electronics

MDPI

Article

A Survey on Citizens Broadband Radio Service (CBRS)

Pranay Agarwal [1,†,‡], Mohammedhusen Manekiya [2,‡], Tahir Ahmad [3], Ashish Yadav [4], Abhinav Kumar [1], Massimo Donelli [2,*] and Saurabh Tarun Mishra [5]

[1] Department of Electrical Engineering, Indian Institute of Technology Hyderabad, Sangareddy 502284, India
[2] Department of Civil, Environmental and Mechanical Engineering, University of Trento, 38123 Trento, Italy
[3] Center for Cybersecurity, Bruno Kessler Foundation, 38123 Trento, Italy
[4] Department of Electrical and Computer Engineering, Tandon School of Engineering, New York University, Brooklyn, NY 11201, USA
[5] Department of Electronics Engineering, Lovely Professional University, Phagwara 144001, India
* Correspondence: massimo.donelli@unitn.it
† Current address: Department of Electrical Engineering, Indian Institute of Technology Mumbai, Mumbai 400076, India.
‡ These authors contributed equally to this work.

Abstract: To leverage the existing spectrum and mitigate the global spectrum dearth, the Federal Communications Commission of the United States has recently opened the Citizens Broadband Radio Service (CBRS) spectrum, spanning 3550–3700 MHz, for commercial cognitive operations. The CBRS has a three-tier hierarchical architecture, wherein the incumbents, including military radars, occupy the topmost tier. The priority access licenses (PAL) and general authorized access (GAA) are second and third tier, respectively, facilitating licensed and unlicensed access to the spectrum. This combination of licensed and unlicensed access to the spectrum in a three-tier model has opened novel research directions in optimal spectrum sharing as well as privacy preservation, and hence, several schemes have been proposed for the same. This article provides a detailed survey of the existing literature on the CBRS. We provide an overview of the CBRS ecosystem and discuss the regulation and standardization process and industrial developments on the CBRS. The existing schemes for optimal spectrum sharing and resource allocation in CBRS are discussed in detail. Further, an in-depth study of the existing literature on the privacy of incumbents, PAL devices, and GAA devices in CBRS is presented. Finally, we discuss the open issues in CBRS, which demand more attention and effort.

Keywords: CBRS; PAL-GAA; CBSDs; privacy; CBRS regulation and standardization; FCC standardization; CBRS spectrum allocation

Citation: Agarwal, P.; Manekiya, M.; Ahmad, T.; Yadav, A.; Kumar, A.; Donelli, M.; Mishra, S.T. A Survey on Citizens Broadband Radio Service (CBRS). *Electronics* **2022**, *11*, 3985. https://doi.org/10.3390/electronics11233985

Academic Editor: Dimitris Kanellopoulos

Received: 18 October 2022
Accepted: 25 November 2022
Published: 1 December 2022

1. Introduction

The ubiquity of smartphones and smart objects has augmented the volume of data flow across the globe. It has propelled the requirement for additional spectra to meet the ever-increasing demands of high data rates. Researchers in industries and academia are striving to explore wireless communications in novel bands such as mmWave, THz spectrum, and visible light spectrum [1–3]. An alternate strategy to mitigate the spectrum dearth lies in the efficient use of the existing spectrum, which requires technological and policy innovation. Technologically, cognitive radio networks can be a promising solution to leverage the existing spectrum for boosting the capacity of wireless networks as their prioritized and dynamic spectrum access capabilities can efficiently transform the spectrum holes into transmission opportunities [4]. At the policy level, the Federal Communications Commission (FCC) has initiated spectrum sharing by allowing wireless service providers to access the underutilized TV broadcast bands in an unlicensed fashion [5]. As a step ahead in this direction, the citizens broadband radio service (CBRS) band has been opened by the FCC in the United States for the commercial cognitive operations between 3550 and 3700 MHz span [6]. A three-tier hierarchical architecture has been followed by the CBRS

that reserves the topmost tier for incumbents, including ground-based and ship-borne military radars and fixed-satellite-service earth stations [7]. The second tier, the priority access license (PAL) tier, opens the spectrum for licensed operations from the wireless service providers who have purchased the license through competitive bidding [7]. The unlicensed operations are permitted in the band through the third tier, also known as the general authorized access (GAA) tier. The hierarchy of the tiers reflects the descending order of spectrum access priority across the tiers, which implies the devices operating in the PAL and GAA tiers should abide by the stringent regulations imposed by the FCC. The spectrum access system (SAS) is the centralized entity in the CBRS ecosystem, which allocates resources to the PAL and GAA devices, while simultaneously protecting the incumbents and PAL devices from any harmful interference.

The CBRS architecture provides an additional 150 MHz spectrum and provisions access to the spectrum in both a licensed and unlicensed manner. It can be pivotal in realizing multiple use cases of evolving wireless communications. For instance, the mobile network operators can purchase the license and use the spectrum to offload their traffic, improving the quality of service for end-users. The GAA tier can be used for private LTE networks, industrial internet-of-things, smart homes, and other use cases [8]. The FCC has specified stringent regulations for protecting incumbents and PAL devices from harmful interference and allocating resources to the PAL and GAA devices [7]. Although the standards do not mandate any interference protection criteria for GAA devices, some coexistence mechanisms between GAA devices are required to ensure the quality of service to the end-user. Therefore, a relevant requirement is that different schemes for spectrum sharing and resource allocation adhere to the FCC regulations and lead to efficient utilization of the CBRS spectrum. The opportunity to unleash the potential of the CBRS spectrum for boosting the capacity of wireless networks is undoubtedly a welcome step in the current scenario of the global spectrum crunch. However, the risk of penetration of commercial devices into the private and confidential operational details of incumbents cannot be overlooked. The incumbents in CBRS include military radars, and hence, the privacy of their operation parameters is a matter of grave concern. As per the standard, incumbents' location, operation time, and operation frequency are confidential, and any loophole in their privacy can have catastrophic effects on national security [9]. An adversary can infer the location of an incumbent by querying the SAS from multiple locations via a compromised device and analyzing the maximum transmission power permitted for the device [10]. Similarly, the operation time and frequency of incumbents can be inferred by an adversary if a compromised device is asked to vacate the spectrum [11,12]. Therefore, the mechanisms to preserve the privacy of incumbents in CBRS while maintaining the utility of PAL and GAA devices are required.

Different schemes have been proposed in the literature for spectrum sharing by PAL and GAA devices and preserving the privacy of incumbents and PAL and GAA devices in CBRS. However, a comprehensive discussion of the proposed schemes is required to demarcate the solved and open issues in CBRS. A comprehensive review of resource allocation in CBRS is not available in the literature. However, due to various restrictions and constraints from the standards and regulations, resource allocation in CBRS is an important problem that should be properly addressed. Regulations are also changing between US and Europe. Motivated by this, a study that explores in depth the various resource allocation schemes in the literature for spectrum sharing, privacy preservation, the latest standards, and regulations along with key issues in CBRS is needed. The main contributions of this paper are as follows.

- We provide a complete overview of the CBRS architecture describing the entities and their functionalities and highlighting different CBRS stakeholders and the regulation and standardization process in CBRS.
- An in-depth discussion of several schemes proposed in the literature for spectrum sharing and resource allocation in CBRS is provided.

- We provide a comprehensive discussion of the contributions and weaknesses of the schemes proposed in the literature for preserving the privacy of incumbents, PAL devices, and GAA devices in CBRS.
- The open issues requiring further research are presented.

To the best of our knowledge, this is the first in-depth survey on spectrum sharing and privacy in CBRS.

The paper is organized as follows. Section 2 provides an overview of the CBRS ecosystem. A comprehensive review of the spectrum sharing in CBRS is provided in Section 3. An in-depth discussion on privacy in CBRS is provided in Section 4. Section 5 presents the regulations and standardization of CBRS and highlights different CBRS stakeholders. Section 6 discusses the key research limitations and highlights possible future research directions for resource allocation, privacy, and some practical implications in CBRS. Section 7 provides the concluding remarks.

2. CBRS—An Overview

In this section, we provide an overview of the CBRS ecosystem. We describe the three-tier hierarchical architecture of the CBRS consisting of the incumbent, PAL, and GAA devices. Further, the regulations specified for the frequency assignment for all the devices are discussed. Finally, we describe the functionalities of the SAS and ESC in the CBRS ecosystem.

2.1. Three-Tier Hierarchical Architecture

Figure 1 illustrates the three-tier hierarchical architecture of the CBRS consisting of the incumbents in the topmost tier, PAL devices in the second tier, and GAA devices in the third tier. The ship-borne and ground-based military radars and fixed-satellite-service (FSS) earth stations are the incumbents occupying the first tier and have traditionally used the CBRS spectrum. Please note that the FSS earth stations only receive and do not transmit. The PAL devices occupying the second tier can access the spectrum in the licensed mode after purchasing the license through competitive bidding. There are certain regulations set forth for the license, which are:

- Each license is valid for a period of ten years;
- Each license is valid for only a single license area consisting of a county, where counties are defined based on the data of the United States Census Bureau;
- Each license authorizes the licensee to transmit on a 10 MHz channel in a license area;
- A licensee can aggregate up to four licenses in the service area consisting of its multiple contiguous license areas;
- More than 7 licenses cannot be given in any license area at any given time [13].

The mobile network operators can be a suitable candidate to purchase the license and utilize the CBRS spectrum as a supplemental downlink offloading their traditionally owned spectrum. The GAA devices in the third tier are permitted unlicensed access to the spectrum. This makes the third tier suitable for establishing a private LTE network, cellular-IoT, and related use cases. The devices operating in the second and third-tier are termed the CBRS devices (CBSDs). The CBSDs typically consist of the fixed stations, for instance, evolved NodeB (eNBs) or a network of the eNBs, but do not include the end-user devices, i.e., user equipment. The CBSDs are categorized into category A and B depending on the maximum effective isotropic power (EIRP), which is 30 dBm/10 MHz and 47 dBm/10 MHz for category A and B CBSDs, respectively. Similarly, the maximum power spectral density allowed for category A and B CBSDs is 20 dBm/10 MHz and 37 dBm/10 MHz, respectively. The maximum EIRP specified for the end-user devices is 23 dBm/10 MHz [7].

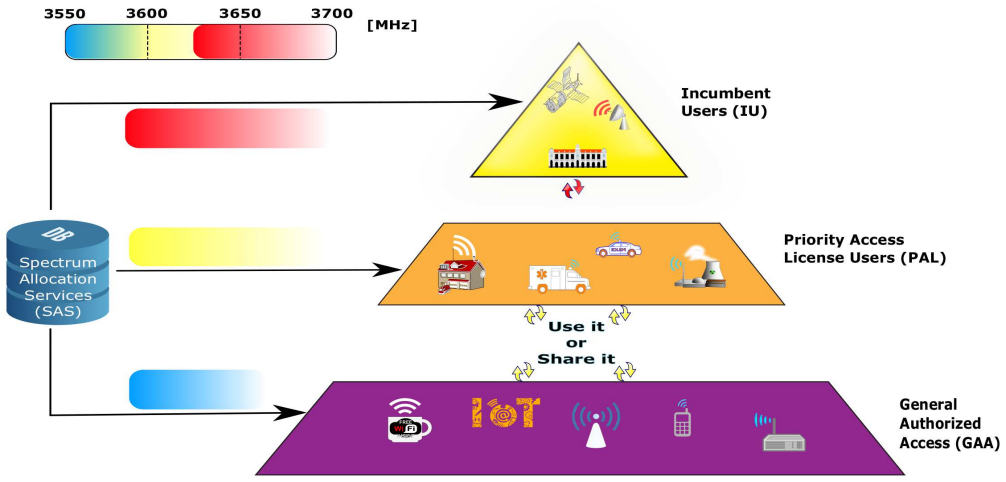

Figure 1. Three-tier hierarchical architecture of the CBRS.

The hierarchy of the incumbents, PAL CBSDs and GAA CBSDs, reflect the decreasing order of their priority to access the spectrum. The incumbents are guaranteed protection against interference from the PAL and GAA CBSDs, implying that the PAL and GAA CBSDs have to reduce their transmission power or, if required, switch to another channel when an incumbent becomes active on the channel. Similarly, the PAL CBSDs are also guaranteed protection against interference from the GAA CBSDs. The exclusion zones are specified around the locations of incumbents, which prohibit any PAL and GAA CBSDs within the zone from accessing the spectrum. The ship-borne military radars are mobile and have their exclusion zones along the coastline. However, the ground-based military radars operate from fixed locations mentioned in [7] and have an exclusion zone of 80 km radius around their location [13]. Similarly, a -96 dBm/10 MHz default protection contour is determined around each PAL CBSD within which any GAA CBSD is not permitted to share the channel with the active PAL CBSD. The PAL CBSDs can also decide to impose a smaller protection contour than the default. Moreover, the overlapping protection contours of multiple CBSDs are combined into a single protection contour. However, the protection area of any PAL CBSD cannot extend beyond the service area of the licensee. The GAA devices operating in the third tier are not given any protection from the top-two tier devices and are expected not to create any harmful interference to the incumbents and PAL CBSDs. Next, we highlight the rules and regulations specified for the frequency assignments for the incumbents and CBSDs.

2.2. Regulations for Frequency Assignment

The CBRS spectrum, spanning 3550–3700 MHz, has a total bandwidth of 150 MHz. Figure 2 depicts the regulations specified for the frequency assignments for different devices. The ship-borne military radars can only operate within the former 100 MHz spectrum, i.e., 3550–3650 MHz, whereas the ground-based military radars can operate within 3650–3700 MHz. The FSS earth stations can operate within 3600–3700 MHz [8]. The regulations regarding the channel allocation for PAL CBSDs are as follows [7].

1. The PAL CBSDs can only operate within the former 100 MHz spectrum, i.e., 3550–3650 MHz.
2. The minimum bandwidth of the channel that can be allocated to the priority access licensee is 10 MHz.
3. A priority access licensee can aggregate up to 4 licenses in a license area at any given time, which implies the PAL CBSDs under a licensee can operate on a maximum bandwidth of 40 MHz.

4. The total number of channels assigned for the operations of the PAL CBSDs cannot exceed 7, as the total number of licenses in a license area is limited to 7. This implies that the PAL CBSDs cannot access more than 70 MHz of the spectrum at any given time.
5. *Geographic Contiguity:* If a priority access licensee holds multiple licenses belonging to contiguous license areas, it should be assigned the same channels in each license area, to the extent feasible.
6. *Channel Contiguity:* If a priority access licensee holds multiple licenses all belonging to a license area, it should be assigned multiple contiguous channels, to the extent feasible.

