2}. In this case, since SU cannot interfere with PU_{k_2}, the attacker can learn that the target SU is situated in the PU_{k_1} coverage area and the complement of PU_{k_2} coverage area. Second, when PU_{k_2} is absent. In this case, the adversary can learn that SU must be within the coverage area of PU_{k_1}, as it must have switched to chn_{k_2} after PU_{k_1}'s return. This same attack is also used by Zhang et al. [55] as a second component of their attack framework.

Physical-layer information based attacks are also possible during the spectrum sharing process. In fact, an adversary can directly extract position-related parameters like RSS, AoA, ToA, etc, from SUs' signals and exploit them to locate SUs, as explained in Section IV-A2. As an example, this kind of attacks is considered by Zhang et al. [238].

C. Location privacy preserving approaches

Few works have addressed the location privacy issue in spectrum sharing and mobility but none, to the best of our knowledge, have addressed this problem during spectrum analysis phase. These works are summarized in Table V.

1) Spectrum sharing

Some approaches try to prevent the location information leakage by hiding sensitive information exchanged during spectrum auction, e.g. location, bid channels, and bid prices, as discussed in Section II-C. Liu et al. [155] propose an approach that aims to preserve the location privacy of the SUs that participate in spectrum auction. This approach consists of two main components: The first component enables SUs to submit their encrypted locations and bid prices, while allowing the auctioneer to construct the conflict graph (explained in Section II-C1a) and determine the maximum bid price. This is done using *HMAC* [245] and the prefix membership verification scheme proposed in [246]. The second component enables the auctioneer to launch the auction using a greedy spectrum allocation algorithm to allocate the spectrum among SUs and a charging algorithm to securely determine the winning bids with the help of a trusted third party. Despite its merit in reducing the effectiveness of some of the attacks presented in Section V-B, and increasing the location privacy of SUs by hiding the bid prices and channels, this scheme suffers from some limitations. First, it relies on a trusted third party which is not always realistic. Second, it cannot achieve high location privacy without degrading the auction's performance.

Other approaches try also to prevent physical-layer based attacks during spectrum sharing, where attackers can capture the target SUs' transmitted signal when they try to access the spectrum and use it to extract position related measurements like RSS, ToA, AoA, etc, as explained in Section II-A3a. For instance, Zhang et al. [238] try to prevent attackers from measuring RSS and using it to localize SUs following some of the approaches presented in Section IV-A2. The authors propose to rely on a random power perturbation approach where SUs perturb their power transmission level to obfuscate their RSS values measured at the adversary side. This perturbation consists of reducing the transmission power to prevent an attacker from correctly estimating SUs' positions. They also provide a design of a socially-aware spectrum sharing algorithm that can operate well together with the power perturbation based privacy protection approach. The main advantage of this scheme is that it tries to address a physical-layer attack that is usually hard to prevent. However, the main shortcoming of this approach comes from the fact that the higher the privacy level, the more significant the degradation of network throughput. This means that using their scheme to preserve the location privacy of SUs would degrade system performance.

2) Spectrum mobility

Spectrum mobility necessarily involves the usage of different spectrum bands over time and as SUs move. However, as explained in Section II-D2, spectrum utilization information can become a serious source of location information leakage especially when the number of used channels increases. Gao et

TABLE V: Location privacy preserving schemes in spectrum sharing and spectrum mobility

Countermeasures	Attack Considered	Techniques	Pros	Cons
Liu et al. [155]	- Location inference from Bid channels and prices	- Prefix membership matching - HMAC	- Efficient in thwarting attacks that use bid prices - Defends to some extent against attacks that exploit bid channels	- Requires a *trusted third party* - Requires a tradeoff between location privacy and auction performance
Zhang et al. [238]	- RSS-based PHY-layer attack	- Random power perturbation	- Mitigates a PHY-layer attack which is usually hard to thwart	- High location privacy level incurs significant degradation of network throughput
Gao et al. [54]	- Location inference from spectrum utilization information	- Spectrum mobility reduction	- Low communication overhead - Reduces the localization probability of SUs	- High computational overhead - The localization probability of SUs increases with the increase of channel switches.

al. [54] propose a technique to prevent this in database-driven CRNs by relying on two observations: The first is that higher location information leakage takes place during the channel switching process; i.e., when SU switches from one channel to another. This means that if there is a way to make a SU only switch to a channel that it has already used previously, then this would not give extra information that could be exploited by the adversary. The second is that SUs that choose the most stable channels are less likely to switch channels. Based on these two observations, each SU constructs a list that stores its used channels and a prediction list that contains the prediction of the duration of channels availability. SU chooses a channel from the first list, containing the usage history, if it is available. Otherwise, SU uses the second list containing the predicted availability duration of each channel to make sure that it picks the one with the best estimated duration, i.e. the most stable. Despite its merit in reducing the localization probability of SUs, this approach does not completely thwart the attack based on SU's spectrum mobility. It just reduces the action space of the adversary which is still able to approximate SU's location when it tunes to other channels. Hence, as the number of channel switching events increases, the localization probability increases. In addition, it suffers from a relatively high computational overhead.

D. Performance metrics and tradeoffs

1) Performance metrics

Computational complexity: This is again an essential metric that needs to be used to evaluate any proposed scheme. It has already been discussed in previous sections.

Communication overhead: This is also an essential metric due to bandwidth constraints in CRNs, and has also been discussed in previous sections.

Privacy level: The approaches used here are very similar to the approaches stressed in the previous sections. For instance, Liu et al. [155] rely on the previously discussed concepts of *uncertainty* and *incorrectness* (see Section IV-A4a) to assess the privacy level of their proposed scheme. Another metric could be the *number of used channels* as it is important to minimize the frequency of SUs' switching events to avoid attacks relying on the channel utilization as explained in Section V-B. So, the number of used channels could be seen as a suitable metric to evaluate how a privacy-preserving scheme performs in preventing such attacks as done in [54].

2) Performance tradeoffs

As in the spectrum discovery phase, designing location privacy preserving protocols for spectrum analysis, sharing and mobility may require some tradeoffs between providing location privacy and maintaining some utility. For example, Zhang et al. [238] consider making tradeoffs between achieving high location privacy and maintaining high network throughput. Indeed, increasing the location privacy level using their approach, as explained in Section V-C, is equivalent to increasing the perturbation level on the transmission power of SUs to prevent the adversary from accurately localizing them. However, as the perturbation level increases, and so does the privacy level, the network throughput decreases, hindering thus the CRN performance.

E. Summary

In this section, we discussed the location privacy issues in the spectrum analysis, spectrum sharing and spectrum mobility components. We detailed the different threat models, location inference attacks, and location privacy preserving approaches that are proposed in the literature to protect the location privacy in CRNs with a focus on the aforementioned components. Finally, we explained the different performance metrics that could be used to assess the efficiency and the privacy level of location privacy preserving protocols in these components. In the following section, we will discuss some of the open research problems and challenges with respect to the location privacy in CRNs.

VI. Open research problems

There are still open research problems that could be further investigated when it comes to location privacy in CRNs. The following is a list of some of these challenges.

Location privacy in spectrum analysis: Location privacy issues arising during the spectrum analysis process have received little attention by the research community in spite of, as discussed in Section II-B, the several vulnerabilities and sources of location information leakage this process has. Much work still needs to be done when it comes to investigating inference attack models that can exploit these sources of leakage, as well as developing countermeasure solution protocols that tackle those inference attacks. For instance, an attack framework could combine information like topology, connectivity, interference and REM to localize SUs, since this information could be accessible during the spectrum analysis process as highlighted in Section II-B. To the best of our knowledge, none of the existing works have exploited these vulnerabilities, nor did they try to defend them.

