Cognitive Computation (2022) 14:475–510
https://doi.org/10.1007/s12559-021-09969-9

Differential Privacy in Cognitive Radio Networks: A Comprehensive Survey

Muneeb Ul Hassan[1] · Mubashir Husain Rehmani[2] · Maaz Rehan[3] · Jinjun Chen[1]

Received: 25 July 2021 / Accepted: 21 November 2021 / Published online: 28 January 2022

Abstract

Integrating cognitive radio (CR) with traditional wireless networks is helping solve the problem of spectrum scarcity in an efficient manner. The opportunistic and dynamic spectrum access features of CR provide the functionality to its unlicensed users to utilize the underutilized spectrum at the time of need because CR nodes can sense vacant bands of spectrum and can also access them to carry out communication. Various capabilities of CR nodes depend upon efficient and continuous reporting of data with each other and centralized base stations, which in turn can cause leakage in privacy. Experimental studies have shown that the privacy of CR users can be compromised easily during the cognition cycle, because they are knowingly or unknowingly sharing various personally identifiable information (PII), such as location, device ID, signal status, etc. In order to preserve this privacy leakage, various privacy preserving strategies have been developed by researchers, and according to us differential privacy is the most significant among them. In this article, we provide a thorough survey on how differential privacy can play an active role in preserving privacy of cognitive radio networks (CRN). Firstly, we provide a thorough comparison of our work with other similar studies to show its novelty and contribution, and afterwards, we provide a thorough analysis from the perspective of various CR scenarios which can cause privacy leakage. After that, we carry out an in-depth assessment from the perspective of integration of differential privacy at different levels of CRN. Then, we discuss various parameters which should be considered while integrating differential privacy in CRN alongside providing a comprehensive discussion about all integrations of differential privacy carried out till date. Finally, we provide discussion about prospective applications, challenges, and future research directions. The discussion about integration of differential privacy in different CR scenarios indicates that differential privacy is one of the most viable mechanisms to preserve privacy of CRN in modern day scenarios. From the discussion in the article, it is evident that the proposed integration of differential privacy can pave the way for futuristic CRN in which CR users will be able to share information during the cognition cycle without the risk of losing their private information.

Keywords Differential Privacy (DP) · Cognitive Radio Networks (CRN) · Privacy in communication

Introduction

The exponential surge in the usage of hand-held Internet of Things (IoT) devices caused a huge rise in wireless traffic. Statista report revealed that the number of hand-held mobile devices is projected to reach up to 17.72 billion by the end of the year 2024 [1]. This surge is causing an irregular usage of spectrum, which is further responsible to cause the issue of 'artificial spectrum scarcity' [2]. Similarly, the worldwide analysis and measurement of spectrum utilization revealed that only 5-10 % of wireless spectrum is being used by licensed/authorized users [3]. All these factors lead researchers to investigate mechanisms which provide spectrum efficiency, and cognitive radio (CR) is one of them. Cognitive

✉ Mubashir Husain Rehmani
mshrehmani@gmail.com

Muneeb Ul Hassan
muneebmh1@gmail.com

Maaz Rehan
maazrehan@gmail.com

Jinjun Chen
jinjun.chen@gmail.com

[1] Swinburne University of Technology, Hawthorn VIC 3122, Australia

[2] Munster Technological University (MTU), Munster, Ireland

[3] Wah Campus, COMSATS University Islamabad, Islamabad, Pakistan

radio is a widely accepted model for efficient spectrum utilization [4]. CR was first coined by J. Mitola in 1999. CR is an ambiance-aware intelligent wireless system which can dynamically adapt changes depending upon its surrounding RF environment [5]. CR works over the principle of allowing CR users (also known as Secondary Users (SUs)), to access spectrum of licensed users (also known as Primary Users (PUs)), during idle time. This functionality of CR allows SUs to exploit underutilized bands of spectrum without causing any harmful inference to the communication of PUs [6]. Thus, SUs can dynamically access available spaces in the spectrum band in order to manage it efficiently [7, 8].