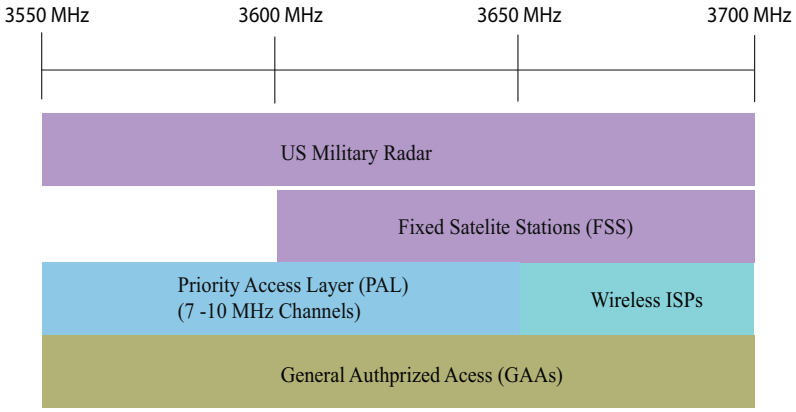

Figure 2. Regulations for frequency assignment.

The GAA CBSDs are allowed to operate within the entire spectrum. However, the actual channel allocation to the PAL and GAA CBSDs depends on the incumbents' activity and the interference relations governed by the locations of the active incumbents, PAL CBSDs and GAA CBSDs. Thus, the channel allocation for the PAL and GAA CBSDs is a non-trivial task and demands a supervising entity that could ensure the system's proper functioning. Next, we describe this supervising entity, i.e., SAS.

2.3. SAS

SAS is the heart of the CBRS ecosystem, which is responsible for

1. Registering the CBSDs, authenticating their location and identity, and authorizing them for spectrum access;
2. Communicating with the ESC sensors regarding the activity of the incumbents and enforcing the exclusion/ protection zones to protect the incumbents from any harmful interference from the PAL and GAA CBSDs;
3. Confirming the relocation or suspension of the CBSDs from a channel within 300 s once the activity of incumbents are detected on the channel;
4. Allocating the channels to the PAL and GAA CBSDs while protecting the PAL CBSDs against any harmful interference from other PAL CBSDs and GAA CBSDs;
5. Determining the maximum transmission power of the CBSDs at their location;
6. Responding to the queries of the PAL and GAA CBSDs regarding the availability of the spectrum.

Different procedures specified for SAS to register and authorize the CBSDs and exchange information between the SAS and CBSDs are as follows [14].

1. *SAS Discovery Procedure:* Each SAS administrator provides a URL to the registered CBSDs. The registered CBSDs can use the list of URLs to connect to a server. The SAS and CBSDs mutually authenticate each other using the transport layer security protocol.

2. *CBSD Registration Procedure:* A CBSD in the *Unregistered* state can send the registration request to the SAS after the mutual authentication procedure is completed successfully. The registration request message contains the identity, location, equipment capabilities, and measurement reporting capabilities of the CBSD. The SAS can either accept or reject the registration request. The CBSD transits to the *Registered* state once the SAS accepts the registration request. However, the CBSD remains in the *Unregistered* state if the SAS rejects the registration request. Figure 3 presents the registration state diagram of the CBSD.
3. *CBSD Spectrum Enquiry Procedure:* A registered CBSD can send the spectrum enquiry request to the SAS to determine the availability of the spectrum. The CBSD can specify one or more channels it plans to use and determine their availability. The SAS can respond with the list of available channels. The CBSD can use this procedure to determine the operational parameters, such as channel, transmission power, etc., that it can use for transmission.
4. *CBSD Grant Procedure:* A CBSD can start the grant procedure once it has successfully completed the registration procedure. Here, a grant can be seen as a contract between the SAS and CBSD through which the SAS authorizes a CBSD to transmit on the band only using the operational parameters specified in the grant. A CBSD in the *Idle* state can send a grant request to the SAS, which contains the operational parameters it plans to use for transmission. The SAS can accept the grant request if the operational parameters mentioned in the grant do not create any interference and reject the request otherwise. The CBSD transits to the *Granted* state if the SAS accepts the request and sends the grant expiry time and heartbeat interval time. The CBSD remains in the *Idle* state if the grant request is rejected. The CBSD in the *Granted* state cannot transmit on the band until it successfully completes the heartbeat procedure and moves to the *Authorized* state. Figure 4 presents the grant state diagram of the CBSD.
5. *CBSD Heartbeat Procedure:* The CBSD sends the first heartbeat request after it has successfully completed the grant procedure and entered into the *Granted* state. The CBSD can transmit on the band using the operational parameters specified in the approved grant only after the SAS accepts its heartbeat request. The heartbeat interval, grant expiry timer, and transmit expiry timer are specified in the heartbeat response message by the SAS. The CBSD has to send heartbeat requests after the heartbeat interval timer elapses. The CBSD has to stop its transmissions within 60 s once the transmit expiry timer has elapsed. The SAS uses the heartbeat procedure to interact with CBSDs and dynamically control their transmissions on the band with respect to the activity of the incumbents by renewing, suspending, and terminating the associated grants.
6. *CBSD Grant Relinquishment Procedure:* The CBSD can send the relinquishment request to the SAS for terminating any existing grant. The SAS can accept the request and terminate the grant. The CBSD is then not authorized to transmit on the band using the operational parameters specified in the terminated grant.
7. *CBSD Deregistration Procedure:* The CBSD uses this procedure to de-register itself from the SAS. The SAS deletes all the grants associated with the CBSD. The CBSD enters into the *Unregistered* state, as shown in the Figure 3.

Next, we describe the role of ESC in the CBRS ecosystem.

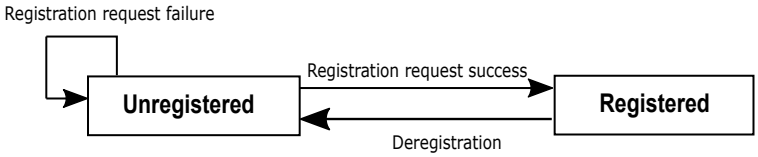

Figure 3. CBSD registration state diagram.

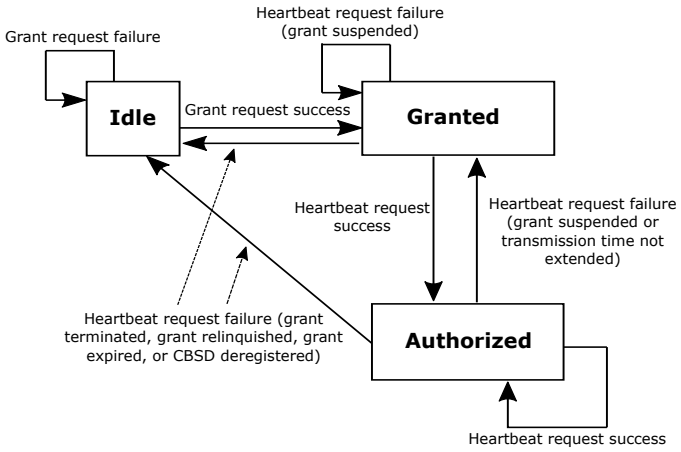

Figure 4. CBSD grant state diagram.

2.4. ESC

ESC is a network of sensor nodes deployed in the vicinity of the exclusion zones by any non-government entity approved by the FCC [7]. The primary purpose of the ESC is to accurately detect the signals of the incumbents and communicate the presence of incumbents to the SAS. The exclusion zones around the locations of incumbents shall be converted to dynamic protection zones once the ESC is deployed and approved by the FCC. The SAS controls the transmission of the PAL and GAA CBSDs and protects the incumbents from any harmful interference once the ESC communicates the presence of the incumbents. Therefore, ensuring the availability at all times, security and privacy of the operation parameters of the incumbents, and precision in detecting the presence of incumbents, are vital requirements for proper management of the spectrum.

3. Spectrum Sharing (Resource Allocation)

In this section, we explain the resource allocation of a spectrum in the CBRS ecosystem. The resource allocation has been examined with different parameters such as Power, Delay Time, Bandwidth, Distance, Traffic, and User. It is presented in Table 1. Each parameter played a major role in the CBRS ecosystem's feasibility and dynamicity. Each parameter of the resource allocation has been illustrated in the following Figure 5.

Table 1. Resource allocation classification of CBRS.

	Power	Delay	Bandwidth	References
	✓	X	X	[15–37]
	X	✓	X	[19–23,26,27,32,33,38–44]
	X	X	✓	[15,16,29,31,34,45–52]
	✓	✓	X	[19–23,26,27,32,33]
	✓	X	✓	[15,16,29,31,35]
Resource	**Distance**	**Traffic**	**Users**	**References**
Allocation	✓	X	X	[16,17,24,29,35,41,44,45,53–56]
	X	✓	X	[15,18,19,39,42,52,53,57,58]
	X	X	✓	[15,16,25,28,32,33,36,43,52,53,59–62]
	✓	✓	X	[31,41,53,63]
	X	✓	✓	[15,53]
	✓	X	✓	[16,53]

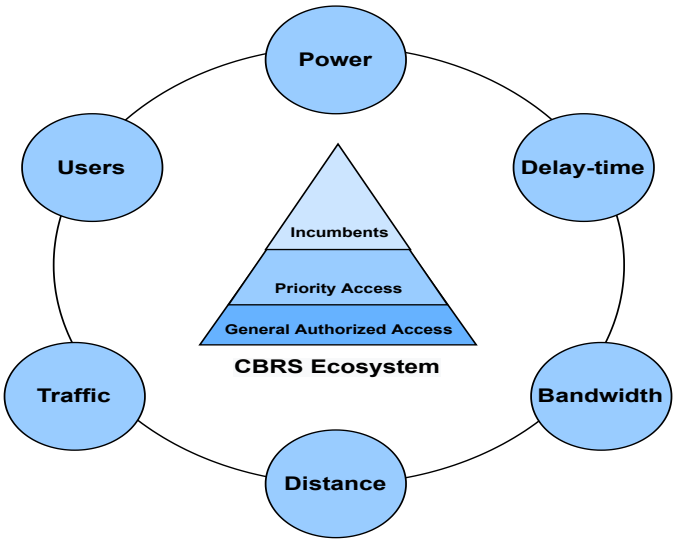

Figure 5. Resource allocation parameters of a spectrum in CBRS ecosystem.

3.1. Power

An overview of the spectrum sharing technology has been presented in [15]. Different types of spectrum sharing models have been discussed and compared. The spectrum sharing model has been explained particularly for the CBRS band. Moreover, the 5 GHz unlicensed band's power consumption has been compared to the application's. In [16], the author has modeled and analyzed a stochastic geometry-based model for the CBRS device. The proposed model has been analyzed on licensed and unlicensed operators. The correlation in the interference power between the licensed and unlicensed user is calculated using the proposed model's probability of the operators' transmission power. In [17], the power control algorithm was proposed to reduce the Naval Radar and coexisting CBRS device interference. The power control of the CBRS device changes according to the distance between the device and the naval Radar. The variation of the device power from the Radar operating range has also been mentioned. In [18], they exhibit a general framework for the local micro operator's spectrum authorization for CBRS. Primarily, different types of elements have been defined for the spectrum authorization model. The transmission and interference power have been considered to define the proposed model's elements. Ref. [19] exhibits the optimal transmit power and spectrum utilization probability of GAA CBRS user while considering the maximum power is transmitted without interfering with the PAL user. Ref. [20] proposes the interference coordination between the Radar and LTE users (they proposed this method in CBRS).

For pulse Radar, the target detection has been evaluated when the LTE user interference is present, and vice-versa. In [21], interference between the Radar and LTE system is compared with a commercial off-the-shelf radio system simulator. The simulation results measured the full throughput at -70 dBm interference power corresponding to a -5 dB signal-to-interference ratio (SIR). In [22], an experiment was performed on the coexistence of the Naval Radar in the CBRS band and LTE-U network. The interference model was designed by considering the transmit power of LTE-U eNodeB, the noise power in a 5 MHz channel, and the Radar's transmit power. Ref. [23] derives the interference power based on a dedicated channel propagation model and proposes two schemes; an open-loop and a closed-loop for power control. The transmit power for all end-users was monitored. The experiment was performed for the WiMax system and USRP device as a small cell. The conclusion was drawn that a network operator may provide a new business model that delivers mobile, small cells to customers close to its base stations, thereby leading to better spectrum utilization and higher revenue. In [24], coexistence performance has been evaluated using the LTE-TDD system. The system measures the trade-off between CBRS device coverage and power for the micro and private network. In [25], the transmit power

allocation algorithm is proposed to maximize the GAA users' capacity while ensuring the interference for a different number of PAL users. In [26], the author proposed the detection of SPN-43 in a low-resolution spectrogram.

Furthermore, utilizing a Short-Time Fourier transform (STFT) to estimate the spectrum occupancy and power of Non-SPN 43 emissions, the Machine Learning Algorithm classifiers identify SPN-43 presence spectrograms. In paper [27], the author proposed a reinforced Q-Learning algorithm to assist the GAA user (secondary user) in sensing the PAL (primary user) unutilized spectrum in Listen-Before-Talk fashion. Moreover, the algorithm dynamizes the energy detection threshold to maximize user-perceived throughput at the secondary user while minimizing the impact on the primary user. To simultaneously provide access to Mobile GAA and Fixed GAA users in the same spectrum, paper [28], models the interfering angle and path loss-based method to calculate maximum allowable transmit power for MGAA to minimize interference between MGAA with FGAA and PAL users. Paper [29] deals with the power and frequency allocation among CBSDs under the coexistence manager's a controlled environment. The author maximizes the spectrum bandwidth assigned to CBSDs over a broader geographical area, i.e., directly proportional to the assigned transmit power. In paper [30], the researcher proposed a Machine Learning-based novel algorithm to detect the incumbent user at ESC under geospatial constraints. The paper modeled the problem as a classification problem to predict the modulation scheme of the incumbent operator. The authors in the paper [31] studied and modeled the WInnForum GAA-GAA coexistence scheme, called Approach 1. The researcher examined the Signal-to-Interference Ratio at a Grid, Average Interference Power per unit Area, Average Interference Power per CBSD per Channel per grid, Propagation Models, the effect of the propagation model, and deployment density. In paper [32], researchers propose a model to reduce total power consumption at CBSDs by dividing user data into two parts, namely, individual interest and shared interest. Moreover, for shared interest user data, the author utilized the GreenLoading network framework and the Broker Priority Assignment Algorithm, which created eNodeB that enables data and computing power closer to the users' location as an edge computing device to minimize power consumption as a function of time.