Location privacy in spectrum sharing and mobility: Not many approaches in the literature have addressed the

location privacy issue in these components of the cognition cycle despite the amount of information that could be leaked during spectrum sharing and mobility as stressed in Sections II-C & II-D. This is still an open issue that requires further efforts from the research community.

Location privacy in distributed cooperative sensing: The research efforts on providing location privacy to SUs in cooperative spectrum sensing have focused on centralized approaches but little has been done to address this issue for distributed cooperative sensing. Little work has been done in this regard (e.g. [72]); this research area is still not mature enough and requires further investigation.

Location privacy with malicious adversaries: Most of the existing location privacy preserving protocols in CRNs consider attack scenarios that assume no collusion between the different network entities; for example, in the context of cooperative spectrum sensing, it is almost always assumed that there is no collusion between FC and some SUs. However, it is not unrealistic to assume that different entities can collude with one another to infer location information, especially that collusion often leads to better inference. Techniques that address colluding attackers still need to be developed and investigated, as not much has been done in this regard.

Location privacy for crowdsourced spectrum sensing: Crowdsourcing is an emerging tool that is gaining lots of interest in the context of CRNs. It enables the discovery of spectrum opportunities in regions with insufficient presence of SUs. In such cases, one can rely on other users (not necessary SUs) to assess which and whether other channels are available, mainly through an open call kind of process. To participate, these other users can be encouraged through various types of incentives (e.g., monetary, credit, etc.). In the context of CRNs, crowdsourcing suffers from location privacy risks that may expose the whereabouts of participating mobile users. Dealing with this issue is still an open problem and only a few works in the literature have dealt with it [46].

Location privacy of PUs: This is another direction that is worth investigating, as the location of PUs could be of paramount importance, especially in the case of military incumbent systems that have stringent requirements in terms of security and privacy. Also, CRN solutions that rely on the cooperation of PUs may fail or poorly perform if PUs are concerned about their location privacy. Addressing the location privacy of PUs is still in its infancy, and more still needs to be done [55], [237], [239], [247].

Location privacy in emerging CR-based technologies: Emerging CR-based technologies [248] may bring additional location privacy challenges on top of the ones that we have discussed in this paper. For instance, in cognitive radio-based cellular networks [249]–[251], multiple base stations may localize or track SUs as they move across different cells. The relatively small size of the cells in this kind of networks could make it easier to localize SUs. In CRN-enabled smart grids [252]–[254], smart meters act as SUs and opportunistically search for the available spectrum to transmit their data. The location privacy concern here is quite different as it does not involve tracking a user but can lead to identifying his own personal address if a smart meter is localized. The location information when augmented with power consumption data sent by the smart meters can further reveal the presence or absence of home owners and could lead to burglary for example. Another emerging CR-based technology is cognitive radio sensor networks ($CRSN$) [255], [256] where the sensor nodes are required to sense the environment and also the spectrum. Depending on the spectrum availability, sensor nodes, acting as SUs, transmit their readings in an opportunistic manner to their next hop cognitive radio sensor nodes, and ultimately, to the sink. As the sensor nodes exchange their sensing results of both the spectrum and the environment with other nodes, this presents considerable threats to the location privacy of these nodes and makes $CRSN$ inherit the location privacy issues of both WSNs and CRNs. All of these technologies share similar privacy threats but also have their unique vulnerabilities as well. Thus, there cannot be a one-fits-all solution to address the location privacy in these technologies, and further research efforts need to be made to investigate and address issues that are specific to each of these technologies.

Location privacy in multi-database-driven CRNs: As FCC has already approved several companies to administrate, operate and manage spectrum databases, leveraging the existence of these multiple databases (which are inherent to spectrum database-driven dynamic spectrum sharing) opens up a new class of very promising, spectrum access techniques that can guarantee the protection of users' location privacy information yet without incurring significant overhead. This area has not been explored yet, and research efforts need to be made to investigate the potential of such an approach.

VII. Conclusion

In this survey, first, we have investigated SUs' location privacy issues in CRNs by exploring each functional component and identifying its inherent vulnerabilities. Then, we have discussed when and why generic and well known privacy enhancing approaches cannot be applied off-the shelf to provide location privacy for SUs. After that we have explored existing attacks and approaches for providing location privacy solutions in the different CRN components. Finally, we have highlighted some related open research problems that require future investigation and attention.

Acknowledgment

This work was supported in part by the US National Science Foundation under NSF award CNS-1162296. The authors would like to thank the editor and the reviewers for their valuable feedback that has improved this survey paper greatly.

References

[1] J. Mitola III and G. Q. Maguire Jr, "Cognitive radio: making software radios more personal," *Personal Communications, IEEE*, vol. 6, no. 4, pp. 13–18, 1999.

[2] F. Akhtar, M. H. Rehmani, and M. Reisslein, "White space: Definitional perspectives and their role in exploiting spectrum opportunities," *Telecommunications Policy*, vol. 40, no. 4, pp. 319–331, 2016.

[3] Z. Tian and G. B. Giannakis, "A wavelet approach to wideband spectrum sensing for cognitive radios," in *Cognitive radio oriented wireless networks and communications, 2006. 1st international conference on*. IEEE, pp. 1–5.

[4] H. V. Poor, *An introduction to signal detection and estimation*. Springer Science & Business Media, 2013.

[5] M. Ghozzi, F. Marx, M. Dohler, and J. Palicot, "Cyclostatilonarilty-based test for detection of vacant frequency bands," in *Cognitive Radio Oriented Wireless Networks and Communications, 2006. 1st International Conference on*. IEEE, 2006, pp. 1–5.

[6] O. Fatemieh, A. Farhadi, R. Chandra, and C. A. Gunter, "Using classification to protect the integrity of spectrum measurements in white space networks." in *NDSS*, 2011.

[7] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: a survey," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 3, pp. 1238–1280, 2013.

[8] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*. IEEE, 2006, pp. 8–pp.

[9] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless lans," in *Proceedings of the 5th international conference on Mobile systems, applications and services*. ACM, 2007, pp. 246–257.

[10] M. Gorlatova, R. Aiello, and S. Mangold, "Managing location privacy in cellular networks with femtocell deployments," in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2011 International Symposium on*. IEEE, 2011, pp. 418–422.

[11] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen, "Location privacy preservation in collaborative spectrum sensing," in *INFOCOM, 2012 Proceedings IEEE*, pp. 729–737.

[12] M. Madden and L. Rainie, "Americans' attitudes about privacy, security, and surveillance," http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf.

[13] A. Araujo, J. Blesa, E. Romero, and D. Villanueva, "Security in cognitive wireless sensor networks. challenges and open problems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, p. 48, 2012.

[14] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE communications surveys and tutorials*, vol. 15, no. 1, pp. 428–445, 2013.

[15] M. H. Ling, K.-L. A. Yau, J. Qadir, G. S. Poh, and Q. Ni, "Application of reinforcement learning for security enhancement in cognitive radio networks," *Applied Soft Computing*, vol. 37, pp. 809–829, 2015.

[16] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks," *Journal of Internet Technology*, vol. 12, no. 2, pp. 181–198, 2011.

[17] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

[18] X. Zhang and H. Y. Bae, "Location positioning and privacy preservation methods in location-based service," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 41–52, 2015.

[19] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *Selected Areas in Communications, IEEE Journal on*, vol. 23, no. 2, pp. 201–220, 2005.

[20] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury, "Crahns: Cognitive radio ad hoc networks," *AD hoc networks*, vol. 7, no. 5, pp. 810–836, 2009.