To dynamically access the spectrum, SUs need to follow complete cycle which involve spectrum sensing (SS), spectrum analysis, and spectrum adaptation (also known as exploitation) [9]. SUs repeatedly carry out these functions in order to achieve the desired environmental conditions. (A detailed explanation of functioning of CRN is provided in "Fundamentals of Differential Privacy in Cognitive Radio Networks".) All other functions, for example, spectrum auction (used to decide winner of spectrum allocation), etc., can be taken as a subvariant of the above-mentioned basic tasks. These functionalities help SUs to find and select the best possible spectrum band in order to carry out seamless communication. Since these steps involve transmission of SUs data, these steps can be exploited by adversaries to infer their personal data. For instance, multiple SUs are collected during collaborative spectrum sensing (CSS) by a fusion centre (FC) to get the best spectrum results. However, this FC can also become an adversary and exploit private data of CR users [10]. Similarly, in case of spectrum auction, the centralized auctioneer can exploit the bidding privacy (BP) because it has all data of multiple SUs and PUs from the bidding perspective. Therefore, it is important to protect the privacy of CR users by integrating some external privacy preservation mechanisms.

In the quest of providing privacy in CRN, extensive research has been carried out by researchers to integrate different privacy preservation strategies with CRN. For example, some works [11, 12] proposed the use of anonymization techniques such as *k-anonymity* to preserve privacy of CR users. Similarly, some other works [15–17] analysed the use of encryption to preserve privacy. Certain works [18–21] investigated the use of private information retrieval to protect private CR data. Alongside these techniques, some works also highlight the use of obfuscation-based privacy (also known as differential privacy) to preserve CR users' privacy. Among all these mechanisms we believe that differential privacy is one of the most viable mechanisms to protect the privacy of CR users because of its dynamic and adaptive nature.

The notion of differential privacy was first discussed by Cynthia Dwork in 2006 in order to protect privacy of statistical databases by adding random independent and identically distributed (i.i.d) noise in the data [22]. However, afterwards researchers working in the field of private CRN tried integrating this differential privacy notion with CRN at different aspects and they got fruitful results. Since then, plenty of works highlighting the integration of differential privacy with CRN have been carried out in the literature. In this paper, we provide a thorough survey regarding integration of differential privacy at various scenarios of CRN in order to demonstrate the useful benefits that one can get via this integration. Similarly, we try to discuss various technical works that have already carried out this integration and published their work in the literature.

Key Contributions of Our Survey Article

Nevertheless, certain surveys from the perspective of security and location privacy of CRN have been presented in the literature, but a specific survey that highlights the need, integration, functioning, and applications of differential privacy in CRN has not been presented yet. In this article, we carry out survey of state-of-the-art works involving the integration of differential privacy and CRN alongside providing certain use cases which can be beneficial for future researchers who are interested to explore this field further. To conclude, the key contributions of our article are as follows:

- We carry out comparative comparison of our survey article with previously published survey literature.
- We provide an in-depth analysis over the scenarios in which privacy of CRN can be compromised.
- We provide a thorough analysis from the perspective of integration of differential privacy at different levels of CRN. Alongside this, we also in-depth survey of all state-of-the-art integrations involving differential privacy and CRN.
- We provide a comprehensive analysis of parameters which should be considered while incorporating differential privacy in CRN models.
- We highlight various challenges, open issues, and prospective future directions for researchers and scientists interested to explore the field of differentially private CRN.

Related Survey Works

A comprehensive literature is available in the field of CRN; however, the aspect of privacy preservation in CRN is not much discussed and only a very few surveys are available in this field. Similarly, this presented survey work is different from other surveys in a context that it discusses the integration, design requirements, functioning, and applications of differential privacy in CRN. To the best of our knowledge, there is no prior work which covers multiple aspects of differential privacy in CRN. None of the works discussed integration of differential privacy in cognitive cycles; therefore, we develop certain comparison matrices such as discussion about differential privacy, location privacy (LP), trading privacy (TP), SS privacy (SSP), and sources of privacy leakage (SoPL). A comprehensive comparison of our survey with other surveys, based on the aforementioned parameters, is presented in Table 1.

The first work discussing vulnerabilities of CRN from the perspective of security, privacy, and deployment threats have been presented by Bhattacharjee et al. [11]. The authors first describe various architectural aspects of CRN focusing weak links having security and privacy threats. Afterwards, they discuss threats and vulnerabilities that CRN can face if they are attacked by some adversary. A brief book purely targeting location privacy of CRN have been presented by Wang and Zhang [12]. The work first highlights certain privacy preservation mechanisms, and then discuss the integration of privacy mechanisms in CRN. The major focus of the work is location privacy leakage during CSS and during database driven CRN. Another comprehensive survey discussing the security threats and defences in CRN have been carried out by Sharma and Rawat [2]. The work focuses over highlighting security vulnerabilities in different layers of CRN. The article started with discussion of CRN physical layer, then discusses security threats in upper and cross-layer CRN. Finally, authors provide in-depth insights on how game theory can play the role in enhancing the security of CRN.