3.2. Delay Time

Along with power, delay time played an important role in measuring and analyzing the frequency change in a field trial environment to protect primary users against interferences. In [38], the analyzed time domain operation in a practical SAS-based CBRS system by utilizing the knowledge of the latest base station model to propose the evacuation and reconfiguration time by 70%. The SAS system [19] proposed the channel allocation for GAA users while considering the spectrum utilization probability. It calculates the switching overhead for the SAS system, which supports GAA CBSDs to switch to a different channel when the spectrum utilization probability is below a threshold level. Regarding coexistence between LTE-WiFi in the 3.5 GHz band, LTE must transmit for a fixed duty cycle, whereas Wi-Fi transmits in the rest of the cycle. The neighborhood spectrum sharing could be possible without interfering with each other's performance. For LTE-Wi-Fi coexistence, ref. [39] proposes a fixed duty cycled LTE-U and WiFi-based smart grid metering infrastructure. The smart meter utilizes WiFi, and Access Point (AP) uses LTE for data transferring in the 3.5 GHz band with an FTP traffic model for system-level simulation. Whereas [22] explores the feasibility of a duty-cycle-based approach to enable the close-range coexistence of an LTE network on the same channel as an incumbent rotating radar in the CBRS bands.

The coexisting LTE eNodeB (implemented using srsLTE) senses the radar transmission pattern to estimate radar rotation speed and pulse duration (equivalent to its 3 dB beamwidth) and mutes its transmissions accordingly (based on averaged values of period and on-duration) so that it would not transmit when a radar transmission is estimated. Paper [40] presents the design and results for a broadcast message termed reject the request to send (RRTS). The RRTS mechanism is used to overcome the problem of inefficient spectrum

allocation among the CBRDs and 5G nodes. This mechanism is based on the IEEE 802.11 distributed coordination function (DCF). The principle idea behind the proposed concept is to apply different initial values to control the nodes' binary-exponential-backoff-process (BEB) to extend the contention window in runtime and enhance the system throughput. Papers [27,41] present a Q-learning algorithm to estimate evacuation time useful within a real-time interference scenario and to show the Secondary Node can improve its throughput by up to 350% with only marginal losses to the Primary Node (4%) by using average and differential Primary Node buffer occupancy as environmental observation, respectively. In [26], various deep learning methods have been investigated for time and frequency steps. It measures the effectiveness of thirteen detection algorithms, including eight deep learning methods, three classical machine learning approaches, and two energy detection strategies in the 3.5 GHz band. Whereas, paper [42] presented the Iris system architecture to embed a dynamic pricing mechanism in a practical neutral-host design for the indoor small-cell environment.

The dynamic pricing mechanism of Iris follows a time-slotted operation for the shared spectrum allocation. The pricing policies are estimated using deep reinforcement learning to request shared spectrum resources on demand while recouping the costs for shared spectrum acquisition. Paper [42] developed Iris for LTE and conducted extensive experimental tests to characterize the dynamic pricing mechanism of Iris under different conditions. Furthermore, it presents the benefits of the Iris approach compared to alternative approaches and examines the deployment feasibility of Iris. In [43], a basic SAS-CBSD protocol simulator has been developed and studied for the impact of the heartbeat interval on the CBRS system in terms of meeting the end-to-end timing constraint set forth by the FCC rules. The simulator shows how a message overload on an SAS can lead to an unnecessary timeout of the transmitExpireTime timer, which can extend to the suspension of CBSD transmission, thereby reducing spectrum utilization. The tradeoff between the number CBSDs and the time taken to meet the end-to-end timing constraint can be served by an SAS without causing unnecessary suspension of CBSD transmission. Ref. [43] simulation results suggest that around 150 s may strike a good balance between the tradeoffs. In [32], the author created a GreenLoading framework for efficiently offloading cellular network traffic to the CBRS band using shared interest information and data brokers. They proposed a Broker Priority Assignment (BPA) algorithm to select the shared-interest user groups for the data brokers to broadcast traffic.

In the GreenLoading framework, one-hop offloading has been considered to restrict the delay for users. The impact of the QoS response time on the power consumption of GreenLoading has been considered with the response time threshold from 200 to 700 ms with a 50 ms step size. The in-field experiment and Google Maps (web-based) data collectioin across four diverse US cities in dense and sparse areas have been conducted. Their experimental results showed that, on average, an order of magnitude power savings via GreenLoading to the CBRS band over a 24 h period and up to 97% at peak traffic times. Additionally, the fairness improves up to 81% with the use of the max-min ratio and 64%. While paper [33] demonstrates that with the proposed framework, both throughput and access delay can be significantly improved over the state-of-the-art LAA system. Furthermore, by optimizing access delay and improving inter-operator resource fairness, the system is designed to be more amenable for operators to invest in deploying networks using a shared spectrum. Furthermore, taking advantage of small timescale variations in traffic demand can lead to large statistical multiplexing gains possible through dynamic sharing instead of static, hard splitting of the shared spectrum, as present in the current CBRS system. In [44], they use time as an observational reference to their general privacy framework for assessing the privacy of primary users in the SAS setting model. The adversary exploits the spectrum access system and obfuscation strategies to protect user privacy.

3.3. Bandwidth

The wireless communities in the United States have undertaken the idea of a three-tier spectrum sharing system. Ref. [45] discusses a spectrum shared system in the US context and provided a focused analysis of the SAS and functionalities to support 3.5 GHz band dynamic management. The analysis shows that dynamic spectrum management significantly improves the spectrum usage efficiency and influences other spectrum band management. Meanwhile, Ref. [46] presented a spectrum sensing system by UAV to improve the quality and amount of the test data. The UAV aircraft acts as "radar" and mimics the radar signal transmission to first-tier incumbent users. The second-tier PAL service acts as a broadband like LTE. Ref. [34] presents a fair resource allocation model and partitioning method to assign resources to SASs in the CBRS band. In current frameworks in the 3.5 GHz band for tiered spectrum, sharing allows for environment sensing capability operators (ESCs) to measure spectrum occupancy. This happens for the commercial users to use the spectrum when federal incumbent users are not present. Refs. [47,48] shows that in licensed and unlicensed bands, the impact of increasing bandwidth decreases the congestion cost for a given number of users. Ref. [47] focuses on a single geographic area and assumes both SAs uses a single shared spectrum. Furthermore, it presents a model of market spectrum management in that wireless service operators acquire information about spectrum availability from an ESC, where different ESCs may offer different qualities of information. The results presented in [47] state that the differences in information quality depend strongly on the licensing model. Whereas in [48], the authors consider a tiered spectrum market. Furthermore, using Nash equilibrium, it explores what happens when SA obtains information from the same or other ESCs. The SAs obtain information from the ESC. Paper [49] proposed a four-layer frequency sharing model to manage the entire wireless communication spectrum and other systems from a conceptual point of view larger than CBRS and licensed shared access (LSA). The proposed model utilizes disaster safety and public welfare communication to provide the direction of efficient frequency use.

In the CBRS band, to broaden the mobile operating system, multiple small cells have been deployed; these deployments cause the inter-operator interference problem while accessing the shared spectrum. In [50], an inter-operator spectrum sharing problem was studied in small cell networks. Ref. [50] designed a communication-free optimal channel assignment scheme, which uses a reproducing Hilbert space kernel to predict the channel vacancy by vector-valued regression. The optimal channel assignment to the base stations takes a traffic load into account, while the prediction values rely on each operator to perform it independently. In the paper, [64] designed and optimized the algorithm to maximize the spectrum utilization and bandwidth. Whereas paper [51] addresses the fair dynamic spectrum management system for distributing incumbents in a licensed shared access system. The proposed system has been tested in different operating scenarios such as a single-incumbent multi-licensee operators case and multi-incumbent multi-operators case. Finally, ref. [51] proposes penalties to reduce spectrum allocation when the LSA licensee operators do not comply with the LSA regulations. Various algorithms have been proposed for the inter-operability of different LSA coalitions. A complete study of the fundamental characteristics numerically compares the mean allocated spectrum for each licensee operator by evaluating unallocated spectrum and dissatisfaction metrics.

3.4. Distance

For incumbent detection [45] used multiple sensor nodes to tackle the multipath and shadowing issue. The correlation between multiple sensor nodes is dependent on the fixed inter-node distance. The availability of multiple sensor nodes reduces the probability of deep fading and increases the spatial diversity over the sensor nodes. Using stochastic geometry, ref. [16] modelled the network evaluating the MAP and the coverage probability by providing an approximate expression for two useful distance distributions specific to the PHP network. The three-tier spectrum sharing model [53] shows a way to reduce the aggregate interference experienced by the GAA users when the number of GAA users is

higher than the vacant channels. The model allocates the same channel with large distance inter-CBSD GAA users. Similarly, in [24], the relation between CBRS device coverage and power has been calculated for inter-CBRS GAA user coexistence. In [17], a detailed analysis is presented to determine an appropriate protection distance from the radar to meet a specific radar interference-to-noise ratio (INR) protection criterion. Based on INR, it proposes power control algorithms to adjust the transmit power of CBSDs to further reduce the protection distance by increasing spectrum access for the coexisting CBSDs. The analysis [17] suggests that maintaining a 30 km protection distance from the radar will ensure the required INR protection criterion of -6 dB at the radar receiver.

In [54], they considered distance in order to characterize SAS, and to determine if two GAA nodes are interfering with each other or not. In [41], the authors considered an urban scenario with an area of A = 1 km^2 on average and a population of W = 2000 on average. The CBSDs are distributed in a 790-by-790 m region with a set-back distance of 210 m. The total number of CBSDs are $N = W \times MP/100$. Where [29] explores the power and distance relation for the resource allocation of CBSDs for various cell distances. For wider distances, the advantages are that it reduces the transmission power but utilizes the whole bandwidth in each CBSD. In paper [31,35], they performed an outdoor experiment for General Authorized Access (GAA) user coexistence with a deployment area of 5 km $\times$ 5 km in size on the east coast at latitude 36.872227 deg and longitude -76.023389 deg, and in the west coast at latitude 32.723588 and longitude -117.145319 of the USA. Meanwhile, Ref. [63] evaluates the indoor performance of the on-demand spectrum access (ODSA) architecture in a 20 node sample CBRS network. Ref. [55] modeled and deployed the minimum separation distance between micro operators to reduce the impact of interference. While [44] studied the primary users (PU) privacy preservation using obfuscation methods for an SAS that grants transmit power assignments based on the distance between secondary users (SU) to the nearest PU.

3.5. Traffic

For small cell networks to improve the efficiency in high traffic geographic location spectrum sharing technique an overview has been presented in paper [15]. Refs. [18,19,53] presents and compares the results of the user traffic while considering the coexistence with the CBRS network. In [39], the coexistence performance of LTE-WiFi in the 3.5 GHz band is investigated using a time division duplexing (TDD)-LTE by WiFi along with an FTP traffic model for system-level simulation. In [57], an outdoor scenario for the coexistence of LBT and GAA users calculated the served traffic in the spectrum-sharing CBRS. In [58], they present a listen-before-talk (LBT) scheme to improve spectrum sharing and throughput. The detailed analysis provides insight that the decreased PAL node (PN) user-perceived throughput (UPT) is a function of PN traffic load and problematic network topologies between PN/SN users. Moreover, the PN Q-learning algorithm has been designed for carrier sensing to reduce the negative consequences of spectrum sharing on the PN Q-learning algorithm. Paper [42] presented a Deep Reinforcement Learning-based shared spectrum access architecture for a small cell indoor scenario, while considering whole-day traffic. The learning behavior for different kinds of traffic loads has been measured and compared with the total traffic served by a cell throughout the day. Furthermore, Ref. [52] discusses the incumbent interference in multi-SAS shared spectrum sharing in CBRS. The paper considers the dynamic protection area for several users and the traffic they generate.

3.6. User

Various resource allocation methods and spectrum management techniques have been studied, but few papers discuss spectrum sharing and management with CBRS users. Refs. [16,32,43,61] discuss primary user spectrum sharing and channel allocation methods. While paper [59,60] discusses spectrum sharing for secondary and primary users. Whereas, Refs. [15,36,53] explore spectrum sharing in all three tiers. Furthermore, Refs. [25,28,33,62]

specifically examine the power and resource allocation for tier-three (GAA) and tier-two (PAL) users.

4. Privacy

The provision of cognitive commercial operations in the CBRS spectrum paves the way toward efficient utilization of the existing spectrum as the cellular base stations and wireless service providers can use the spectrum to boost the capacity of their networks. However, the risk of penetration of PAL and GAA CBSDs into the operational parameters of the incumbents and the consequential violation of their privacy is a matter of grave concern. Per the standards, incumbents' location, operation frequency, and operation time are confidential, and any leakage of them can jeopardize national security [9]. Figure 6 illustrates the confidential operational parameters of the incumbents, which are susceptible to the inference attacks of the adversary.

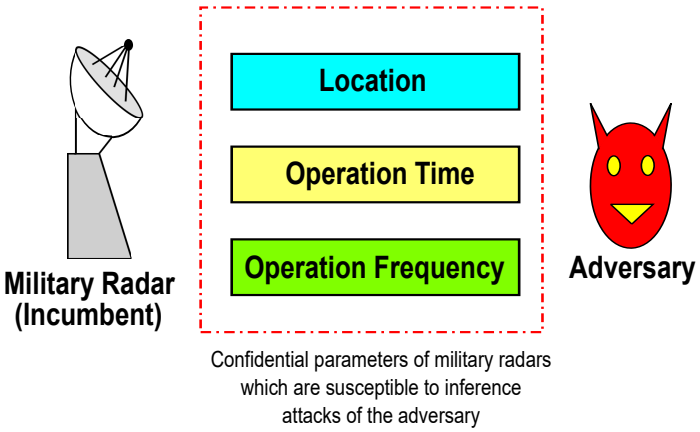

Figure 6. Confidential operational parameters of incumbents susceptible to inference attacks of the adversary.