[21] E. Hossain, D. Niyato, and Z. Han, *Dynamic spectrum access and management in cognitive radio networks*. Cambridge university press, 2009.

[22] T. Yücek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *Communications Surveys & Tutorials, IEEE*, vol. 11, no. 1, pp. 116–130, 2009.

[23] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: requirements, challenges and design trade-offs," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 32–39, 2008.

[24] E. Axell, G. Leus, E. G. Larsson, and H. V. Poor, "Spectrum sensing for cognitive radio: State-of-the-art and recent advances," *Signal Processing Magazine, IEEE*, vol. 29, no. 3, pp. 101–116, 2012.

[25] K. B. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 878–893, 2009.

[26] N. Hoven, R. Tandra, and A. Sahai, "Some fundamental limits on cognitive radio," *Wireless Foundations EECS, Univ. of California, Berkeley*, 2005.

[27] J. Ma, G. Y. Li, and B. H. F. Juang, "Signal processing in cognitive radio," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 805–823, 2009.

[28] J. G. Proakis, *Intersymbol interference in digital communication systems*. Wiley Online Library, 2003.

[29] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Signals, systems and computers, 2004. Conference record of the thirty-eighth Asilomar conference on*, vol. 1. IEEE, 2004, pp. 772–776.

[30] J. Lundén, V. Koivunen, A. Huttunen, and H. V. Poor, "Collaborative cyclostationary spectrum sensing for cognitive radio systems," *IEEE Transactions on Signal Processing*, vol. 57, no. 11, pp. 4182–4195, 2009.

[31] F. Salahdine, N. Kaabouch, and H. El Ghazi, "A survey on compressive sensing techniques for cognitive radio networks," *Physical Communication*, vol. 20, pp. 61–73, 2016.

[32] D. L. Donoho, "Compressed sensing," *IEEE Transactions on information theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[33] S. K. Sharma, E. Lagunas, S. Chatzinotas, and B. Ottersten, "Application of compressive sensing in cognitive radio communications: A survey," *IEEE Commun. Surveys and Tutorials*, no. 99, pp. 1–24, 2016.

[34] P. Cheng, R. Deng, and J. Chen, "Energy-efficient cooperative spectrum sensing in sensor-aided cognitive radio networks," *Wireless Communications, IEEE*, vol. 19, no. 6, pp. 100–105, 2012.

[35] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, pp. 137–143.

[36] ——, "Cooperative spectrum sensing in cognitive radio, part i: Two user networks," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 6, pp. 2204–2213, 2007.

[37] S. Althunibat, M. Di Renzo, and F. Granelli, "Optimizing the k-out-of-n rule for cooperative spectrum sensing in cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2013 IEEE*, pp. 1607–1611.

[38] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh, "White space networking with wi-fi like connectivity," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 4, pp. 27–38, 2009.

[39] *IEEE 802.22 Working Group on Wireless Regional Area Networks: Enabling Broadband Wireless Access Using Cognitive Radio Technology and Spectrum Sharing in White Spaces*, IEEE Std. [Online]. Available: http://www.ieee802.org/22/

[40] *IEEE 802.11af Draft 5.0, Amendment 5: TV White Spaces Operation*, IEEE 802.11 Working Group Std., June 2013.

[41] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical communication*, vol. 4, no. 1, pp. 40–62, 2011.

[42] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Preserving the location privacy of secondary users in cooperative spectrum sensing," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 418–431, 2017.

[43] O. Fatemieh, R. Chandra, and C. A. Gunter, "Secure collaborative sensing for crowd sourcing spectrum data in white space networks," in *New Frontiers in Dynamic Spectrum, IEEE Symposium on*, 2010, pp. 1–12.

[44] R. Zhang, J. Zhang, Y. Zhang, and C. Zhang, "Secure crowdsourcing-based cooperative spectrum sensing," in *INFOCOM, 2013 Proceedings IEEE*, pp. 2526–2534.

[45] Z. Feng, Y. Zhu, Q. Zhang, L. M. Ni, and A. V. Vasilakos, "Trac: Truthful auction for location-aware collaborative sensing in mobile crowdsourcing," in *INFOCOM, 2014 Proceedings IEEE*, pp. 1231–1239.

[46] X. Jin and Y. Zhang, "Privacy-preserving crowdsourced spectrum sensing," in *Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on*, pp. 1–9.

[47] J. Sun, R. Zhang, X. Jin, and Y. Zhang, "Securefind: Secure and privacy-preserving object finding via mobile crowdsourcing," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1716–1728, 2016.

[48] *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper*, Cisco Std., February 2016. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

[49] A. Nika, Z. Zhang, X. Zhou, B. Y. Zhao, and H. Zheng, "Towards commoditized real-time spectrum monitoring," in *Proceedings of the 1st ACM Workshop on Hot Topics in Wireless*. ACM, 2014, pp. 25–30.

[50] D. Teguig, B. Scheers, and V. L. Nir, "Data fusion schemes for cooperative spectrum sensing in cognitive radio networks," in *Communications and Information Systems Conference (MCC), 2012 Military*. IEEE, pp. 1–7.

[51] F. C. Commission *et al.*, "Third memorandum opinion and order," *FCC 12*, vol. 36, 2012.

[52] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl, "Senseless: A database-driven white spaces network," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 2, pp. 189–203, 2012.

[53] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Cuckoo filter-based location-privacy preservation in database-driven cognitive radio networks," in *Computer Networks and Information Security (WSCNIS), 2015 World Symposium on*. IEEE, 2015, pp. 1–7.

[54] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *INFOCOM, 2013 Proceedings IEEE*, pp. 2751–2759.

[55] L. Zhang, C. Fang, Y. Li, H. Zhu, and M. Dong, "Optimal strategies for defending location inference attack in database-driven crns," in *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 7640–7645.

[56] R. Zekavat and R. M. Buehrer, *Handbook of position location: Theory, practice and advances*. John Wiley & Sons, 2011, vol. 27.

[57] K. Sithamparanathan and A. Giorgetti, *Cognitive radio techniques: spectrum sensing, interference mitigation, and localization*. Artech house, 2012.

[58] M. Vossiek, L. Wiebking, P. Gulden, J. Weighardt, and C. Hoffmann, "Wireless local positioning-concepts, solutions, applications," in *Radio and Wireless Conference, 2003. RAWCON'03. Proceedings*. IEEE, pp. 219–224.

[59] J. Bachrach and C. Taylor, "Localization in sensor networks," *Handbook of sensor networks: Algorithms and Architectures*, vol. 1, 2005.

[60] K. Whitehouse, C. Karlof, and D. Culler, "A practical evaluation of radio signal strength for ranging-based localization," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 11, no. 1, 2007.

[61] R. Peng and M. L. Sichitiu, "Angle of arrival localization for wireless sensor networks," in *Sensor and Ad Hoc Communications and Networks, 2006. SECON'06. 2006 3rd Annual IEEE Communications Society on*, vol. 1, pp. 374–382.

[62] A. Boukerche, H. A. Oliveira, E. F. Nakamura, and A. A. Loureiro, "Localization systems for wireless sensor networks," *wireless Communications, IEEE*, vol. 14, no. 6, pp. 6–12, 2007.

[63] K. R. Chowdhury and M. D. Felice, "Search: A routing protocol for mobile cognitive radio ad-hoc networks," *Computer Communications*, vol. 32, no. 18, pp. 1983–1997, 2009.

[64] M. Youssef, M. Ibrahim, M. Abdelatif, L. Chen, and A. V. Vasilakos, "Routing metrics of cognitive radio networks: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 1, pp. 92–109, 2014.