Another survey by Grissa et al. [10] focuses location privacy leakage and its mitigation techniques in CRN. This work first discusses the sources of CRN which may cause privacy leakage, then presents CRN privacy preservation mechanisms, and finally states CRN location privacy methods of spectrum discovery along with attack scenarios. One more work providing an in-depth classification of security threats of physical layer of CRN is presented by Hamamreh et al. [13]. The article first classifies security techniques of CRN physical layer and then presents its detailed applications. Another similar article discussing the basics, detection, functioning, and countermeasures of physical layer threats of CRN have been presented by Salahdine and Kaabouch [14]. The work first classifies all physical layer attacks in CRN, then classifies and discusses attack detection techniques and the possible countermeasures.

However, considering this discussion and after analysing all possible surveys presenting privacy preservation in CRN, it can be concluded that the prevailing literature does not give an in-depth knowledge and analysis of differential privacy in CRN. Our presented work is the first one that covers integration of differential privacy with CRN from an in-depth technical perspective.

Overview of the Article

A brief list of acronyms used in our survey article is given in Table 2. The rest of the article is structured as follows: "Fundamentals of Differential Privacy in Cognitive Radio

Table 1 Summary of Related Survey Articles with their Contribution, and Various Scopes such as Differential Privacy (DP), Location Privacy (LP), Trading Privacy (TP), Spectrum Sensing Privacy (SSP), and Sources of Privacy Leakage (SoPL). Tick(✓) Shows that the mentioned topic is covered, Cross(✗) shows that the provided domain is not covered, and Asterisk(✻) shows that the particular topic is partially covered

					Scope				
Major Domain	**Ref.**	**Year**	**Type**	**Contribution Summary**	**DP**	**LP**	**TP**	**SSP**	**SoPL**
Cognitive Radio Networks Vulnerabilities	[11]	2013	Survey	Comprehensive survey on security concerns and prospective threats linked to deployment of CRN	✗	✻	✗	✗	✻
Location Privacy in CRN	[12]	2014	Book	Provided an extensive survey on location privacy and its mitigation strategies in CRN.	✓	✓	✗	✻	✻
Security Threats & Defences in CRN	[2]	2015	Survey	Carried out a detailed survey on threats & countermeasures of secure for both primary & secondary CRN users.	✗	✻	✗	✻	✻
Location Privacy in CRN	[10]	2017	Survey	A comprehensive survey on leakage sources and mitigation strategies for location privacy in CRN.	✻	✓	✻	✻	✓
Physical Layer Security	[13]	2019	Survey	Extensively classified security techniques and applications for CRN physical layer.	✗	✗	✗	✗	✗
Physical Layer Security	[14]	2020	Survey	A thorough discussion and analyzation of security attacks on physical layer of CRN is provided.	✗	✻	✗	✗	✗
Differential Privacy in CRN	This Work	2020	Survey	A state-of-the-art survey on privacy leakage of CRN along with extensive evaluation from the perspective of integration of differential privacy in CRN.	✓	✓	✓	✓	✓

Networks" provides a brief discussion about fundamental concepts and preliminaries of article from the perspective of differential privacy, CR, and sources of privacy leakage. Afterwards, "Scenarios of Privacy Leakage During Cognitive Cycle and Prospective Role of Differential Privacy" provides an in-depth discussion about integration of differential privacy with CRN in different CR scenario. After that "Performance Matrices for Evaluating Differentially Private CRN Mechanisms" talks about various performance matrices that can be used to evaluate integration of differentially private approaches in CRN scenarios. Then, "Differential Privacy Approaches for Cognitive Radio Networks" carries out an extensive survey of all technical works that have integrated differential privacy in CRN. Afterwards, "Applicability of Differential Privacy in Futuristic Cognitive Radios" provides in-depth discussion about applicability of CRN in various futuristic scenarios and applications. Similarly, "Challenges and Future Research Directions" provides insights about possible challenges and prospective future research directions. Finally, the article is concluded in "Conclusion".