An adversary can compromise a legitimate CBSD, query the SAS from multiple locations, and observe the maximum transmission power permitted to infer the location of the incumbents [10]. Similarly, the adversary can learn the operation time and frequency of the incumbents if a compromised CBSD is asked to vacate the spectrum or shift to another frequency [11,12]. Therefore, we need to preserve the privacy of the operation parameters of the incumbents. However, the privacy of incumbents comes at the cost of the capacity of the PAL and GAA CBSDs. Hence, a trade-off exists between the privacy of the incumbents and the capacity of the PAL and GAA CBSDs. Further, the PAL and GAA CBSDs must provide their location and other operational details to the SAS during registration, violating their privacy. Thus, we also require schemes that preserve the privacy of PAL and GAA CBSDs without undermining the efficiency of the CBRS architecture.

The privacy of secondary users (SUs) in traditional cognitive radio networks (CRNs) has been a concern, and different schemes have been proposed in the literature. A cloaking-based approach and cryptographic tools have been employed to preserve the location privacy of the SUs in [65,66], respectively. The perturbation of the actual location of the primary users (PUs) and SUs by using the exponential and two-sided Laplacian distribution, respectively, have been proposed to preserve the location privacy of PUs and SUs in [67]. A comprehensive survey on the location privacy of SUs has been provided in [68]. The existing literature on privacy in traditional CRNs has focussed more on SUs. However, the privacy of the incumbents in CBRS demands more attention as they include military radars. Moreover, the technical dissimilarities between CBRS architecture and traditional CRNs limit the proposed schemes' direct extension from traditional CRNs to CBRS architecture. For instance, CBRS is a centralized, database-driven, and three-tier cognitive architecture wherein the CBSDs can determine their operating parameters by querying the SAS. Thus, contrary to the traditional CRNs, CBSDs are not expected to perform spectrum sensing.

Next, we discuss the different schemes that have been proposed in the existing literature to preserve the privacy of incumbents and CBSDs in the CBRS. The existing schemes can be classified into

1. *Obfuscation-based schemes* relying on the addition of the noise or dummy information to create ambiguity in the estimation of the adversary, and
2. *Cryptography-based schemes* employing the cryptographic tools to limit the adversary's access to the incumbents' private details.

Please note that this section only covers the privacy of the operation parameters of the incumbents and CBSDs and does not delve into the security aspects of the CBRS architecture. The WinnForum standard [69] discusses the different threats and requirements for the security of the CBRS architecture. In [70,71], a comprehensive survey on the security aspects of the CBRS. Table 2 classifies the existing literature on the privacy of incumbents and CBSDs in CBRS in *Obfuscation-based schemes* and *Cryptography-based schemes*. Next, we discuss the *Obfuscation based schemes* for preserving the privacy of incumbents and CBSDs in CBRS. Table 3 presents the classification of the obfuscation-based schemes based on the parameter for which privacy has been preserved.

Table 2. Incumbents and CBSDs privacy classification in CBRS.

Obfuscation-Based Schemes	Cryptography-Based Schemes
[10–12,44,59,72], [79–84], [91–96]	[73–78], [85–90], [97]

Table 3. Classification of obfuscation-based schemes for privacy in CBRS.

Parameter	Related Works
Location	[10,44,72,79,80], [81–84,91–93],
Operation Time	[12,59]
Operation Frequency	[11,94,95]

4.1. Obfuscation-Based Schemes

The location privacy of non-stationary incumbents has been studied in [72]. The CBSDs aim to infer the location of the incumbents by sending multiple innocuous queries to the SAS from the locations selected optimally by minimizing the mean estimation error. It has been proposed that the SAS randomly prohibits the transmission of a fraction of the querying CBSDs. However, an optimum value for a fraction of the querying CBSDs needs to be determined. In [79], it has been considered that the CBSDs send innocuous queries from multiple locations and sequentially update the a posteriori probability of the presence of the incumbent in a grid using the Bayesian inference model. It has been proposed that the incumbents can

1. Add random non-positive noise to the transmit power to be allocated to the CBSDs;
2. Change the shape of their protection contours;
3. Enlarge the protection contours by combining the protection contours of other incumbents.

A trade-off between the privacy of incumbents and the CBSDs capacity of the network has been shown through simulations. The location privacy of stationary incumbents has been studied in [10]. Given the knowledge of the method and path loss function used by the SAS to determine the transmit power for a querying CBSD at its location, the adversary aims to infer the location of the incumbents by pretending as a legitimate CBSD and querying the SAS from multiple locations as shown in Figure 7. The performance metric to quantify location privacy is the mean deviation of the location of the incumbent estimated

by the adversary from the ground truth. Two types of adversaries have been considered, which are

1. A random adversary querying from multiple locations selected randomly;
2. A strategic adversary querying from multiple locations selected optimally by minimizing the performance metric.

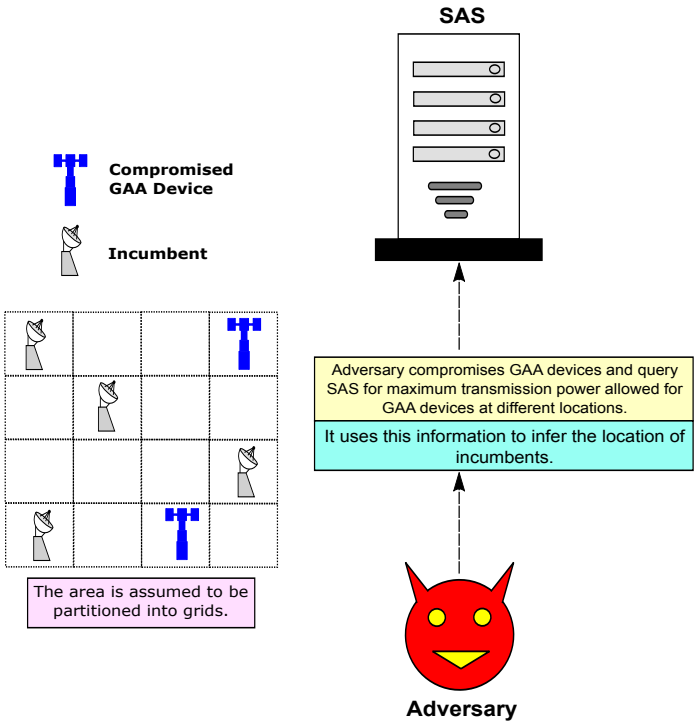

Figure 7. Adversary infers the location of the incumbents.

The authors have proposed that the SAS adds random non-positive noise to the transmit power allocated to the querying CBSD to obfuscate the incumbent's exact location. The optimal solution has been determined by maximizing the mean estimation error while bounding the reduction in the capacity of the CBSDs. An (ω, ε) differential privacy-based scheme has been proposed to preserve the location privacy of incumbents in [80]. The adversary sends multiple innocuous queries and follows a Bayesian inference approach to geo-locate the incumbents. It has been proposed that the SAS generates a conflict graph, obtains the maximum independent set, and utilizes the Hilbert space-filling curve to create the location cloaking set containing the incumbent and non-interfering CBSDs for obfuscating the location of the incumbent. Therefore, the SAS obfuscates the location of incumbents using the locations of CBSDs. A lower bound has been obtained for the size of the location cloaking set. A linear problem has been formulated that minimizes the spectrum efficiency loss by considering the CBSDs as incumbents, while ensuring differential privacy. However, the performance of the proposed scheme needs to be verified for scenarios when all the CBSDs are compromised and incumbents are mobile with different patterns and speeds.

The generation of privacy zone and exclusion zone to preserve the location privacy of the incumbents has been proposed in [81,82]. The area has been divided into grids, and $K-1$ grid cells have been selected uniformly such that the selected grid cells form a contiguous set with the grid cell containing the real incumbent. The total interference in each of the K grid cells has to be below a pre-specified threshold. Therefore, some CBSDs need to cease transmission, whereas some need to reduce their power. A convex problem has been formulated which maximizes the total capacity of CBSDs while imposing a constraint on the privacy of incumbents.

In [44,83], the authors have studied the privacy of location, interference threshold, and reliability threshold (which is the maximum probability of exceeding the interference threshold) for stationary and mobile incumbents. The adversary has been considered to

- Have access to the information exchange between the incumbents and SAS either by hacking the SAS or by eavesdropping on the link between SAS and incumbents;
- Have access to the communication between the SAS and all CBSDs;
- Have access to the allocations made to a subset of CBSDs in the network.

The obfuscation strategies that have been proposed to preserve the privacy of incumbents are

- Insertion of false entries of incumbents into the database;
- Perturbation of resources to be allocated to the CBSDs;
- Addition of uncertainty to the adversary's a priori distribution by making the incumbents' behavior more dynamic.

A generalized problem has been formulated that maximizes the incumbents' utility, while bounding the utility of the CBSDs. The authors have derived a lower bound on the expected time for which the privacy of an incumbent can be maintained. A variation of sequential importance of the selection particle filter has been provided, which an adversary can use to track the location of a stationary and mobile incumbent.

The generation of fake trajectories has been proposed to preserve the privacy of trajectories of mobile incumbents in [84]. The area has been divided into square grids, and a modified Gauss–Markov mobility model has been used to determine the direction of the fake incumbents. The problem of generation of fake trajectories has been modeled as a Markov decision process, wherein the location of CBSDs at timeslot n and locations of real and dummy incumbents at timeslot $n-1$ form the state for timeslot n and the possible locations for the dummy incumbents at the timeslot n specify the action for the timeslot n. The loss in throughput of CBSDs has been considered as the cost, which depends on the state and action for timeslot n. A heuristic for generating fake trajectories has also been provided. However, an insightful discussion on the occurrence (or avoidance) and impact of the potential overlap between different trajectories (real or fake) is still required. Moreover, it needs to be ascertained that the fake trajectories generated through the proposed heuristic are indistinguishable from the real trajectories of the incumbents.

The privacy of location information of static and mobile incumbents against ESC has been studied in [91]. The ESC is required to detect and inform the SAS regarding the activity of the incumbents without learning their whereabouts. It has been proposed that the incumbents create similar radiation patterns leading to similar ESC sensor readings at different locations by utilizing the smart antenna, which can electronically tune the radiation patterns or a mechanical rotating directional antenna that can adjust its transmitting power in different directions. However, the impact of the proposed scheme on the spectrum utilization by the CBSDs needs further investigation. It has been shown in [92] that although the relatively high density of ESC sensors does prove beneficial in meeting the interference thresholds of the incumbents, limiting the false alarms, and hence, providing more spectral opportunities to the CBSDs, but leads to a good resolution of location of the incumbents diluting the privacy shield. Thus, the density of the ESC sensors to be deployed is a crucial parameter that should be decided optimally to achieve desired system performance.

Federated learning and compressed sensing have been utilized to preserve the location privacy of the incumbents. At the same time, ESC sensors detect and inform the SAS regarding the activity of the incumbents in [93]. An honest-but-curios model has been considered for the SAS. It has been proposed that

- The ESC sensors obtain the parameters by performing the local machine learning models;
- The ESC sensors then aggregate the parameters using the compressed sensing and transmit the aggregated signals to the SAS;
- The SAS then optimizes the global parameters and transmits them to the ESC sensors;

- The ESC sensors perform incumbent detection using the global detection method and report the decision to the SAS.

The SAS only receives the aggregated information and cannot decompose the aggregated information to extract the information of any particular ESC sensor. This prevents access of the SAS to the raw samples and preserves the location privacy of the incumbents. The proposed scheme has achieved good detection accuracy for larger training samples ($\sim 10^4$).

In ref. [59], the scheme, termed PriDSS, has been proposed to preserve the privacy of the operation time of incumbents by utilizing differential privacy. The CBSDs provide a bid for using the spectrum, and the database administrator, i.e., SAS selects the set of winner CBSDs that can access without harming the incumbents. Given that the adversary knows the location and transmitting power of the incumbents and CBSDs, it has been shown to infer if any incumbent is inactive by analyzing the different winner sets over time. The adversary has been further shown to identify the inactive incumbent. In the PriDSS scheme, it has been proposed that the SAS selects the winner set by preparing the ranking for the CBSDs and fitting it into the exponential mechanism, which adds obfuscation to the operation time of the incumbents. The PriDSS scheme has been shown to preserve differential operation time privacy. However, the pre-processing step in the proposed PriDSS scheme has been shown to impact the utility of the CBSDs significantly.

It has been proposed that the incumbents transmit dummy signals periodically to preserve the privacy of operation time of incumbents in [12]. The adversary can learn the operation time of the incumbents by hacking into the SAS, compromising all SUs, or eavesdropping on the communication between SAS and CBSDs as presented in Figure 8. The utility of the incumbents has been characterized as the time for which the incumbents transmit the dummy signals. Whereas the utility of the CBSDs has been characterized as the time used by the CBSDs to deliver their traffic. The risk-averse stochastic optimization approach has been followed to study the trade-off, which jointly maximizes the utility of the incumbent and CBSDs while constructing the conflict graph to characterize the interference relations of the CBSDs and modeling the uncertain demands of the CBSDs by the worst-case distribution as the true distribution of demands of the CBSDs is not known. The formulated problem is NP-hard, and a heuristic has been developed for incumbents to determine the optimum time duration for transmitting dummy signals.

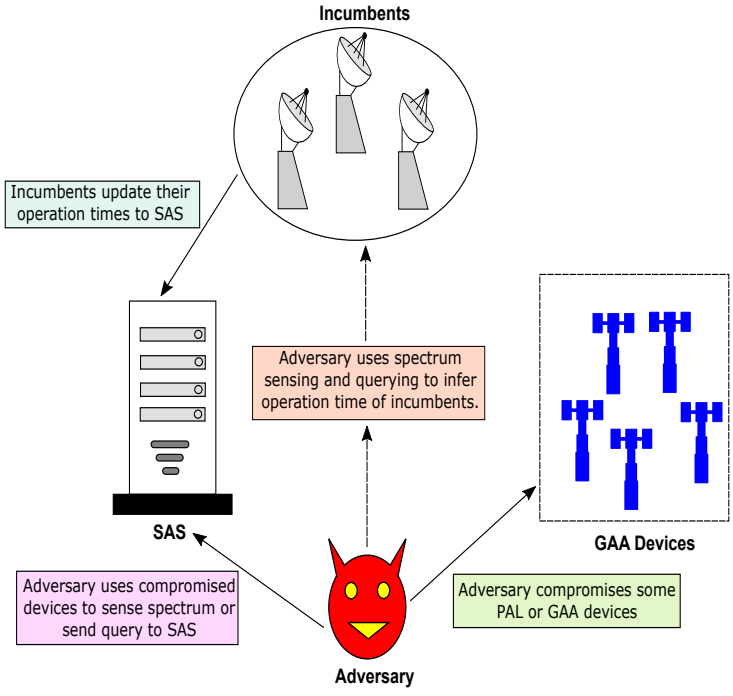

Figure 8. Adversary infers the operation time of the incumbents.