[65] D. Niculescu and B. Nath, "Ad hoc positioning system (aps)," in *Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE*, vol. 5, pp. 2926–2931.

[66] C. S. J. Rabaey and K. Langendoen, "Robust positioning algorithms for distributed ad-hoc wireless sensor networks," in *USENIX technical annual conference*, 2002, pp. 317–327.

[67] K.-L. A. Yau, N. Ramli, W. Hashim, and H. Mohamad, "Clustering algorithms for cognitive radio networks: A survey," *Journal of Network and Computer Applications*, vol. 45, pp. 79–95, 2014.

[68] H. Chan, M. Luk, and A. Perrig, "Using clustering information for sensor network localization," in *Distributed Computing in Sensor Systems*. Springer, 2005, pp. 109–125.

[69] A. Youssef, M. Younis, M. Youssef, and A. Agrawala, "Wsn16-5: Distributed formation of overlapping multi-hop clusters in wireless sensor networks," in *Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE*, pp. 1–6.

[70] X. Hao, M. H. Cheung, V. W. Wong, and V. Leung, "A coalition formation game for energy-efficient cooperative spectrum sensing in cognitive radio networks with multiple channels," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pp. 1–6.

[71] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, and T. Başar, "Coalitional games for distributed collaborative spectrum sensing in cognitive radio networks," in *INFOCOM 2009, IEEE*, pp. 2114–2122.

[72] B. Kasiri, I. Lambadaris, F. R. Yu, and H. Tang, "Privacy-preserving distributed cooperative spectrum sensing in multi-channel cognitive radio manets," in *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 7316–7321.

[73] A. C. Malady and C. R. da Silva, "Clustering methods for distributed spectrum sensing in cognitive radio systems," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pp. 1–5.

[74] G. Ding, Q. Wu, F. Song, and J. Wang, "Decentralized sensor selection for cooperative spectrum sensing based on unsupervised learning," in *Communications (ICC), 2012 IEEE International Conference on*, pp. 1576–1580.

[75] M. T. Masonta, M. Mzyece, and N. Ntlatlapa, "Spectrum decision in cognitive radio networks: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 3, pp. 1088–1107, 2013.

[76] A. Rabbachin, T. Q. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 2, pp. 480–493, 2011.

[77] T. S. Rappaport *et al.*, *Wireless communications: principles and practice*. Prentice Hall PTR New Jersey, 1996, vol. 2.

[78] G. Mao, B. D. Anderson, and B. Fidan, "Path loss exponent estimation for wireless sensor network localization," *Computer Networks*, vol. 51, no. 10, pp. 2467–2483, 2007.

[79] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. S. Sukhatme, "Robomote: enabling mobility in sensor networks," in *Proceedings of the 4th international symposium on Information processing in sensor networks*. IEEE Press, 2005, p. 55.

[80] Y. Chen and H.-S. Oh, "A survey of measurement-based spectrum occupancy modeling for cognitive radios," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 848–859, 2016.

[81] Y. Saleem and M. H. Rehmani, "Primary radio user activity models for cognitive radio networks: A survey," *Elsevier Journal of Network and Computer Applications*, vol. 43, pp. 1–16, 2014.

[82] M. Höyhtyä, A. Mämmelä, M. Eskola, M. Matinmikko, J. Kalliovaara, J. Ojaniemi, J. Suutala, R. Ekman, R. Bacchus, and D. Roberson, "Spectrum occupancy measurements: A survey and use of interference maps," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2386–2414, 2016.

[83] W.-Y. Lee and I. F. Akyldiz, "A spectrum decision framework for cognitive radio networks," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 2, pp. 161–174, 2011.

[84] Y. Zhao, J. H. Reed, S. Mao, and K. K. Bae, "Overhead analysis for radio environment mapenabled cognitive radio networks," in *Networking Technologies for Software Defined Radio Networks, 2006. SDR'06.1 st IEEE Workshop on*, 2006, pp. 18–25.

[85] Y. Zhao, B. Le, and J. H. Reed, "Network support–the radio environment map," *Cognitive radio technology*, pp. 325–366, 2006.

[86] H. B. Yilmaz, T. Tugcu, F. Alagöz, and S. Bayhan, "Radio environment map as enabler for practical cognitive radio networks," *Communications Magazine, IEEE*, vol. 51, no. 12, pp. 162–169, 2013.

[87] E. Z. Tragos, S. Zeadally, A. G. Fragkiadakis, and V. A. Siris, "Spectrum assignment in cognitive radio networks: A comprehensive survey," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 3, pp. 1108–1135, 2013.

[88] N. Hoven and A. Sahai, "Power scaling for cognitive radio," in *Wireless networks, communications and mobile computing, 2005 International Conference on*, vol. 1. IEEE, 2005, pp. 250–255.

[89] M. H. Islam, Y.-c. Liang, and A. T. Hoang, "Joint power control and beamforming for cognitive radio networks," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 7, pp. 2415–2419, 2008.

[90] M. B. Ghorbel, B. Khalfi, B. Hamdaoui, and M. Guizani, "Power allocation analysis for dynamic power utility in cognitive radio systems," in *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 3732–3737.

[91] N. Chakchouk and B. Hamdaoui, "Traffic and interference aware scheduling for multiradio multichannel wireless mesh networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 555–565, 2011.

[92] A. T. Hoang and Y.-C. Liang, "Maximizing spectrum utilization of cognitive radio networks using channel allocation and power control," in *Vehicular Technology Conference, 2006. VTC-2006 Fall. 2006 IEEE 64th*, pp. 1–5.

[93] C.-G. Yang, J.-D. Li, and Z. Tian, "Optimal power control for cognitive radio networks under coupled interference constraints: A cooperative game-theoretic perspective," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 4, pp. 1696–1706, 2010.

[94] L. Qian, X. Li, J. Attia, and Z. Gajic, "Power control for cognitive radio ad hoc networks," in *Local & Metropolitan Area Networks, 2007. LANMAN 2007. 15th IEEE Workshop on*, pp. 7–12.

[95] D. Jiang, Y. Wang, C. Yao, and Y. Han, "An effective dynamic spectrum access algorithm for multi-hop cognitive wireless networks," *Computer Networks*, vol. 84, pp. 1–16, 2015.

[96] N. Nie, C. Comaniciu, and P. Agrawal, "A game theoretic approach to interference management in cognitive networks," in *Wireless Communications*. Springer, 2007, pp. 199–219.

[97] B. Hamdaoui, "Adaptive spectrum assessment for opportunistic access in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 922–930, 2009.

[98] C. Peng, H. Zheng, and B. Y. Zhao, "Utilization and fairness in spectrum assignment for opportunistic spectrum access," *Mobile Networks and Applications*, vol. 11, no. 4, pp. 555–576, 2006.

[99] B. Khalfi, M. B. Ghorbel, B. Hamdaoui, and M. Guizani, "Dynamic power pricing using distributed resource allocation for large-scale dsa systems," in *Wireless Communications and Networking Conference (WCNC), 2015 IEEE*. IEEE, 2015, pp. 1090–1094.

[100] M. B. Ghorbel, B. Khalfi, B. Hamdaoui, and M. Guizani, "Resources allocation for large-scale dynamic spectrum access system using particle filtering," in *Globecom Workshops (GC Wkshps), 2014*. IEEE, 2014, pp. 219–224.

[101] B. Khalfi, M. B. Ghorbel, B. Hamdaoui, and M. Guizani, "Distributed fair spectrum assignment for large-scale wireless dsa networks," in *International Conference on Cognitive Radio Oriented Wireless Networks*. Springer, 2015, pp. 631–642.