Fundamentals of Differential Privacy in Cognitive Radio Networks

Since CRN serve as a viable solution to overcome spectrum scarcity issue, these have therefore been integrated with many domains, for example, smart grid, IoT, multimedia transmission, transportation systems, healthcare and other [23]. Although CR provides amazing features, it also has an issue of privacy leakage. Thus, CRN privacy protection is also an important aspect that needs to be taken care of while implementing this paradigm. In this section, fundamental concepts of our survey such as CRN, differential privacy, importance of privacy in CRN, privacy threats, and sources of privacy leakage in CRN are discussed.

Table 2 List of Acronyms Used in the Article

Acronyms	Definitions
BP	Bidding Privacy
CR	Cognitive Radio
CRN	Cognitive Radio Networks
CSS	Collaborative Spectrum Sensing
DP	Differential Privacy
FC	Fusion Centre
IU	Incumbent User
IoT	Internet of Things
LP	Location Privacy
PU	Primary User
RF	Radio Frequency
SU	Secondary User
SVM	Support Vector Machine
SSP	Spectrum Sensing Privacy
SS	Spectrum Sensing
SoPL	Sources of Privacy Leakage
TP	Trading Privacy

Cognitive Radio and its Preliminaries

Discussion about is further categorized into five different aspects: (i) spectrum bands, (ii) CRN users, (iii) white space exploitation and utilization, (iv) CRN cognitive cycle, and (v) SS.

Licensed and Unlicensed Bands of Spectrum

Spectrum band, also known as frequency band, is used to carry out communication between devices, and the band is widespread and ranges between 9 KHz to 3 THz depending upon the type of application [24]. The spectrum bands can be further subdivided into licensed spectrum band and unlicensed spectrum band [25]. The licensed band is allocated to licensed users who have paid licensing fees. These users can use the allocation frequency at any time without any inference and interruption. The licensed bands are usually allocated to telecom/Internet companies via auctions, who further allocate the bands to their customers [26]. Contrarily, unlicensed spectrum bands have been excluded from auction-based sale/international licensing; therefore, these bands are used to carry out low-cost communication. These bands are limited and their users are pretty large; therefore, these bands face the issue of heavy inference. Since a large base of users compete for these unlicensed bands, National Authorities regulating these bands carry out a conventional auction to manage these bands [24]. In this way, these authorities allocate a high paying user a fixed spectrum band and they can use it as a licensed user. An analysis indicates that the utilization of these bands greatly varies depending upon the geographical region. For example, the overall utilization is 85% at some places while it is 15% at other places [27]. This underutilization of spectrum leads to the formation of large unused white spaces, which gets wasted. To overcome this spectrum wastage, researchers are getting benefit from the dynamic spectrum access functionality of CRN, through which CR users can access the unoccupied spectrum band and can leave at the time of PU activity.

Primary & Secondary Cognitive Radio Users

The underutilization of spectrum can be controlled and reduced with the help of CRN with very minimal level of inference to licensed users. CRN mainly comprises of two types of users. First one is known as primary users (PUs), who are licensed and can access the spectrum at any time without any permission. The second type of users are secondary users (SUs), also known as CR users, who are unlicensed and can only access spectrum when it is unoccupied. SUs have to leave the spectrum in case PU arrives [28]. CR users continuously sense the activity of PUs on the network and always look for white spaces. Once an SU finds a white space, it moves to it and starts utilizing it for communication. In this way, SUs help to overcome the issue of spectrum underutilization in an efficient manner.

White Space Utilization

CR is an intelligent radio, which changes and adapts to the changes according to environment. Similarly, extensive research has been carried out in order to efficiently utilize the underutilized spectrum. Generally, CRN can be further subdivided into three paradigms on the basis of their spectrum utilization [29]. First type of CRN is interweave CRN, where CRN continuously senses the activity of PUs and access the network only when it is vacant. These are conventional CRN, which wait for the spectrum to become idle. Second type of CRN is underlay CRN, which allows CR users to carry out operations alongside PU activity if the inference caused by CR users is less than a specific threshold value. Third type of CRN is overlay, in which CR users overhear the continuous PUs transmissions and then use sophisticated algorithms of signal processing to enhance PUs performance, and in turn they get some additional patch of bandwidth which they can use to carry out their own transmission.