In Figure 9, a violation of operation frequency privacy of the incumbent is illustrated. The authors have studied the privacy of the operation frequency of the incumbents in [94,95]. The adversary is a legitimate CBSD that aims to infer the channels occupied by the incumbents by requesting a channel from the SAS. The SAS responds with an idle channel if available and discards the request; otherwise. Two schemes for the selection of the idle channel have been considered, which are

1. The SAS selects a channel randomly from the set of idle channels available;
2. The SAS orders the channel and selects the lowest available idle channel.

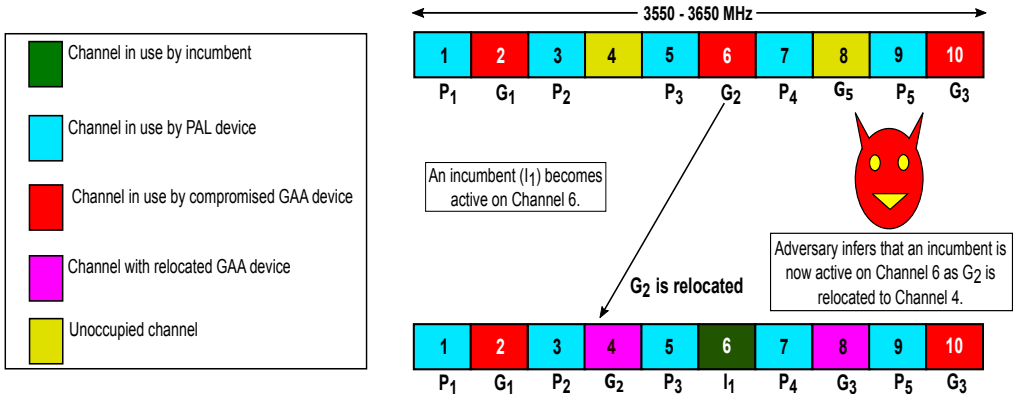

Figure 9. An example of operation frequency privacy violation of the incumbent in CBRS.

The activity of CBSDs has been modeled as an $M/M/l/l$ queue, and the expected number of queries required to infer the operation frequency of incumbents has been calculated for both schemes. The transmission of dummy incumbent signals by the SAS on a channel with probability p to preserve the operation frequency of the incumbent has been proposed in [11]. A GAA CBSD has to shift to another channel if an incumbent becomes active on the channel used by the GAA CBSD. This frequency relocation of the GAA CBSD reveals the operation frequency of the incumbent, especially if the GAA CBSD is compromised. Given that the adversary knows frequency suspension or relocation by compromising some (or all) GAA CBSDs, it intends to jam/eavesdrop on the channel in use by the real incumbent and aims to identify the same correctly. The utility of the incumbents has been characterized as the probability of incorrect identification of the operation frequency of the real incumbent by the adversary. The utility of the GAA CBSDs has been characterized as the expected number of devices transmitting over the band. The optimum value of p has been numerically obtained by studying a trade-off, which maximizes the utility of the GAA CBSDs while maintaining the utility of the incumbents above a threshold. However, the analysis is only limited to incumbents and GAA CBSDs.

The authors have developed a generalized framework to preserve the privacy of operation parameters of the incumbents in [96]. Two cases of adversary have been considered, which are

1. The adversary compromises the CBSDs and observes the assignments made to the CBSDs by the SAS;
2. The adversary hacks the SAS and eavesdrops on the communications between the SAS, ESC, and incumbents.

The adversary then aims to infer the probability distribution of the operation parameters of the incumbents consisting of the location, power, interference threshold, and reliability parameter. The obfuscation strategies which have been considered are

- The inherent noise in the readings of the ESC sensors;
- The false entries of incumbents injected by the military forces;
- The perturbation in the resources allocated by the SAS to the CBSDs.

The optimization problem is then formulated by minimizing the mutual information between the probability distributions of the true and estimated parameters of the incum-

bents, while maintaining the utility of the CBSDs above a certain threshold. The optimal solution is not in closed form and does not have direct practical applicability. A heuristic sampling of the state space and generating the allocation and reporting codebook (ARC) for the incumbents or SAS has been proposed a sub-optimal solution to the formulated problem. The performance of the proposed heuristic has been tested for the location privacy use case, and it has been shown that the ARC closely approximates the optimal solution for small-scale settings. In [98], a generalization of the operation frequency privacy preserving framework in [96] to a more practical three-tier CBRS has been proposed. However, a joint evaluation for the privacy of the location and operational parameters of the incumbents is still required.

4.2. Cryptography-Based Schemes

A multi-server private information retrieval-based scheme has been proposed to preserve the location privacy of the stationary and mobile incumbents and CBSDs in [73,74]. Private information retrieval allows the retrieval of the required information from a database, while preserving the identity of the retrieving user from the database owner. The incumbents and CBSDs have employed the Shamir secret sharing concept to query the multiple synchronized databases to preserve their location privacy. In (t, l) Shamir secret sharing, a secret holder divides a secret and distributes one share each to l parties such that no information is leaked until $t(<l)$ or fewer parties collude. The proposed scheme has been shown to preserve the location privacy of the incumbents and CBSDs against collusion of databases and byzantine attacks on the databases with query end-to-end delay in the order of seconds. A privacy-preserving scheme, termed IP-SAS, has been proposed to preserve the privacy of the operational data of the incumbents in [75]. The scheme involves an additional entity entitled the key distributor, which provides a public/private key pair to the incumbents and CBSDs. The SAS and CBSDs have been considered honest but curious. In IP-SAS, the incumbents encrypt the exclusion zone-based information and send it to the SAS. The SAS utilizes the additive properties of the homomorphic encryption and performs the spectrum allocation to the CBSDs without decrypting the exclusion zone information. It has been shown that the IP-SAS responds to the spectrum request of CBSDs within 1.25 s with a communication overhead of 17.8 KB.

The authors have proposed a P^2-SAS architecture in [76,77], which utilizes the multiparty computation and Pailier cryptosystem to preserve the privacy of the operation data such as location, antenna height, etc., of the incumbents and CBSDs. The architecture involves an additional entity entitled key distributor, which generates the public/private keys and performs ciphertext conversion. The key distributor keeps all of the private keys with itself and ensures that the spectrum allocation happens by performing the computations on the encrypted data. The SAS has been considered honest but curious, whereas the key distributor has been assumed trustworthy. Therefore, the operation data of the incumbents and CBSDs have been hidden from each other and the SAS. The experimental results have shown that the CBSDs request for spectrum is responded to within 6.96 s with communication overhead not exceeding 4 MB. However, the proposed architecture heavily relies on the trustworthiness of the key distributor, which can act as a single point of failure if compromised. A novel privacy-preserving scheme for dynamic spectrum access, termed PriDSA, has been proposed to preserve the location privacy of the incumbents in [78]. The honest-but-curious model has been considered for the SAS. ESC determines the safe zone, wherein the CBSDs are always permitted to transmit and inform the SAS. In pride, the ESC encrypts the safe zone information using the AFGH cryptosystem before sending it to the SAS, and SAS allocates the spectrum using the encrypted information. A blinding factor has been added to upgrade the PriDSA scheme, which preserves the location privacy of the incumbents for the scenario, wherein the SAS turns malicious, colludes with the CBSDs, or both.

A privacy-enhanced scheme for database sharing systems, termed PeDSS, have been proposed to preserve the privacy of the operational data of the incumbents and locations of the CBSDs in [85]. The SAS has been considered honest but curious, and a trusted third party, termed a key distributor, has been introduced, which generates public/private keys for incumbents and CBSDs only during the setup and becomes inactive once the initial setup is complete. The incumbents have proposed that they provide their operational data in encrypted form using homomorphic encryption. CBSDs add random noise to their location, ensuring differential privacy, and the SAS performs spectrum allocation using only the encrypted data. The query processing time for the PeDSS scheme is significantly less than that of the P^2-SAS scheme proposed in [76,77]. However, a detailed investigation on the loss of the utility of CBSDs is still required for the PeDSS scheme.

The authors have proposed a privacy-preserving scheme by leveraging encryption and obfuscation (PSEO) in [86,87], while considering honest and dishonest CBSDs. The dishonest CBSDs can report incorrect identities or lower their transmission power than they plan to use while requesting spectrum access. The privacy threats can occur by eavesdropping on the communications between the SAS, incumbents, and CBSDs and compromising the SAS. The PSEO generates public/private key pairs for all the incumbents and CBSDs using the Paillier cryptosystem, wherein the private key is only known to the belonging entity. The PSEO relies on the blind interference calculation scheme, wherein each CBSD computes its interference budget locally without requiring the information of the incumbents. The obfuscation is added to the encrypted data to control information leakage in case of collusion. Unlike [76], the PSEO performs resource allocation while hiding the operational parameters of incumbents and CBSDs to any entity, including SAS, without any additional entity. PF-PSEO is an addition to the PSEO for dishonest CBSDs, which punishes the dishonest CBSDs by rejecting their requests and later forgives them while considering their reputation scores and reputation history. The experimental results have shown that PSEO and PF-PSEO preserve the privacy of operational data with a reduction in the online overhead. However, the delayed performance of PSEO and PF-PSEO in responding to multiple spectrum requests is unknown.

A distributed CBRS-blockchain model to preserve the privacy of the operation parameters of the GAA CBSDs has been proposed in [88]. In the proposed CBRS-blockchain model, the PAL CBSDs are allocated an additional spectrum so that they can allocate the residual spectrum to the GAA CBSDs. The PAL CBSDs establish independent blockchains, create smart contracts defining the spectrum usage for the GAA CBSDs, and compute their reward by jointly maximizing the local and global number of GAA CBSDs served while fulfilling the capacity requirement of the network. The SAS combines proof-of-strategy consensus with spectrum allocation and regulates the behavior of the PAL CBSDs through the independent blockchains. The ring signature technique has been adopted to preserve the privacy of the operation parameters of the GAA CBSDs. However, it has not been clearly explained if the proposed architecture fulfills the regulations specified for the PAL CBSDs by the FCC, such as a limited spectrum for transmission, the relation between channel assignment and number of licenses issued, etc.

A privacy-preserving architecture, namely *TrustSAS*, to preserve the privacy of operational data of the CBSDs is proposed in [89,90]. *TrustSAS* redesigns the SAS by combining multiple cryptographic blocks and unique properties of blockchain, while adhering to the requirements specified for SAS by the FCC. The architecture of *TrustSAS* consists of

- FCC, which is responsible for generating system keys, authorizing the CBSDs, and ensuring compliance with the regulations;
- Multiple synchronized databases containing smart contracts in each record, which defines the rules of channel usage;
- Multiple CBSDs, which query the SAS for channel allocation.

The CBSDs are clustered into groups, and a leader CBSD is elected for each cluster, which sends and receives information for its cluster. The proposed *TrustSAS* scheme is extremely fast in processing batch spectrum queries compared to [76,86].

The spectrum sharing paradigm, similar to CBRS, involves a dynamic interaction between the SAS, eNBs, and the associated UEs. Therefore, the compliance of the radio context encompassing the system configuration, radio configuration, and location of the UEs to the rules and regulations imposed by the FCC is crucial for properly managing the spectrum. Therefore, we require different schemes to attest to the radio context of the UEs. However, preventing any leakage of the sensitive operational details of the incumbents and SUs while attesting to radio context is highly required. In [97], a scheme entitled PriRoster has been proposed to attest to the radio context of the CBSDs without violating the privacy of incumbents and CBSDs. The SAS, regulatory authority (RA), and local appraiser (LA) are three major entities in the PriRoster, wherein the FCC and eNBs play the roles of RA and LA, respectively. The eNBs use Intel software guard extensions (SGX) to develop a trusted execution environment (TEE), referred to as an enclave, allowing the SAS to verify the identity and securely provide keys to an untrusted host eNBs. RA initiates the radio context attestation procedure by sending a request to the SAS containing a nonce to prevent replay and denial-of-service attacks. The SAS forwards the request to the eNBs, which perform attestation for the associated UEs and respond with the aggregated report. The readers are requested to refer to [70] and the references therein for a deeper understanding of the TEE, SGX, and related concepts.

5. Regulation and Standardization

This section provides the year-wise spectrum sharing initiatives by the National Telecommunications and Information Administration (NTIA) and the Federal Communications Commission (FCC), together with the contribution of other stakeholders (such as WinnForum and CBRS Alliance). We scrutinized policy documents, academic papers, position papers, and analysis reports to gather information on technical and regulatory aspects of the CBRS spectrum sharing regimes.

Figure 10 shows the spectrum management schema in the US. The FCC and NTIA jointly determine spectrum access regulations [72]. They collaboratively decide which spectrum is allocated to Federal users, non-Federal users, and shared users. The NTIA is responsible for managing Federal use of the spectrum, while the FCC is responsible for managing non-Federal use of the spectrum. NTIA and the FCC have to coordinate on the spectrum shared among Federal and non-Federal users.

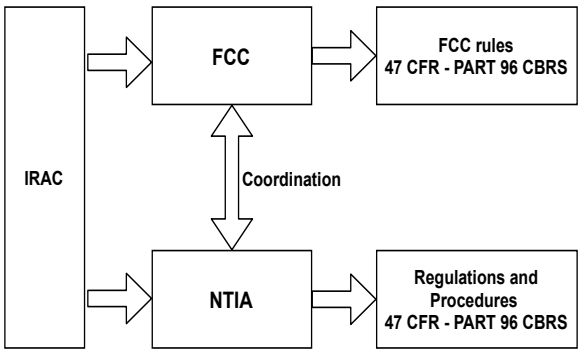

Figure 10. CBRS stakeholders.

In the following, we enlist the CBRS evolution. The roles of involved CBRS stakeholders are given in Table 4. We also provide a summary of CBRS evolution in Table 5.

Table 4. CBRS Stakeholders.