[102] S. Ehsan, B. Hamdaoui, and M. Guizani, "Radio and medium access contention aware routing for lifetime maximization in multichannel sensor networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3058–3067, 2012.

[103] R. Hamdi, M. B. Ghorbel, B. Hamdaoui, M. Guizani, and B. Khalfi, "Implementation and analysis of reward functions under different traffic models for distributed dsa systems," *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5147–5155, 2015.

[104] N. Nie and C. Comaniciu, "Adaptive channel allocation spectrum etiquette for cognitive radio networks," *Mobile networks and applications*, vol. 11, no. 6, pp. 779–797, 2006.

[105] M. Bkassiny, Y. Li, and S. K. Jayaweera, "A survey on machine-learning techniques in cognitive radios," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 3, pp. 1136–1159, 2013.

[106] O. Alsaleh, P. Venkatraman, B. Hamdaoui, and A. Fern, "Enabling opportunistic and dynamic spectrum access through learning techniques," *Wireless Communications and Mobile Computing*, vol. 11, no. 12, pp. 1497–1506, 2011.

[107] L. T. Tan and L. B. Le, "Channel assignment with access contention resolution for cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2808–2823, 2012.

[108] V. Teotia, V. Kumar, and S. Minz, "Conflict graph based channel allocation in cognitive radio networks," in *Reliable Distributed Systems Workshop (SRDSW), 2015 IEEE 34th Symposium on*, pp. 52–56.

[109] L. Yang, X. Xie, and X. Y. Zheng, "A historical-information-based algorithm in dynamic spectrum allocation," in *Communication Software and Networks, 2009. ICCSN'09. International Conference on*. IEEE, pp. 731–736.

[110] N. B. Priyantha, H. Balakrishnan, E. Demaine, and S. Teller, "Anchor-free distributed localization in sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems*. ACM, 2003, pp. 340–341.

[111] H. Wymeersch, J. Lien, and M. Z. Win, "Cooperative localization in wireless networks," *Proceedings of the IEEE*, vol. 97, no. 2, 2009.

[112] Y. Shang, W. Ruml, Y. Zhang, and M. P. Fromherz, "Localization from mere connectivity," in *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, 2003.

[113] Y. Shang, W. Rumi, Y. Zhang, and M. Fromherz, "Localization from connectivity in sensor networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 15, no. 11, pp. 961–974, 2004.

[114] S. Lederer, Y. Wang, and J. Gao, "Connectivity-based localization of large-scale sensor networks with complex shape," *ACM Transactions on Sensor Networks (TOSN)*, vol. 5, no. 4, p. 31, 2009.

[115] Y. Wang, S. Lederer, and J. Gao, "Connectivity-based sensor network localization with incremental delaunay refinement method," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 2401–2409.

[116] B. Wang, Y. Wu, and K. R. Liu, "Game theory for cognitive radio networks: An overview," *Computer networks*, vol. 54, no. 14, 2010.

[117] Y. Huang, J. Wang, and H. Jiang, "Modeling of learning inference and decision-making engine in cognitive radio," in *Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on*, vol. 2. IEEE, pp. 258–261.

[118] B. Bahrak and J.-M. Park, "Security of spectrum learning in cognitive radios," *arXiv preprint arXiv:1304.0606*, 2013.

[119] M. NoroozOliaee, B. Hamdaoui, and K. Tumer, "Efficient objective functions for coordinated learning in large-scale distributed osa systems," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 931–944, 2013.

[120] C. Clancy, J. Hecker, E. Stuntebeck, and T. O. Shea, "Applications of machine learning to cognitive radio networks," *Wireless Communications, IEEE*, vol. 14, no. 4, pp. 47–52, 2007.

[121] M. J. N. Oliaee, B. Hamdaoui, and M. Guizani, "Adaptive service function for system reward maximization under elastic traffic model," in *Globecom Workshops (GC Wkshps), 2013 IEEE*. IEEE, 2013, pp. 4781–4785.

[122] N. Baldo, B. R. Tamma, B. Manoj, R. Rao, and M. Zorzi, "A neural network based cognitive controller for dynamic channel selection," in *Communications, 2009. ICC'09. IEEE International Conference on*, pp. 1–5.

[123] H. Li, "Multi-agent q-learning of channel selection in multi-user cognitive radio systems: A two by two case," in *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on*, pp. 1893–1898.

[124] M. NoroozOliaee, B. Hamdaoui, and K. Tumer, "Achieving optimal elastic traffic rewards in dynamic multichannel access," in *High Performance Computing and Simulation (HPCS), 2011 International Conference on*. IEEE, 2011, pp. 155–161.

[125] B. Hamdaoui, M. NoroozOliaee, K. Tumer, and A. Rayes, "Coordinating secondary-user behaviors for inelastic traffic reward maximization in large-scale\ osa networks," *IEEE Transactions on Network and Service Management*, vol. 9, no. 4, pp. 501–513, 2012.

[126] ——, "Aligning spectrum-user objectives for maximum inelastic-traffic reward," in *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*. IEEE, 2011, pp. 1–6.

[127] M. NoroozOliaee, B. Hamdaoui, and M. Guizani, "Maximizing secondary-user satisfaction in large-scale dsa systems through distributed team cooperation," *IEEE Transactions on Wireless Communications*, vol. 11, no. 10, pp. 3588–3597, 2012.

[128] M. NoroozOliaee and B. Hamdaoui, "Distributed resource and service management for large-scale dynamic spectrum access systems through coordinated learning," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*. IEEE, 2011, pp. 522–527.

[129] K.-L. A. Yau, P. Komisarczuk, and P. D. Teal, "A context-aware and intelligent dynamic channel selection scheme for cognitive radio networks," in *Cognitive Radio Oriented Wireless Networks and Communications, 2009. CROWNCOM'09. 4th International Conference on*. IEEE, pp. 1–6.

[130] L. Akter, B. Natarajan, and C. Scoglio, "Modeling and forecasting secondary user activity in cognitive radio networks," in *2008 Proceedings of 17th International Conference on Computer Communications and Networks*. IEEE, 2008, pp. 1–6.

[131] X. Xing, T. Jing, W. Cheng, Y. Huo, and X. Cheng, "Spectrum prediction in cognitive radio networks," *IEEE Wireless Communications*, vol. 20, no. 2, pp. 90–96, 2013.

[132] M. Bkassiny and S. K. Jayaweera, "Optimal channel and power allocation for secondary users in cooperative cognitive radio networks," in *International Conference on Mobile Lightweight Wireless Systems*. Springer, 2010, pp. 180–191.

[133] H. W. Kuhn, "The hungarian method for the assignment problem," *Naval research logistics quarterly*, vol. 2, no. 1-2, pp. 83–97, 1955.

[134] L. Ding, T. Melodia, S. N. Batalama, and J. D. Matyjas, "Distributed routing, relay selection, and spectrum allocation in cognitive and cooperative ad hoc networks," in *Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on*, pp. 1–9.

[135] M. B. Ghorbel, B. Hamdaoui, M. Guizani, and B. Khalfi, "Distributed learning-based cross-layer technique for energy-efficient multicarrier dynamic spectrum access with adaptive power allocation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1665–1674, 2016.

[136] M. B. Ghorbel, B. Hamdaoui, R. Hamdi, M. Guizani, and M. NoroozOliaee, "Distributed dynamic spectrum access with adaptive power allocation: Energy efficiency and cross-layer awareness," in *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on*. IEEE, 2014, pp. 694–699.