Cognitive Cycle for White Space Exploitation

The spectrum utilization and exploitation phenomenon of CRN works in a stepwise manner, which is also known as the cognitive cycle. The cycle comprises four functional steps in which CR performs different actions to access spectrum in the most efficient manner. The steps of the cycle are sensing, analysis, sharing, and mobility [30]. The details of these steps are given as follows:

- **Spectrum sensing** is the first step in the cognitive cycle. Through SS, CR nodes carry out efficient detection of spectrum opportunities around themselves in order to develop an initial idea of which spectrum band to access.
- **Spectrum analysis** is the next step in which SUs select the best spectrum band from the available bands. The values collected via SS are used in spectrum analysis to choose a band in which inference to PUs is minimum and utilization is maximum.
- **Spectrum sharing** is the third step in the cognitive cycle which is used to exploit the chosen spectrum for communication. In this step, the decision of choosing the appropriate CR model (such as interweave, underlay, or overlay) is taken on the basis of data collected from previous two steps. At the end of this step, CR nodes can carry out transmission of their data via the selected spectrum band.
- **Spectrum mobility** is the final step in the cognitive cycle and it involves the immediate mobility of SU nodes after detection of PUs. As the name suggests, this step is responsible for making the spectrum available to PUs by vacating the activity of SUs in case if PU returns to resume its activity.

Similarly, a figure to demonstrate functioning of the cognition cycle for CRN is provided in Fig. 2.

Spectrum Sensing and Access

Since a large proportion of researchers focus on the integration of differential privacy during SS and access, let’s demonstrate these steps in a bit detail for better understanding.

Collaborative Spectrum Sensing Usually, SS in CRN is carried out in a collaborative manner, in which all CR nodes collaborate with each other to generate the best SS outcome. This collaborative sensing is carried out to overcome the issue of shadowing of PU. For instance, if a PU is present on the rooftop of a high building and SU is on the ground level, then the presence or absence of PU cannot be sensed with precision using a normal sensing mechanism due to low signal-to-noise ratio (SNR) of the signal received from PU [31]. To overcome this issue of fading, multiple CR users collaborate with each other to carry out SS to ensure that they do not miss any specific PU. This whole process of collaborative sensing is done with the help of a centralized data collection centre called FC. Generally speaking, FC collects data from all CRN and determines the final values regarding presence or absence of PU in a particular region.

Database-Driven Spectrum Access According to database-driven spectrum access, data administrations are considered responsible for keeping up to date knowledge of spectrum and whitespaces in order to provide SUs with the most beneficial information [32]. A selected database collects necessary information from PUs including their usage times, tolerable inference, available channels, allowed power transmission, and other useful information. This information is then forwarded to SUs upon request, and the decision of joining or leaving a specific spectrum band is taken on the basis of this information.

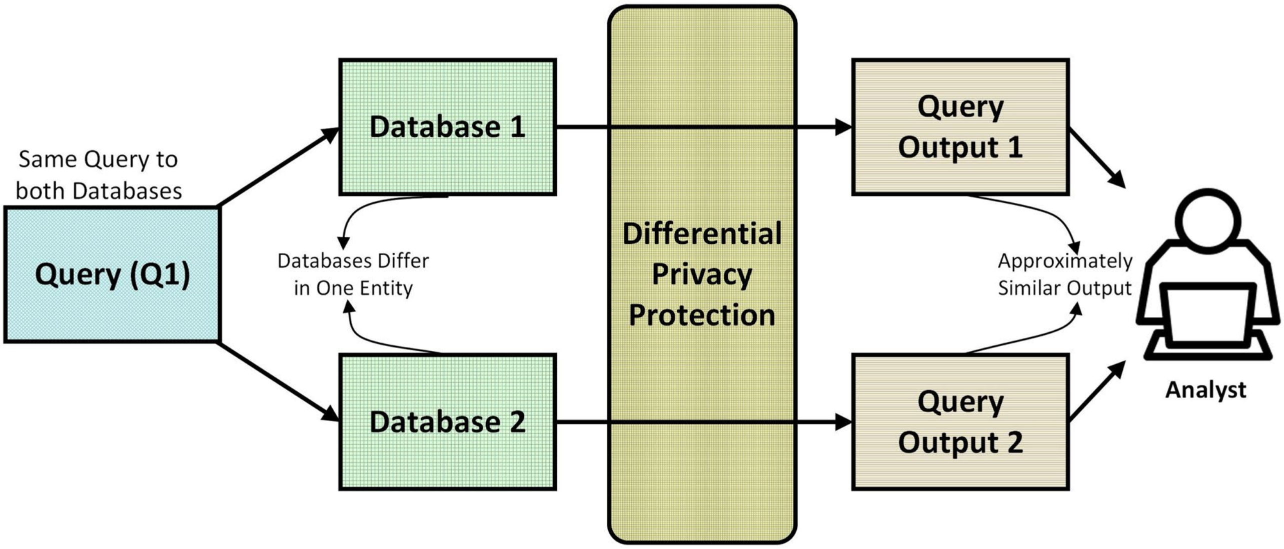
Same Query to both Databases
Query (Q1)
Database 1
Database 2
Databases Differ in One Entity
Differential Privacy Protection
Query Output 1
Query Output 2
Approximately Similar Output
Analyst