Entity	Roles
NTIA & FCC	They are jointly responsible for spectrum management in the US.
IRAC [99]	Federal agencies provide input to NTIA and FCC deliberations through the Interdepartmental Radio Advisory Committee (IRAC).
47 CFR—PART 96—CBRS [100]	Title 47 Section 96 sets forth the regulations governing the use of devices in CBRS. CBSDs may be used in the frequency bands listed in S:96.11, and their operation shall be coordinated by one or more authorized Spectrum Access Systems (SASs). Similarly, PAL and GAA Users must not cause harmful interference to Incumbent Users and must accept interference from Incumbent Users. At the same time, GAA Users must not cause harmful interference to Priority Access Licensees, and must accept interference from Priority Access Licensees.
3GPP	It defines the 4G and 5G standards used in the CBRS band. Since the CBRS band is technology-neutral, therefore, other access technologies can also be used in this band.
CBRS ALLIANCE	It promotes the adoption of 3GPP technologies in the CBRS band through its members, which include vendors, carriers, service providers and SAS/ESC providers. It also defines specifications and manages the certification program for OnGo. OnGo is the CBRS Alliance created a brand for LTE-based CBRS equipment and its certification program.
WINNFORUM	It focuses on the CRBS spectrum sharing mechanism, testing, and certification.However, its scope is much wider than CBRS. It includes other countries, bands and ways to manage spectrum such as software-defined radio, cognitive radio, and dynamic spectrum access.

- 2010 [101]: The Presidential Memorandum of June 2010 titled "Unleashing the Wireless Broadband Revolution" calls for the National Telecommunications and Information Administration (NTIA), in collaboration with the Federal Communications Commission (FCC), to re-purpose 500 MHz of spectrum from existing Federal and non-Federal uses to wireless broadband use within ten years. The idea was to improve America's economic competitiveness, create jobs, and help maintain America's leadership role in technological innovation. In this context, the US President's Council of Advisors on Science and Technology also released a report titled "Realizing the Full Potential of government-held Spectrum to Spur Economic Growth" on spectrum sharing.
- 2012 [102]: The US President directs the Federal Government to establish a new Federal Spectrum Access System (SAS) using industry partners that will serve as an information and control clearinghouse for band-by-band spectrum registrations and conditions of use and allow non-Federal users to access underutilized spectrum in Federal bands. The SAS will practice the fundamental principle that underutilized spectrum capacity should be used or shared to the greatest extent.
- 2013 [103]: The Presidential Memorandum of June 2013, "Expanding America's Leadership in Wireless Innovation," calls for continued efforts to make more spectra available for wireless broadband applications. The memorandum advocates spectra sharing as an essential means of making more spectra available. In doing so, it sustains the momentum of [2], which made a case for advanced spectrum sharing and called for identifying 1000 MHz of Federal spectra dedicated to pilot projects.
- 2014 [104,105]: FCC proposed the baseline technical standards for the operation of Citizens Broadband Radio Service Devices (CBSDs) and End User Devices in the 3.5 GHz band and general rules for the operation of the SAS and approval of SAS Administrators. The WInnForum created a Spectrum Sharing Committee focused on

implementing the US Federal Communications Commission's regulations for three-tiered spectrum sharing in the 3550–3700 MHz Citizens Broadband Radio Service (CBRS) band. The Committee presently has broad participation from over 60 organizational stakeholders in the new 3.5 GHz band, including wireless operators, Spectrum Access System developers, equipment manufacturers, satellite operators, Wireless Internet Service Providers (WISPs), utilities, the US government, and others.

- 2015 [106]: In April 2015, the FCC formally established a three-tier framework to support making the federal band comprising 3550–3700 MHz, available for shared broadband commercial use under the title the Citizens Broadband Radio Service (CBRS), utilizing the SAS model. The Commission adopted service and technical rules governing the 3.5 GHz band as the new Part 96 of its rules.
- 2016 [104] The FCC completed the regulatory framework and finalized the rules governing the use of the CBRS band, including the finalized specific licensing, technical, and service rules for dynamic sharing between the three tiers of users. Furthermore, the formation of CRBS Alliance initiatives with participation from Access Technologies (Alphabet), Federated Wireless, Intel, Nokia, Qualcomm, and Ruckus Wireless.
- 2017 [107]: To promote additional investment to facilitate 5G network deployment in the CBRS band, the industrial stakeholders (such as CTIA and T-Mobile) filed petitions for rulemaking, which asked the Commission to reexamine several of the Part 96 rules related to PALs. They also proposed several changes to the PAL licensing rules, including much larger license areas, longer license terms, and renewability. The Commission carefully considered input from the various stakeholders to develop an approach that strikes an improved balance among the different use cases for the band.
- 2018 [107]: With the release of the FCC's third Report and Order, the FCC increased PAL license areas to county size and lengthened PAL license terms to 10 years. It is anticipated that adopting similar rules in this band will help promote additional investment in the next generation of wireless services. FCC also adopted changes to the technical rules to facilitate transmissions over wider bandwidth channels without significant power reduction and changes to the information security requirements to safeguard commercially sensitive information better and protect critical infrastructure. It was anticipated that the targeted changes described herein would spur additional investment and broader deployment in the band, promote robust and efficient spectrum use, and help ensure the rapid deployment of advanced wireless technologies (including 5G) in the United States. The FCC and NTIA started the Spectrum Access System (SAS) and Environmental Sensing Capability (ESC) certification process and SAS testing for Amdocs, CommScope, Google, Federated Wireless, and Sony. The FCC announced the establishment of the initial commercial deployments (ICD) process and ESC registration process, and SAS administrators submitted ICD proposals to the FCC. It also issued the first CBSD certifications to Ericsson, Nokia, Sercomm, and Ruckus Networks and the first End-User Device (EUD) certification to Sierra Wireless. The CBRS Alliance published Release 1 of the Network and Coexistence Baseline Specifications and launched the OnGo brand and certification program. WInnForum released the final code for CBSD protocol testing and approved the first six test labs for CBRS standards compliance.
- 2019 [108–110]: The CBRS Baseline Standards Release 1 was created by the WInnForum to address the requirements of 47 CFR (Code for Federal Regulation) Part 96 and develop an ecosystem of interoperable Spectrum Access System and CBRS device technologies. WinnForum approved Nokia, CommScope, Federated Wireless, and Google as CBRS Certified Professional Installer (CPI) Training Program Administrators and Insta, Kyrio, and CommScope as CBRS Root CA Operators. Similarly, FCC approved five SAS administrators: Amdocs, CommScope, Google, Sony, and Federated Wireless.
- 2020 [111–113]: This release 2 of CBRS Baseline Standards by WInnForum is the beginning of bringing new functionality to the CBRS ecosystem, moving beyond the features required for regulatory compliance to the features users, operators, and

suppliers desire to make CBRS more effective for their missions. Throughout 2020, the Forum has continued to expand Release 2 specification enhancements to the baseline CBRS Operational and Functional Requirements. The resulting optional features and functionality can be incorporated at any time, with a special focus on supporting specific vertical markets and their deployments. To address backward compatibility with the WinnForum Release 1 Baseline Standards, the only mandatory feature in Release 2 for a SAS or CBSD is to support the feature-capability exchange between SASs and CBSDs. After 76 rounds, the FCC auction of PAL licenses in the 3550–3650 MHz band was completed on August 25th, 2020, raising more than USD 4.58 billion in bids. The auction made the greatest number of spectrum licenses available in a single FCC auction.

- 2021 [114]: The issuance of PAL Licenses, i.e., SAS support for PAL, is expected by the FCC in 2021. FCC-approved SAS Administrators (Amdocs, CommScope, Federated Wireless, Google, and Sony) have notified the WInnForum that they are working to implement PAL support based on the current FCC rules and established WInnForum standards.
- 2022: The National Advanced Spectrum and Communications Test Network (NASCTN) is hosting a public meeting (https://www.federalregister.gov/documents/2022/07/01/2022-14164/national-advanced-spectrum-and-communications-test-network-citizens-broadband-radio-service-sharing (accessed on 29 November 2022)) on NASCTN's next project, the Citizens Broadband Radio Service (CBRS) Sharing Ecosystem Assessment. This meeting aims to bring together federal, industry, and academic stakeholders to disseminate information about NASCTN's next project. NASCTN's next project, the CBRS Sharing Ecosystem Assessment, seeks to provide data-driven insight into the CBRS sharing ecosystem's effectiveness between commercial and DoD radar systems and to track changes in the spectrum environment over time.

Table 5. CBRS timeline.

Year	Activity
2010	The presidential memorandum called NTIA and FCC to fully utilize the government-held spectrum to spur economic growth.
2012	US President initiated reforming spectrum policy and improve America's wireless infrastructure.
2013	Presidential memorandum giving the FCC a mandate to pursue spectrum-sharing opportunities for the 3.5 GHz band.
2014	The FCC finalized a proposal for the creation of CBRS. WInnForum formed a Spectrum Sharing Committee to develop baseline standards.
2015	The FCC formally released a three-tier CBRS model.
2016	The FCC adopted rules for shared commercial use of the 3550–3700 MHz band, with three-tiered access and authorization framework.
2017	The FCC finalized rules for spectrum sharing in the CBRS band.
2018	The FCC increased PAL license areas to county size and lengthens PAL license terms to 10 years in the 3rd Report and Order. Several standardization initiatives from FCC, NTIA, CBRS Alliance, and WInnForum.
2019	WInnForum released CBRS Baseline Standards (Release 1). Approval of vendors for CBRS Certified Professional Installer (CPI) Training program Administrator and Root CA operator by WInnForum and SAS administrators by FCC.
2020	WInnForum released an enhancement to CBRS Baseline standards (Release 2) [111]. The completion of FCC auction of PAL licenses in August 2020.
2021	The issuance of PAL Licenses is expected by the FCC in 2021. FCC-approved SAS Administrators working to implement PAL support based on the current FCC rules and established WInnForum standards.
2022	NASCTN's next project, the CBRS Sharing Ecosystem Assessment, seeks to provide data-driven insight into the CBRS sharing ecosystem's effectiveness between commercial and DoD radar systems and to track changes in the spectrum environment over time.

6. Discussion

In this section, we discuss the key research limitations of the works presented in this paper. We also highlight possible future research directions for resource allocation, privacy, and some practical implications in CBRS.

6.1. Resource Allocation

Different resource allocation schemes for PAL and GAA devices have been proposed in the literature. The proposed schemes have only focused on allocating resources to PAL and GAA devices without considering load dynamics at the associated user equipment. Further, the existing resource allocation schemes have not suitably considered the participation of mobile network operators in the second tier. Therefore, suitable modifications in the existing resource allocation schemes are required. Further, a proportionally fair joint resource allocation scheme for both second and third-tier is still an open research direction. Stochastic geometry-based modeling of CBRS has been presented in [16], wherein a lower bound on the medium access probability of an unlicensed operator has been analyzed. In a similar direction, the queueing theory and stochastic geometry can be combined to analyze the performance of user equipment in the second and third tier, i.e., the expected latency and queue occupancy of the user equipment can be studied while combining the concepts of server vacation and stochastic geometry. The mobile network operators can utilize the CBRS spectrum in addition to their traditional spectrum. Therefore, developing schemes that promote optimal utilization of both traditional and CBRS spectrum for improving the quality of services by the mobile network operators is another possible research direction.

Beamforming [115], non-orthogonal multiple access (NOMA) [116], and reconfigurable intelligent surface (RIS) [117] have been some promising solutions proposed for various wireless networks in recent years. The use of RIS for boosting the received SINR in the context of spectrum sharing has been recently discussed in [118]. However, NOMA and suitable beamforming for multi-antenna CBRS systems is a relatively unexplored area. Thus, significantly more work is required in future to consider the joint interplay of beamforming, NOMA, and RIS in resource allocation for CBRS.

6.2. Privacy

Different obfuscation-based schemes have been proposed to preserve the location, operation time, and frequency of the incumbents in CBRS. However, most of the proposed schemes have focused on a parameter. The scheme proposed in [96] has attempted to combine different parameters, while preserving the privacy of incumbents. However, the proposed scheme has been evaluated for only location privacy use cases. Further, the scheme is not scalable for a dense network of incumbents, PAL, and GAA devices. Therefore, more research is required to develop schemes that jointly preserve the privacy of location, operation time, and operation frequency of incumbents and are scalable to dense network scenarios. Further, a snapshot-based study of operation time privacy has been conducted in [12,59]. However, a continuous time-based model for operation time privacy of incumbents is required. This is because real incumbents may have a random transmission pattern over time. If dummy incumbents deviate from the pattern of real incumbents, it can be used to segregate the operations of real and dummy incumbents leading to the loss of privacy. Further, the privacy-preserving schemes proposed in the existing literature have considered the traditional data analysis tools for the adversary. Given that the adversary is aware of the presence of dummy incumbents in the system, it can use adversarial machine learning techniques to obtain a more precise estimate of the operation details of the incumbents. Therefore, the design of privacy-preserving schemes considering the adversarial machine learning techniques employed by the adversary is also a possible and open research direction.

The CBRS Sharing Ecosystem Assessment (SEA) project [119] is an ongoing effort that aims to collect suitable data that can be shared with defence organizations to evaluate the co-existence of CBRS with defence radar systems and its effectiveness in spectrum sharing.

It is expected to be a 5 year project out of which the first two stages, namely, proposal screening and test framework development outreach, have been completed. However, three key stages, including the actual testing, Metrology, and Implementation are still pending. Thus, suitable future work is required in actual sensor development and deployment, data analysis, and experiments before a practical CBRS deployment acceptable by both the defence partners and industry is realized.

7. Conclusions

In this article, we have presented an in-depth survey of CBRS. An overview of the CBRS ecosystem has been provided, followed by a discussion on the regulation and standardization process and developments made at the industrial level. We have studied and classified the existing schemes proposed in the literature for optimal spectrum sharing and resource allocation in CBRS. The existing schemes for preserving the privacy of incumbents, PAL devices, and GAA devices in CBRS have been discussed in detail. Lastly, we have discussed the open issues in spectrum sharing and privacy preservation for future research in CBRS.

Author Contributions: Conceptualization, P.A. and M.M.; methodology, P.A. and M.M.; software, P.A. and M.M.; validation, P.A., M.M. and T.A.; formal analysis, P.A., M.M. and T.A.; investigation, P.A. and M.M.; resources, P.A. and M.M.; data curation, P.A., M.M., T.A. and S.T.M.; writing—original draft preparation, P.A., M.M., T.A., S.T.M. and A.Y.; writing—review and editing, P.A., M.M., T.A., A.K. and A.Y.; visualization, S.T.M.; supervision, A.K.; project administration, A.K. and A.Y.; funding acquisition, M.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research receives no external funding.