[137] H. A. B. Salameh, "Throughput-oriented channel assignment for opportunistic spectrum access networks," *Mathematical and Computer Modelling*, vol. 53, no. 11, pp. 2108–2118, 2011.

[138] Q. Xin and J. Xiang, "Joint qos-aware admission control, channel assignment, and power allocation for cognitive radio cellular networks," in *Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on*, pp. 294–303.

[139] H. B. Salameh, M. Krunz, and O. Younis, "Distance-and traffic-aware channel assignment in cognitive radio networks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON'08. 5th Annual IEEE Communications Society Conference on*, pp. 10–18.

[140] L. Zhang, Y.-C. Liang, and Y. Xin, "Joint beamforming and power allocation for multiple access channels in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, 2008.

[141] L. B. Le and E. Hossain, "Resource allocation for spectrum underlay in cognitive radio networks," *IEEE Transactions on Wireless communications*, vol. 7, no. 12, pp. 5306–5315, 2008.

[142] D. I. Kim, L. B. Le, and E. Hossain, "Joint rate and power allocation for cognitive radios in dynamic spectrum access environment," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, 2008.

[143] G. Zheng, K.-K. Wong, and B. Ottersten, "Robust cognitive beamforming with bounded channel uncertainties," *IEEE Transactions on Signal Processing*, vol. 57, no. 12, pp. 4871–4881, 2009.

[144] A. De Domenico, E. C. Strinati, and M.-G. Di Benedetto, "A survey on mac strategies for cognitive radio networks," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 1, pp. 21–44, 2012.

[145] A. Goldsmith, S. A. Jafar, I. Marić, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, 2009.

[146] S. Srinivasa and S. A. Jafar, "Cognitive radios for dynamic spectrum access-the throughput potential of cognitive radio: A theoretical perspective," *Communications Magazine, IEEE*, vol. 45, no. 5, 2007.

[147] Y. R. Kondareddy and P. Agrawal, "Synchronized mac protocol for multi-hop cognitive radio networks," in *Communications, 2008. ICC'08. IEEE International Conference on*, pp. 3198–3202.

[148] B. Hamdaoui and K. G. Shin, "OS-MAC: An efficient MAC protocol for spectrum-agile wireless networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 8, pp. 915–930, 2008.

[149] L. Ma, X. Han, and C.-C. Shen, "Dynamic open spectrum sharing mac protocol for wireless ad hoc networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, pp. 203–213.

[150] J. Jia, Q. Zhang, and X. Shen, "Hc-mac: A hardware-constrained cognitive mac for efficient spectrum management," *Selected Areas in Communications, IEEE Journal on*, vol. 26, no. 1, pp. 106–117, 2008.

[151] H. B. Salameh, M. Krunz, and O. Younis, "Mac protocol for opportunistic cognitive radio networks with soft guarantees," *IEEE transactions on mobile computing*, vol. 8, no. 10, pp. 1339–1352, 2009.

[152] J. Zhao, H. Zheng, and G.-H. Yang, "Distributed coordination in dynamic spectrum allocation networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, pp. 259–268.

[153] S. Maharjan, Y. Zhang, and S. Gjessing, "Economic approaches for cognitive radio networks: A survey," *Wireless Personal Communications*, vol. 57, no. 1, pp. 33–51, 2011.

[154] D. Niyato and E. Hossain, "Spectrum trading in cognitive radio networks: A market-equilibrium-based approach," *Wireless Communications, IEEE*, vol. 15, no. 6, pp. 71–80, 2008.

[155] S. Liu, H. Zhu, R. Du, C. Chen, and X. Guan, "Location privacy preserving dynamic spectrum auction in cognitive radio network," in *Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on*, pp. 256–265.

[156] M. Khaledi and A. A. Abouzeid, "Auction-based spectrum sharing in cognitive radio networks with heterogeneous channels," in *Information Theory and Applications Workshop (ITA), 2013*, 2013, pp. 1–8.

[157] X. Wang, Z. Li, P. Xu, Y. Xu, X. Gao, and H.-H. Chen, "Spectrum sharing in cognitive radio networks—an auction-based approach," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 40, no. 3, pp. 587–596, 2010.

[158] G. S. Kasbekar and S. Sarkar, "Spectrum auction framework for access allocation in cognitive radio networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 18, no. 6, pp. 1841–1854, 2010.

[159] N. H. Tran, L. B. Le, S. Ren, Z. Han, and C. S. Hong, "Joint pricing and load balancing for cognitive spectrum access: Non-cooperation versus cooperation," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 5, pp. 972–985, 2015.

[160] C. T. Do, N. H. Tran, Z. Han, L. B. Le, S. Lee, and C. S. Hong, "Optimal pricing for duopoly in cognitive radio networks: Cooperate or not cooperate?" *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2574–2587, 2014.

[161] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury, "Spectrum management in cognitive radio ad hoc networks," *Network, IEEE*, vol. 23, no. 4, pp. 6–12, 2009.

[162] W. Chengyu, H. Chen, and J. Lingge, "Spectrum handoff scheme based on recommended channel sensing sequence," *Communications, China*, vol. 10, no. 8, pp. 18–26, 2013.

[163] W.-Y. Lee and I. F. Akyildiz, "Spectrum-aware mobility management in cognitive radio cellular networks," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 4, pp. 529–542, 2012.

[164] I. Christian, S. Moh, I. Chung, and J. Lee, "Spectrum mobility in cognitive radio networks," *Communications Magazine, IEEE*, vol. 50, no. 6, pp. 114–121, 2012.

[165] K. Kumar, A. Prakash, and R. Tripathi, "Spectrum handoff in cognitive radio networks: A classification and comprehensive survey," *Journal of Network and Computer Applications*, vol. 61, pp. 161–188, 2016.

[166] L.-C. Wang, C.-W. Wang, and C.-J. Chang, "Modeling and analysis for spectrum handoffs in cognitive radio networks," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 9, pp. 1499–1513, 2012.

[167] W. Hu, D. Willkomm, M. Abusubaih, J. Gross, G. Vlantis, M. Gerla, and A. Wolisz, "Cognitive radios for dynamic spectrum access-dynamic frequency hopping communities for efficient ieee 802.22 operation," *Communications Magazine, IEEE*, vol. 45, no. 5, pp. 80–87, 2007.

[168] L.-C. Wang and C.-W. Wang, "Spectrum handoff for cognitive radio networks: Reactive-sensing or proactive-sensins?" in *Performance, Computing and Communications Conference, 2008. IPCCC 2008. IEEE International*, pp. 343–348.

[169] D. Willkomm, J. Gross, and A. Wolisz, "Reliable link maintenance in cognitive radio systems," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pp. 371–378.

[170] C.-W. Wang, L.-C. Wang, and F. Adachi, "Modeling and analysis for reactive-decision spectrum handoff in cognitive radio networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1–6.

[171] Y. Song and J. Xie, "Prospect: A proactive spectrum handoff framework for cognitive radio ad hoc networks without common control channel," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 7, 2012.

[172] S. Nejatian, S. K. Syed-Yusof, N. M. A. Latiff, V. Asadpour, and H. Hosseini, "Proactive integrated handoff management in cognitive radio mobile ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 1–19, 2013.

[173] Y.-C. Wei and Y.-M. Chen, "Safe distance based location privacy in vehicular networks," in *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*. IEEE, 2010, pp. 1–5.

[174] L. Tang, X. Hong, and P. G. Bradford, "Privacy-preserving secure relative localization in vehicular networks," *Security and Communication Networks*, vol. 1, no. 3, pp. 195–204, 2008.