Fig. 1 A Graphical Illustration of Functioning of Differential Privacy Mechanism in Two Adjacent Databases (adapted from [22])

Differential Privacy

The perception of differential privacy as a medium to protect database privacy was first proposed by Cynthia Dwork in 2006 [22]. This notion was later used by researchers in almost every field to protect the privacy of their participants. For example, in auction, differential privacy has been used in auction to protect bid privacy. Similarly, it has been used in SS to protect location privacy. To summarize, it will not be wrong to say that differential privacy is being applied to all real-life domains ranging from statistical databases to real-time decision analysis [33]. The formal definition of differential privacy from the perspective of two adjacent datasets x and x' is as follows [34]:

$$P_R[R(x) \in O_p] \leq \exp \varepsilon x P_R[R(x') \in O_p] \tag{1}$$

In the above equation, R is the randomized differentially private algorithm, x and x' are two adjacent datasets, P_R is the probability value for an outcome O_p to be in range of function $Range(R)$. Furthermore, ε is privacy parameter which is also known as privacy budget. The value of ε is used to control the amount of noise which is going to be added in query result.

Alongside ε, sensitivity is the other parameter that plays an important role in determining noise value. Sensitivity can be defined as the maximum difference an observer can get from the result of a query applied to two adjacent datasets x and x'. The formal definition of sensitivity can be defined as follows [35]:

$$\Delta S_q = \underset{x,x^p rime}{max} ||f(x) - f(x')|| \tag{2}$$

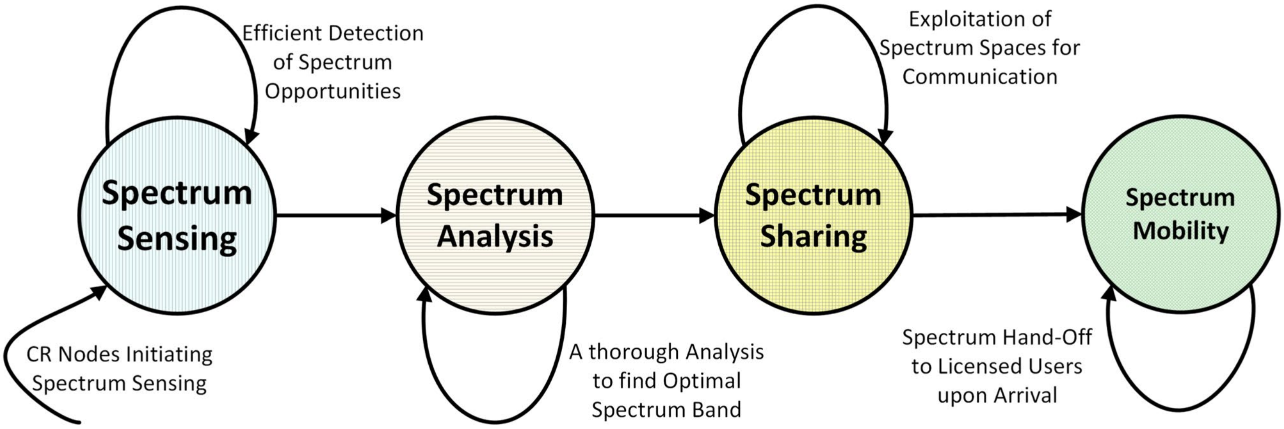
Efficient Detection of Spectrum Opportunities
Exploitation of Spectrum Spaces for Communication
Spectrum Sensing
Spectrum Analysis
Spectrum Sharing
Spectrum Mobility
CR Nodes Initiating Spectrum Sensing
A thorough Analysis to find Optimal Spectrum Band
Spectrum Hand-Off to Licensed Users upon Arrival