Acknowledgments: The work of Abhinav Kumar is partially supported by the TiHAN Faculty Fellowship from DST, Government of India.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xie, X.; Rong, B.; Kadoch, M. Explaining 6G Spectrum THz, MmWave, Sub 6, and Low-Band. In *6G Wireless Communications and Mobile Networking*; Xie, X., Rong, B., Kadoch, M., Eds.; Bentham Science Publishers: Sharjah, United Arab Emirates, 2021; pp. 1–22. ISBN 978-1-68-108796-2.
2. Xiao, M.; Mumtaz, S.; Huang, Y.; Dai, L.; Li, Y.; Matthaiou, M.; Karagiannidis, G.K.; Björnson, E.; Yang, K.; Chih-Lin, I.; et al. Millimeter Wave Communications for Future Mobile Networks. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 1909–1935. [CrossRef]
3. Zhang, Z.; Xiao, Y.; Ma, Z.; Xiao, M.; Ding, Z.; Lei, X.; Karagiannidis, G.K.; Fan, P. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. *IEEE Veh. Technol. Mag.* **2019**, *14*, 28–41. [CrossRef]
4. Hassan, M.R.; Karmakar, G.C.; Kamruzzaman, J.; Srinivasan, B. Exclusive Use Spectrum Access Trading Models in Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2192–2231. [CrossRef]
5. In the Matter of Unlicensed Operation in the TV Broadcast Bands, Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band. Available online: https://www.fcc.gov/document/matter-unlicensed-operation-tv-broadcast-bands-additional (accessed on 19 November 2022).
6. FCC Releases Rules for Innovative Spectrum Sharing in 3.5 GHz Band. Available online: https://www.fcc.gov/document/fcc-releases-rules-innovative-spectrum-sharing-35-ghz-band (accessed on 19 November 2022).
7. 47 CFR Part 96—Citizens Broadband Radio Service. Available online: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-D/part-96 (accessed on 19 November 2022).
8. Private LTE Networks. Available online: https://www.qualcomm.com/media/documents/files/private-lte-networks.pdf (accessed on 19 November 2022).
9. CBRS Operational Security. WINNF-TS-0071. Wireless Innovation Forum. Available online: https://cbrs.wirelessinnovation.org/release-1-standards-specifications (accessed on 19 November 2022).
10. Bhattarai, S.; Vaka, P.R.; Park, J.-M. Thwarting Location Inference Attacks in Database-Driven Spectrum Sharing. *IEEE Trans. Cogn. Commun. Netw.* **2018**, *4*, 314–327. [CrossRef]
11. Agarwal, P.; Kumar, A.; Yamaguchi, R.S. Privacy Preserving Scheme for Operating Frequency of Incumbents in Citizens Broadband Radio Service. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11–14 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10.
12. Wang, J.; Errapotu, S.M.; Gong, Y.; Qian, L.; Jantti, R.; Pan, M.; Han, Z. Data-Driven Optimization Based Primary Users' Operational Privacy Preservation. *IEEE Trans. Cogn. Commun. Netw.* **2018**, *4*, 357–367. [CrossRef]

13. Requirements for Commercial Operation in the U.S. 3550–3700 MHz Citizens Broadband Radio Service Band. WINNF-TS-0112. Wireless Innovation Forum. Available online: https://cbrs.wirelessinnovation.org/release-1-standards-specifications (accessed on 19 November 2022).
14. Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS)—Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification. WINNF-TS-0016. Wireless Innovation Forum. Available online: https://cbrs.wirelessinnovation.org/release-1-standards-specifications (accessed on 19 November 2022).
15. Ye, Y.; Wu, D.; Shu, Z.; Qian, Y. Overview of LTE Spectrum Sharing Technologies. *IEEE Access* **2016**, *4*, 8105–8115. [CrossRef]
16. Parida, P.; Dhillon, H.S.; Nuggehalli, P. Stochastic Geometry-Based Modeling and Analysis of Citizens Broadband Radio Service System. *IEEE Access* **2017**, *5*, 7326–7349. [CrossRef]
17. Krishnan, N.N.; Kumbhkar, R.; Mandayam, N.B.; Seskar, I.; Kompella, S. Coexistence of Radar and Communication Systems in CBRS Bands through Downlink Power Control. In Proceedings of the MILCOM 2017, 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 713–718.
18. Manosha, K.B.S.; Matinmikko-Blue, M.; Latva-aho, M. Framework for Spectrum Authorization Elements and Its Application to 5G Micro-Operators. In Proceedings of the 2017 Internet of Things Business Models, Users, and Networks, Copenhagen, Denmark, 23–24 November 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–8.
19. Basnet, S.; Jayawickrama, B.A.; He, Y.; Dutkiewicz, E. Considering Switching Overhead for Transmit Power Allocation for GAA in Spectrum Access System. In Proceedings of the 2017 17th International Symposium on Communications and Information Technologies (ISCIT), Cairns, Australia, 25–27 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.
20. Yin, L.; Li, S.; Zhu, H.; Ma, Y.; Teng, Y.; Liu, H. Reduced-Power Almost Black Subframe Based Pulse Radar Spectrum Sharing for LTE System. *IEEE Trans. Electromagn. Compat.* **2018**, *60*, 1223–1230. [CrossRef]
21. Achatz, R.J. Interference Protection Criteria Simulation. In Proceedings of the 2018 IEEE Radar Conference (RadarConf18), Oklahoma City, OK, USA, 23–27 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 473–477.
22. Krishnan, N.N.; Mandayam, N.; Seskar, I.; Kompella, S. Experiment: Investigating Feasibility of Coexistence of LTE-U with a Rotating Radar in CBRS Bands. In Proceedings of the 2018 IEEE 5G World Forum (5GWF), Silicon Valley, CA, USA, 8–11 July 2018; pp. 65–70.
23. Kliks, A.; Kryszkiewicz, P.; Kulacz, L.; Kowalik, K.; Kolodziejski, M.; Kokkinen, H.; Ojaniemi, J.; Kivinen, A. Spectrum Management Application for Virtualized Wireless Vehicular Networks: A Step Toward Programmable Spectrum Management in Future Wireless Networks. *IEEE Veh. Technol. Mag.* **2018**, *13*, 94–105. [CrossRef]
24. Kang, D.H.; Balachandran, K.; Buchmayer, M. Coexistence Performance of GAA Use Cases Using LTE-TDD Technologies in 3.5GHz CBRS Spectrum. In Proceedings of the 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Republic of Korea, 22–25 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–7.
25. Basnet, S.; Jayawickrama, B.A.; He, Y.; Dutkiewicz, E. Transmit Power Allocation for General Authorized Access in Spectrum Access System Using Carrier Sensing Range. In Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–5.
26. Lees, W.M.; Wunderlich, A.; Jeavons, P.J.; Hale, P.D.; Souryal, M.R. Deep Learning Classification of 3.5-GHz Band Spectrograms with Applications to Spectrum Sensing. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 224–236. [CrossRef]
27. Tarver, C.; Tonnemacher, M.; Chandrasekhar, V.; Chen, H.; Ng, B.L.; Zhang, J.; Cavallaro, J.R.; Camp, J. Enabling a "Use-or-Share" Framework for PAL–GAA Sharing in CBRS Networks via Reinforcement Learning. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 716–729. [CrossRef]
28. Basnet, S.; He, Y.; Dutkiewicz, E.; Jayawickrama, B.A. Resource Allocation in Moving and Fixed General Authorized Access Users in Spectrum Access System. *IEEE Access* **2019**, *7*, 107863–107873. [CrossRef]
29. Kulacz, L.; Kryszkiewicz, P.; Kliks, A.; Bogucka, H.; Ojaniemi, J.; Paavola, J.; Kalliovaara, J.; Kokkinen, H. Coordinated Spectrum Allocation and Coexistence Management in CBRS-SAS Wireless Networks. *IEEE Access* **2019**, *7*, 139294–139316. [CrossRef]
30. Troglia, M.; Melcher, J.; Zheng, Y.; Anthony, D.; Yang, A.; Yang, T. FaIR: Federated Incumbent Detection in CBRS Band. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
31. Gao, W.; Sahoo, A. Performance Study of a GAA-GAA Coexistence Scheme in the CBRS Band. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10.
32. Cui, P.; Chen, S.; Camp, J. GreenLoading: Using the Citizens Band Radio for Energy-Efficient Offloading of Shared Interests. *Comput. Commun.* **2019**, *144*, 66–75. [CrossRef]
33. Jeon, J.; Ford, R.D.; Ratnam, V.V.; Cho, J.; Zhang, J. Coordinated Dynamic Spectrum Sharing for 5G and Beyond Cellular Networks. *IEEE Access* **2019**, *7*, 111592–111604. [CrossRef]
34. Sahoo, A. Fair Resource Allocation in the Citizens Broadband Radio Service Band. In Proceedings of the 2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Piscataway, NJ, USA, 6–9 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–2.
35. Gao, W.; Sahoo, A. Performance Impact of Coexistence Groups in a GAA-GAA Coexistence Scheme in the CBRS Band. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *7*, 184–196. [CrossRef] [PubMed]

36. Cai, M.; Laneman, J.N. Wideband Distributed Spectrum Sharing with Multichannel Immediate Multiple Access. *Analog. Integr. Circ. Sig. Process* **2017**, *91*, 239–255. [CrossRef]
37. Parida, P.; Dhillon, H.S.; Nuggehalli, P. Stochastic Geometry Perspective of Unlicensed Operator in a CBRS System. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), San Francisco, CA, USA, 19–22 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–7.
38. Palola, M.; Hoyhtya, M.; Aho, P.; Mustonen, M.; Kippola, T.; Heikkila, M.; Yrjola, S.; Hartikainen, V.; Tudose, L.; Kivinen, A.; et al. Field Trial of the 3.5 GHz Citizens Broadband Radio Service Governed by a Spectrum Access System (SAS). In Proceedings of the 2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Piscataway, NJ, USA, 6–9 March 2017; IEEE: Piscataway, NJ, USA, 2019; pp. 1–9.
39. Parvez, I.; Khan, T.; Sarwat, A.I.; Parvez, Z. LAA-LTE and WiFi Based Smart Grid Metering Infrastructure in 3.5 GHz Band. In Proceedings of the 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 21–23 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 151–155.
40. Youssef, Z.; Majeed, E.; Mueck, M.D.; Karls, I.; Drewes, C.; Bruck, G.; Jung, P. Performance Enhancement of the CSMA/CA MAC Mechanisms Using a Reject Request to Send (RRTS) Message for 3.5 GHz Shared Spectrum Systems. In Proceedings of the 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–8.
41. Youssef, Z.; Majeed, E.; Mueck, M.D.; Karls, I.; Drewes, C.; Bruck, G.; Jung, P. Concept Design of Medium Access Control for Spectrum Access Systems in 3.5 GHz. In Proceedings of the 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2018; pp. 1–8.
42. Foukas, X.; Marina, M.K.; Kontovasilis, K. Iris: Deep Reinforcement Learning Driven Shared Spectrum Access Architecture for Indoor Neutral-Host Small Cells. *IEEE J. Select. Areas Commun.* **2019**, *37*, 1820–1837. [CrossRef]
43. Sahoo, A.; El Ouni, N.; Shenoy, V. A Study of Timing Constraints and SAS Overload of SAS-CBSD Protocol in the CBRS Band. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
44. Clark, M.A.; Psounis, K. Trading Utility for Privacy in Shared Spectrum Access Systems. IEEE/ACM Trans. *Networking* **2018**, *26*, 259–273. [CrossRef]
45. Sohul, M.M.; Yao, M.; Yang, T.; Reed, J.H. Spectrum Access System for the Citizen Broadband Radio Service. *IEEE Commun. Mag.* **2015**, *53*, 18–25. [CrossRef]
46. Kuester, D.G.; Jacobs, R.T.; Ma, Y.; Coder, J.B. Testing Spectrum Sensing Networks by UAV. In Proceedings of the 2016 United States National Committee of URSI National Radio Science Meeting (USNC-URSI NRSM), Boulder, CO, USA, 6–9 January 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–2.
47. Ghosh, A.; Berry, R.A.; Aggarwal, V. Spectrum Measurement Markets for Tiered Spectrum Access. *IEEE Trans. Cogn. Commun. Netw.* **2018**, *4*, 929–941. [CrossRef]
48. Ghosh, A.; Aggarwal, V.; Chakraborty, P. Tiered Spectrum Measurement Markets for Joint Licensed and Unlicensed Secondary Access. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 1295–1309. [CrossRef]
49. Jo, M.; Chen, X.; Kim, K.S. OP-Map Based Next Generation Frequency Sharing System. In Proceedings of the 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Republic of Korea, 22–25 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–5.
50. Hasan, C.; Marina, M.K. Communication-Free Inter-Operator Interference Management in Shared Spectrum Small Cell Networks. In Proceedings of the 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Republic of Korea, 22–25 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–10.
51. Butt, M.M.; Macaluso, I.; Galiotto, C.; Marchetti, N. Fair Dynamic Spectrum Management in Licensed Shared Access Systems. *IEEE Syst. J.* **2019**, *13*, 2363–2374. [CrossRef]
52. Souryal, M.R.; Nguyen, T.T. Independent Calculation of Move Lists for Incumbent Protection in a Multi-SAS Shared Spectrum Environment. *IEEE Wireless Commun. Lett.* **2021**, *10*, 38–42. [CrossRef]
53. Manosha, K.B.S.; Joshi, S.; Hanninen, T.; Jokinen, M.; Pirinen, P.; Posti, H.; Horneman, K.; Yrjola, S.; Latva-aho, M. A Channel Allocation Algorithm for Citizens Broadband Radio Service/Spectrum Access System. In Proceedings of the 2017 European Conference on Networks and Communications (EuCNC), Oulu, Findland, 12–15 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
54. Ying, X.; Buddhikot, M.M.; Roy, S. SAS-Assisted Coexistence-Aware Dynamic Channel Assignment in CBRS Band. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 6307–6320. [CrossRef]
55. Hiltunen, K.; Matinmikko-Blue, M.; Latva-aho, M. Impact of Interference Between Neighbouring 5G Micro Operators. *Wirel. Pers. Commun.* **2018**, *100*, 127–144. [CrossRef]
56. Souryal, M.R.; Nguyen, T.T. Effect of Federal Incumbent Activity on CBRS Commercial Service. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5.
57. Karaki, R.; Mukherjee, A. Coexistence of Contention-Based General Authorized Access Networks in 3.5 GHz CBRS Band. In Proceedings of the 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), Porto, Portugal, 3–6 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.