[175] A. Görlach, A. Heinemann, and W. W. Terpstra, "Survey on location privacy in pervasive computing," in *Privacy, Security and Trust within the Context of Pervasive Computing*. Springer, 2005, pp. 23–34.

[176] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE, 2007, pp. 1955–1963.

[177] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2004, pp. 88–93.

[178] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*. IEEE, 2005, pp. 113–126.

[179] E. C.-H. Ngai and I. Rodhe, "On providing location privacy for mobile sinks in wireless sensor networks," *Wireless networks*, vol. 19, no. 1, pp. 115–130, 2013.

[180] E. Troja and S. Bakiras, "Leveraging p2p interactions for efficient location privacy in database-driven dynamic spectrum access," in *Proceedings of the 22nd ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*. ACM, 2014.

[181] ——, "Efficient location privacy for moving clients in database-driven dynamic spectrum access," in *Computer Communication and Networks (ICCCN), 2015 24th International Conference on*. IEEE, 2015, pp. 1–8.

[182] H. Li, Q. Pei, and W. Zhang, "Location privacy-preserving channel allocation scheme in cognitive radio networks," *International Journal of Distributed Sensor Networks*, vol. 12, no. 7, p. 3794582, 2016.

[183] Q. Huang, Y. Gui, F. Wu, G. Chen, and Q. Zhang, "A general privacy-preserving auction mechanism for secondary spectrum markets," 2015.

[184] R. Reddy, T. Kiernan, and A. Mody, "Method for ensuring security and privacy in a wireless cognitive network," Nov. 25 2014, uS Patent 8,898,468. [Online]. Available: https://www.google.com/patents/US8898468

[185] K. Zeng, S. Kondaji Ramesh, and Y. Yang, "Location spoofing attack and its countermeasures in database-driven cognitive radio networks," in *Communications and Network Security (CNS), 2014 IEEE Conference on*. IEEE, 2014, pp. 202–210.

[186] F. Hahn and F. Kerschbaum, "Searchable encryption with secure and efficient updates," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 310–320.

[187] A. A. Yavuz and J. Guajardo, "Dynamic searchable symmetric encryption with minimal leakage and efficient updates on commodity hardware," in *Selected Areas in Cryptography – SAC 2015*, ser. Lecture Notes in Computer Science. Springer International Publishing, August 2015.

[188] B. Wang, S. Yu, W. Lou, and Y. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in *INFOCOM, 2014 Proceedings IEEE*, April 2014, pp. 2112–2120.

[189] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawcyk, M.-C. Rosu, and M. Steiner, "Dynamic searchable encryption in very-large databases: Data structures and implementation," in *21th Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014*. The Internet Society.

[190] M. Naveed, M. Prabhakaran, and C. A. Gunter, "Dynamic searchable encryption via blind storage," in *35th IEEE Symposium on Security and Privacy*, May 2014, pp. 48–62.

[191] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," *J. ACM*, vol. 43, no. 3, pp. 431–473, 1996.

[192] E. Stefanov, E. Shi, and D. X. Song, "Towards practical oblivious RAM," in *19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012*, 2012. [Online]. Available: http://www.internetsociety.org/towards-practical-oblivious-ram

[193] B. Pinkas and T. Reinman, "Oblivious ram revisited," in *Proceedings of the 30th Annual Conference on Advances in Cryptology*, ser. CRYPTO'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 502–519.

[194] J. Cheon and D. Stehlé, "Fully homomophic encryption over the integers revisited," in *Advances in Cryptology – EUROCRYPT 2015*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2015, vol. 9056, pp. 513–536.

[195] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques*, ser. EUROCRYPT'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 24–43.

[196] N. P. Smart and F. Vercauteren, "Fully homomorphic simd operations," *Des. Codes Cryptography*, vol. 71, no. 1, pp. 57–81, 2014.

[197] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in *Theory of Cryptography*, ser. Lecture Notes in Computer Science, O. Reingold, Ed. Springer Berlin Heidelberg, 2009, vol. 5444, pp. 457–473.

[198] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters, "Candidate indistinguishability obfuscation and functional encryption for all circuits," in *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, Oct 2013, pp. 40–49.

[199] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proceedings of the 13th ACM conference on Computer and communications security*, ser. CCS '06. New York, NY, USA: ACM, 2006, pp. 79–88.

[200] P. Samarati, "Protecting respondents identities in microdata release," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 13, no. 6, pp. 1010–1027, 2001.

[201] A. Khoshgozaran and C. Shahabi, "Private information retrieval techniques for enabling location privacy in location-based services," in *Privacy in Location-Based Applications*. Springer, 2009, pp. 59–83.

[202] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *Journal of the ACM (JACM)*, vol. 45, no. 6, 1998.

[203] S. Wang, D. Agrawal, and A. El Abbadi, "Generalizing pir for practical private retrieval of public data," in *Data and Applications Security and Privacy XXIV*. Springer, 2010, pp. 1–16.

[204] S. T. Peddinti and N. Saxena, "On the limitations of query obfuscation techniques for location privacy," in *Proceedings of the 13th international conference on Ubiquitous computing*. ACM, 2011, pp. 187–196.

[205] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, pp. 121–132.

[206] C. Gentry *et al.*, "Fully homomorphic encryption using ideal lattices." in *STOC*, vol. 9, 2009, pp. 169–178.

[207] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in cryptology—EUROCRYPT'99*. Springer, 1999, pp. 223–238.

[208] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[209] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[210] M. O. Rabin, "How to exchange secrets with oblivious transfer." *IACR Cryptology ePrint Archive*, p. 187, 2005.

[211] C. Cachin, S. Micali, and M. Stadler, "Computationally private information retrieval with polylogarithmic communication," in *Advances in Cryptology—EUROCRYPT'99*. Springer, 1999, pp. 402–414.

[212] A. Ambainis, "Upper bound on the communication complexity of private information retrieval," in *Automata, Languages and Programming*. Springer, 1997, pp. 401–407.

[213] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[214] C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," in *Automata, Languages and Programming*. Springer, 2005, pp. 803–815.

[215] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 79–88.

[216] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," *Journal of the ACM (JACM)*, vol. 43, no. 3, pp. 431–473, 1996.

[217] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of cryptography*. Springer, 2006, pp. 265–284.

[218] A. Groce, J. Katz, and A. Yerukhimovich, "Limits of computational differential privacy in the client/server setting," in *Theory of Cryptography*. Springer, 2011, pp. 417–431.

[219] C. Dwork, "Differential privacy," in *Automata, languages and programming*. Springer, 2006, pp. 1–12.

[220] V. Rastogi and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in *Proceedings of the 2010 ACM SIGMOD International Conference on Management of data*, pp. 735–746.

[221] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 901–914.

[222] A. Yao, "How to generate and exchange secrets," in *Foundations of Computer Science, 1986., 27th Annual Symposium on*. IEEE, 1986, pp. 162–167.

[223] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, 1987, pp. 218–229.

[224] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter *et al.*, "Secure multiparty computation goes live," in *International Conference on Financial Cryptography and Data Security*. Springer, 2009, pp. 325–343.

[225] S. Bhattacharjee, S. Sengupta, and M. Chatterjee, "Vulnerabilities in cognitive radio networks: A survey," *Computer Communications*, vol. 36, no. 13, pp. 1387–1398, 2013.

[226] Y. Mao, T. Chen, Y. Zhang, T. Wang, and S. Zhong, "Protecting location information in collaborative sensing of cognitive radio networks," in *Proceedings of the 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. ACM, 2015.

[227] W. Wang and Q. Zhang, "Privacy-preserving collaborative spectrum sensing with multiple service providers," *Wireless Communications, IEEE Transactions on*, vol. 14, no. 2, pp. 1011–1019, 2015.