58. Tonnemacher, M.; Tarver, C.; Chandrasekhar, V.; Chen, H.; Huang, P.; Ng, B.L.; Charlie Zhang, J.; Cavallaro, J.R.; Camp, J. Opportunistic Channel Access Using Reinforcement Learning in Tiered CBRS Networks. In Proceedings of the 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Republic of Korea, 22–25 October 2018; pp. 1–10.
59. Dong, X.; Gong, Y.; Ma, J.; Guo, Y. Protecting Operation-Time Privacy of Primary Users in Downlink Cognitive Two-Tier Networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 6561–6572. [CrossRef]
60. Tuukkanen, T.; Yrjola, S.; Matinmikko, M.; Ahokangas, P.; Mustonen, M. Armed Forces' Views on Shared Spectrum Access. In Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 15–16 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–8.
61. Palola, M.; Hartikainen, V.; Mäkeläinen, M.; Kippola, T.; Aho, P.; Lähetkangas, K.; Tudose, L.; Kivinen, A.; Joshi, S.; Hallio, J. The first end-to-end live trial of CBRS with carrier aggregation using 3.5 GHz LTE equipment. In Proceedings of the IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Baltimore, MD, USA, 6–9 March 2017; pp. 1–2.
62. Saha, G.; Abouzeid, A.A.; Matinmikko-Blue, M. Online Algorithm for Leasing Wireless Channels in a Three-Tier Spectrum Sharing Framework. *IEEE/ACM Trans. Netw.* **2018**, *26*, 2623–2636. [CrossRef]
63. Xin, C.; Song, M. Analysis of the On-Demand Spectrum Access Architecture for CBRS Cognitive Radio Networks. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 970–978. [CrossRef]
64. Saha, G.; Abouzeid, A.A. Optimal Joint Partitioning and Licensing of Spectrum Bands in Tiered Spectrum Access under Stochastic Market Models. In Proceedings of the 2020 18th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT), Volos, Greece, 15–19 June 2020; pp. 1–8.
65. Xing, L.; Ma, Q.; Gao, J.; Chen, S. An Optimized Algorithm for Protecting Privacy Based on Coordinates Mean Value for Cognitive Radio Networks. *IEEE Access* **2018**, *6*, 21971–21979. [CrossRef]
66. Mao, Y.; Chen, T.; Zhang, Y.; Wang, T.; Zhong, S. Towards Privacy-Preserving Aggregation for Collaborative Spectrum Sensing. *IEEE Trans. Inform. Forensic Secur.* **2017**, *12*, 1483–1493. [CrossRef]
67. Zhang, Z.; Zhang, H.; He, S.; Cheng, P. Bilateral Privacy-Preserving Utility Maximization Protocol in Database-Driven Cognitive Radio Networks. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 236–247. [CrossRef]
68. Grissa, M.; Hamdaoui, B.; Yavuz, A.A. Location Privacy in Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1726–1760. [CrossRef]
69. CBRS Communications Security Technical Specification. WINNF-TS-0065. Wireless Innovation Forum. Available online: https://cbrs.wirelessinnovation.org/release-1-standards-specifications (accessed on 19 November 2022).
70. Shi, S.; Xiao, Y.; Lou, W.; Wang, C.; Li, X.; Hou, Y.T.; Reed, J.H. Challenges and New Directions in Securing Spectrum Access Systems. *IEEE Internet Things J.* **2021**, *8*, 6498–6518. [CrossRef]
71. An, K.; Lin, M.; Ouyang, J.; Zhu, W.-P. Secure Transmission in Cognitive Satellite Terrestrial Networks. *IEEE J. Select. Areas Commun.* **2016**, *34*, 3025–3037. [CrossRef]
72. Vaka, P.R.; Bhattarai, S.; Park, J.-M. Location Privacy of Non-Stationary Incumbent Systems in Spectrum Sharing. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
73. Grissa, M.; Yavuz, A.A.; Hamdaoui, B. Location Privacy in Cognitive Radios With Multi-Server Private Information Retrieval. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 949–962. [CrossRef]
74. Grissa, M.; Yavuz, A.A.; Hamdaoui, B. When the Hammer Meets the Nail: Multi-Server PIR for Database-Driven CRN with Location Privacy Assurance. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017; IEEE: Piscataway, NJ, USA; pp. 1–9.
75. Dou, Y.; Zeng, K.; Yang, Y.; Ren, K. Preserving Incumbent Users' Privacy in Exclusion-Zone-Based Spectrum Access Systems: Poster. In Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, New York City, NY, USA, 3 October 2016; ACM: New York, NY, USA, 2016; pp. 473–474.
76. Dou, Y.; Zeng, K.; Li, H.; Yang, Y.; Gao, B.; Ren, K.; Li, S. P^2-SAS: Privacy-Preserving Centralized Dynamic Spectrum Access System. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 173–187. [CrossRef]
77. Dou, Y.; Zeng, K.; Li, H.; Yang, Y.; Gao, B.; Guan, C.; Ren, K.; Li, S. P^2-SAS: Preserving Users' Privacy in Centralized Dynamic Spectrum Access Systems. In Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Paderborn, Germany, 5 July 2016; ACM: New York, NY, USA, 2016; pp. 321–330.
78. Li, H.; Dou, Y.; Lu, C.; Zabransky, D.; Yang, Y.; Park, J.-M.J. Preserving the Incumbent Users' Location Privacy in the 3.5 GHz Band. In Proceedings of the 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Republic of Korea, 22–25 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–10.
79. Bahrak, B.; Bhattarai, S.; Ullah, A.; Park, J.-M.J.; Reed, J.; Gurney, D. Protecting the Primary Users' Operational Privacy in Spectrum Sharing. In Proceedings of the 2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN), McLean, VA, USA, 1–4 April 2014; pp. 236–247.
80. Liu, J.; Zhang, C.; Lorenzo, B.; Fang, Y. DPavatar: A Real-Time Location Protection Framework for Incumbent Users in Cognitive Radio Networks. *IEEE Trans. Mobile Comput.* **2020**, *19*, 552–565. [CrossRef]

81. Salama, A.M.; Li, M.; Lazos, L.; Xiao, Y.; Krunz, M. On the Privacy and Utility Tradeoff in Database-Assisted Dynamic Spectrum Access. In Proceedings of the 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Republic of Korea, 22–25 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–10.
82. Salama, A.M.; Li, M.; Lazos, L.; Xiao, Y.; Krunz, M. Trading Privacy for Utility in Database-Assisted Dynamic Spectrum Access. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 611–624. [CrossRef]
83. Clark, M.; Psounis, K. Can the Privacy of Primary Networks in Shared Spectrum Be Protected? In Proceedings of the IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 10–14 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–9.
84. He, X.; Jin, R.; Dai, H. Camouflaging Mobile Primary Users in Database-Driven Cognitive Radio Networks. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 21–24. [CrossRef]
85. Li, H.; Yang, Y.; Dou, Y.; Park, J.-M.J.; Ren, K. PeDSS: Privacy Enhanced and Database-Driven Dynamic Spectrum Sharing. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1477–1485.
86. Cheng, Q.; Nguyen, D.N.; Dutkiewicz, E.; Mueck, M. Preserving Honest/Dishonest Users' Operational Privacy with Blind Interference Calculation in Spectrum Sharing System. *IEEE Trans. Mob. Comput.* **2020**, *19*, 2874–2890. [CrossRef]
87. Cheng, Q.; Nguyen, D.N.; Dutkiewicz, E.; Mueck, M.D. Preserving Operational Information in Spectrum Access System with Dishonest Users. In Proceedings of the 2017 17th International Symposium on Communications and Information Technologies (ISCIT), Cairns, Australia, 25–27 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
88. Zhang, H.; Leng, S.; Chai, H. A Blockchain Enhanced Dynamic Spectrum Sharing Model Based on Proof-of-Strategy. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
89. Grissa, M.; Yavuz, A.A.; Hamdaoui, B. TrustSAS: A Trustworthy Spectrum Access System for the 3.5 GHz CBRS Band. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1495–1503.
90. Grissa, M.; Yavuz, A.A.; Hamdaoui, B.; Tirupathi, C. Anonymous Dynamic Spectrum Access and Sharing Mechanisms for the CBRS Band. *IEEE Access* **2021**, *9*, 33860–33879. [CrossRef]
91. Lin, Y.; Ye, Y.; Yang, Y. Preserving Incumbent User's Location Privacy Against Environmental Sensing Capability. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10.
92. Clark, M.; Psounis, K. Designing Sensor Networks to Protect Primary Users in Spectrum Access Systems. In Proceedings of the 2017 13th Annual Conference on Wireless On-Demand Network Systems and Services (WONS), Jackson, WY, USA, 21–24 February 2017; pp. 112–119.
93. Wang, N.; Le, J.; Li, W.; Jiao, L.; Li, Z.; Zeng, K. Privacy Protection and Efficient Incumbent Detection in Spectrum Sharing Based on Federated Learning. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–9.
94. Ben Mosbah, A.; Hall, T.A.; Souryal, M.; Afifi, H. Analysis of the Vulnerability of the Incumbent Frequency to Inference Attacks in Spectrum Sharing. In Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 640–642.
95. Ben Mosbah, A.; Hall, T.A.; Souryal, M.; Afifi, H. An Analytical Model for Inference Attacks on the Incumbent's Frequency in Spectrum Sharing. In Proceedings of the 2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Piscataway, NJ, USA, 6–9 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–2.
96. Clark, M.; Psounis, K. Optimizing Primary User Privacy in Spectrum Sharing Systems. *IEEE/ACM Trans. Netw.* **2020**, *28*, 533–546. [CrossRef]
97. Zhang, R.; Wang, N.; Zhang, N.; Yan, Z.; Lou, W.; Thomas Hou, Y. PriRoster: Privacy-Preserving Radio Context Attestation in Cognitive Radio Networks. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10.
98. Agarwal, P.; Kumar, A.; Yamaguchi, R.S. Preserving Operation Frequency Privacy of Incumbents in CBRS. *IEEE Access* **2022**, *10*, 111022–111041. [CrossRef]
99. Interdepartment Radio Advisory Committee (IRAC). National Telecommunications and Information Administration. Available online: https://www.ntia.doc.gov/page/interdepartment-radio-advisory-committee-irac (accessed on 20 November 2022).
100. CFR 47 CFR 96. Available online: https://ecfr.io/Title-47/Part-96 (accessed on 20 November 2022).
101. The CBRS Commercial Launch, Senza Fili. Available online: https://senzafili.com/reports/cbrs_launch/ (accessed on 13 August 2022).
102. Presidential Memorandum: Unleashing the Wireless Broadband Revolution. Available online: https://obamawhitehouse.archives.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution (accessed on 20 November 2022).
103. Report to the President: Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth. Available online: https://apps.dtic.mil/sti/citations/ADA565091 (accessed on 20 November 2022).

104. Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550–3650 MHz Band. Available online: https://www.federalregister.gov/documents/2016/07/26/2016-14505/amendment-of-the-commissions-rules-with-regard-to-commercial-operations-in-the-3550-3650-mhz-band (accessed on 20 November 2022).
105. FCC Announces NOTICE of Proposed Rulemaking for 3.5 GHz Band Auction, Federal Communications Commission, 23 April 2014. Available online: https://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0425/FCC-14-49A1.pdf (accessed on 20 November 2022).
106. Shared Commercial Operations in the 3550–3650 MHz Band. Available online: https://www.federalregister.gov/documents/2015/06/23/2015-14494/shared-commercial-operations-in-the-3550-3650-mhz-band (accessed on 20 November 2022).
107. Promoting Investment in the 3550–3700 MHz Band. Available online: https://www.federalregister.gov/documents/2018/12/07/2018-25795/promoting-investment-in-the-3550-3700-mhz-band (accessed on 20 November 2022).
108. CBRS Certified Professional Installer (CPI) Training | WInnForum. Available online: https://cbrs.wirelessinnovation.org/cpi-program-administrator (accessed on 20 November 2022).
109. WInnForum Approved CBRS Root CA Operators. Available online: https://cbrs.wirelessinnovation.org/cbrs-root-ca-operators (accessed on 20 November 2022).
110. CBRS Baseline Standards Release 1. Wireless Innovation Forum. Available online: https://cbrs.wirelessinnovation.org/release-1-standards-specifications (accessed on 20 November 2022).
111. Enhancements to Baseline Specifications. Available online: https://cbrs.wirelessinnovation.org/enhancements-to-baseline-specifications (accessed on 20 November 2022).
112. PAL (CBRS) Auction Closes with 4.58*B* in Bids. *Connected Real Estate Magazine*, 27 August 2020.
113. FCC Announces Winning Bidders of 3.5 GHz Band Auction. Available online: https://www.fcc.gov/document/fcc-announces-winning-bidders-35-ghz-band-auction (accessed on 20 November 2022).
114. Inside the CBRS Ecosystem. Available online: https://cbrs.wirelessinnovation.org/cbrs-status-summary (accessed on 20 November 2022).
115. Lin, Z.; An, K.; Niu, H.; Hu, Y.; Chatzinotas, S.; Zheng, G.; Wang, J. SLNR-Based Secure Energy Efficient Beamforming in Multibeam Satellite Systems. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, 1–4. [CrossRef]
116. Lin, Z.; Lin, M.; Wang, J.-B.; de Cola, T.; Wang, J. Joint Beamforming and Power Allocation for Satellite-Terrestrial Integrated Networks with Non-Orthogonal Multiple Access. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 657–670. [CrossRef]
117. Lin, Z.; Niu, H.; An, K.; Wang, Y.; Zheng, G.; Chatzinotas, S.; Hu, Y. Refracting RIS-Aided Hybrid Satellite-Terrestrial Relay Networks: Joint Beamforming Design and Optimization. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 3717–3724. [CrossRef]
118. Tian, Z.; Chen, Z.; Wang, M.; Jia, Y.; Dai, L; Jin, S. Reconfigurable Intelligent Surface Empowered Optimization for Spectrum Sharing: Scenarios and Methods. *IEEE Veh. Technol. Mag.* **2022**. [CrossRef]
119. CBRS Sharing Ecosystem Assessment. Available online: https://www.nist.gov/programs-projects/cbrs-sharing-ecosystem-assessment (accessed on 20 November 2022).