[228] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Lpos: Location privacy for optimal sensing in cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2015 IEEE*, pp. 1–6.

[229] M. Grissa, A. Yavuz, and B. Hamdaoui, "An efficient technique for protecting location privacy of cooperative spectrum sensing users," in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, April 2016, pp. 915–920.

[230] D. Dolev and A. C. Yao, "On the security of public key protocols," *Information Theory, IEEE Transactions on*, vol. 29, no. 2, pp. 198–208, 1983.
[231] A. Boukerche, *Algorithms and protocols for wireless sensor networks*. John Wiley & Sons, 2008, vol. 62.
[232] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic game theory*. Cambridge University Press Cambridge, 2007, vol. 1.
[233] E. Shi, T. H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proc. NDSS*, vol. 2, 2011, pp. 1–17.
[234] A. Boldyreva, N. Chenette, Y. Lee, and A. O'neill, "Order-preserving symmetric encryption," in *Advances in Cryptology-EUROCRYPT 2009*. Springer, pp. 224–241.
[235] A. C. Yao, "Protocols for secure computations," in *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*. IEEE, 1982, pp. 160–164.
[236] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Security and privacy (sp), 2011 ieee symposium on*. IEEE, 2011, pp. 247–262.
[237] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*, pp. 236–247.
[238] M. Zhang, L. Yang, D.-H. Shin, X. Gong, and J. Zhang, "Privacy-preserving database assisted spectrum access: A socially-aware distributed learning approach," in *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2015, pp. 1–6.
[239] Z. Zhang, H. Zhang, S. He, and P. Cheng, "Achieving bilateral utility maximization and location privacy preservation in database-driven cognitive radio networks," in *Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on*, pp. 181–189.
[240] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.
[241] H. Zang and J. Bolot, "Anonymization of location data does not work: A large-scale measurement study," in *Proceedings of the 17th annual international conference on Mobile computing and networking*. ACM, 2011, pp. 145–156.
[242] J. Trostle and A. Parrish, "Efficient computationally private information retrieval from anonymity or trapdoor groups," in *International Conference on Information Security*. Springer, 2010, pp. 114–128.
[243] B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher, "Cuckoo filter: Practically better than bloom," in *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*. ACM, 2014, pp. 75–88.
[244] I. Kamel and C. Faloutsos, "On packing r-trees," in *Proceedings of the second international conference on Information and knowledge management*. ACM, 1993, pp. 490–499.
[245] H. Krawczyk, R. Canetti, and M. Bellare, "Hmac: Keyed-hashing for message authentication," 1997.
[246] F. Chen and A. X. Liu, "Safeq: Secure and efficient query processing in sensor networks," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–9.
[247] M. Clark and K. Psounis, "Can the privacy of primary networks in shared spectrum be protected?" in *Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on*, pp. 1–9.
[248] J. Wang, M. Ghosh, and K. Challapali, "Emerging cognitive radio applications: A survey," *IEEE Communications Magazine*, vol. 49, no. 3, 2011.
[249] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 996–1019, 2013.
[250] K. G. M. Thilina, E. Hossain, and M. Moghadari, "Cellular ofdma cognitive radio networks: Generalized spectral footprint minimization," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 7, pp. 3190–3204, 2015.
[251] M. Guizani, B. Khalfi, M. B. Ghorbel, and B. Hamdaoui, "Large-scale cognitive cellular systems: resource management overview," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 44–51, 2015.
[252] B. Khalfi, M. B. Ghorbel, B. Hamdaoui, and M. Guizani, "Optimal power allocation for smart-grid powered point-to-point cognitive radio system," in *Computing, Communications and IT Applications Conference (ComComAp), 2014 IEEE*. IEEE, 2014, pp. 316–320.
[253] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 860–898, 2016.
[254] A. O. Bicen, O. B. Akan, and V. C. Gungor, "Spectrum-aware and cognitive sensor networks for smart grid applications," *IEEE Communications Magazine*, vol. 50, no. 5, 2012.
[255] O. B. Akan, O. B. Karli, and O. Ergul, "Cognitive radio sensor networks," *IEEE network*, vol. 23, no. 4, 2009.
[256] S. H. R. Bukhari, M. H. Rehmani, and S. Siraj, "A survey of channel bonding for wireless networks and guidelines of channel bonding for futuristic cognitive radio sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 924–948, 2016.

Mohamed Grissa (S'14) received the Diploma of Engineering (with highest distinction) in telecommunication engineering from Ecole Superieure des Communications de Tunis, Tunis, Tunisia, in 2011, and the M.S. degree in electrical and computer engineering (ECE) from Oregon State University, Corvallis, OR, USA, in 2015. He is currently working toward the Ph.D. degree at the School of Electrical Engineering and Computer Science (EECS), Oregon State University, Corvallis, OR, USA.

Before pursuing the Ph.D. degree, he worked as a Value Added Services Engineer at Orange France Telecom Group from 2012 to 2013. His research interests include privacy and security in wireless networks, cognitive radio networks, IoT and eHealth systems.

Bechir Hamdaoui (S'02–M'05–SM'12) is presently an Associate Professor in the School of EECS at Oregon State University. He received the Diploma of Graduate Engineer (1997) from the National School of Engineers at Tunis, Tunisia. He also received M.S. degrees in both ECE (2002) and CS (2004), and the Ph.D. degree in ECE (2005) all from the University of Wisconsin-Madison. His research interest spans various areas in the fields of computer networking, wireless communications, and mobile computing, with a current focus on distributed optimization, parallel computing, cognitive networks, cloud computing, and Internet of Things. He has won several awards, including the 2016 EECS Outstanding Research Award and the 2009 NSF CAREER Award. He is presently an Associate Editor for IEEE Transactions on Wireless Communications (2013-present). He also served as an Associate Editor for IEEE Transactions on Vehicular Technology (2009-2014), Wireless Communications and Mobile Computing Journal (2009-2016), and for Journal of Computer Systems, Networks, and Communications (2007-2009). He is currently serving as the chair for the 2017 IEEE INFOCOM Demo/Posters program. He has also served as the chair for the 2011 ACM MOBICOM's SRC program, and as the program chair/co-chair of several IEEE symposia and workshops, including GC 16, ICC 2014, IWCMC 2009-2017, CTS 2012, and PERCOM 2009. He also served on technical program committees of many IEEE/ACM conferences, including INFOCOM, ICC, and GLOBECOM. He has been selected as a Distinguished Lecturer for the IEEE Communication Society for 2016 and 2017. He is a Senior Member of IEEE, IEEE Computer Society, IEEE Communications Society, and IEEE Vehicular Technology Society.

Attila A. Yavuz (S'05–M'10) received a BS degree in Computer Engineering from Yildiz Technical University (2004) and a MS degree in Computer Science from Bogazici University (2006), both in Istanbul, Turkey. He received his PhD degree in Computer Science from North Carolina State University in August 2011. Between December 2011 and July 2014, he was a member of the security and privacy research group at the Robert Bosch Research and Technology Center North America. Since August 2014, he has been an Assistant Professor in the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, USA. He is also an adjunct faculty at the University of Pittsburgh's School of Information Sciences since January 2013.

Attila A. Yavuz is interested in design, analysis and application of cryptographic tools and protocols to enhance the security of computer networks and systems. His current research focuses on the following topics: Privacy enhancing technologies (e.g., dynamic symmetric and public key based searchable encryption), security in cloud computing, authentication and integrity mechanisms for resource-constrained devices and large-distributed systems, efficient cryptographic protocols for wireless sensor networks.