Fig. 2 A Graphical Illustration of Functioning of Cognition Cycle for CR Nodes (adapted from [27])

Furthermore, various mechanisms of differential privacy have been proposed to calculate noise, and the two most famous among them are Laplace and Exponential. These two use the pseudorandom noise generated from their respective database to perturb the query output. A detailed discussion of differential privacy from the perspective of mechanisms, composition theorem, sensitivity, and privacy budget can be found in [36]. Moreover, an illustrative explanation of differential privacy is provided in Fig. 1.

Importance of Privacy Protection in CRN

Despite great advantages by CRN, they do suffer from a serious threat related to the privacy of its users. As discussed in the previous section, CR nodes have to sense the spectrum in order to generate the environment map of PUs [37]. Similarly, queries and spectrum auctions are also carried out by FC to access and trade spectrum. However, while doing all these tasks, CR participating nodes have to report numerous amounts of data to FC. Although FCs are usually trusted entities, in certain cases such as when there is an adversarial attack on FC, the privacy of CR participants can be compromised [38]. For instance, the location of SUs and PUs can be compromised which can lead to serious consequences. Similarly, the PUs and SUs usage and occupancy times can be analysed for malicious purposes. Similar to that, bidding and asking prices can be analysed by adversaries for unethical actions. Some of the key benchmarks from the perspective of differential privacy and CRN have been presented in Table 3. (Detailed discussion on privacy sources and their countermeasures using differential privacy is given in "Scenarios of Privacy Leakage During Cognitive Cycle and Prospective Role of Differential Privacy")

Adversary Models in CRN

CR is a diversified network; it therefore faces numerous types of adversarial attacks. In this section, we categorize privacy-related adversaries into four subtypes which cover approximately all types of adversarial attacks. The discussion about these adversaries is as follows:

External Adversary

This type is one of the most prominent and dangerous as compared to others. The adversary in this type includes any type of external intruder who is interested to get insights about the network in order to fulfil malicious objectives. For example, this adversary could be an external pharmaceutical company who is interested in finding out the number of CR users who visit hospitals/pharmacies frequently. They will do so by compromising the location of PUs and SU. This company will collect all required information and can-do targeted advertisements. Usually, these adversaries operate in two ways, either compromised communication link or via compromised database.

Compromised Communication Link In this case, adversaries try to attack the communication link between SU/PU and central authority (usually FC). In this way, these adversaries try to overhear the communication between SU and FC to infer their private information. One way is to launch man-in-the-middle attack [39] on the communication link, thus adversaries can get required private information. Similarly, another attack in this type is exogenous attack [2], in which an external adversary tries to jam the whole CR network to carry out malicious operations during this time.

Compromised Database The second type of attack by external adversaries could be in the form of compromising the FC database. In this attack, adversaries try to carry out a direct attack on FC database to get personal information of participants including topology map of PUs and SUs [40]. This type of attack is usually carried out in database-driven CRN. In collaborative sensing, this can also be done by intruding attack [2], where an intruder tries to get into the network externally by masquerading itself as a regular CR

Table 3 Benchmarks achieved from the perspective of differential privacy, cognitive radio networks, and their integration

1999	[5]	J. Mitola coined the concept of cognitive radio as a dynamic and intelligent radio.
2006	[22]	C. Dwork introduced the notion of differential privacy to protect private data during queries.
2007	[95]	H. Celebi highlighted the need of privacy preservation in location-aware CRN.
2008	[96]	N.R. Prasad discussed security & privacy concerns in CRN alongside proposing a secure authentication framework.
2012	[63]	S. Li worked over preserving location privacy during collaborative spectrum sensing of CRN via differential privacy.
2014	[12]	W. Wei wrote a comprehensive book on preserving location privacy for CRN.
2014	[51]	R. Zhu integrated differential privacy in spectrum trading auction of CRN.
2014	[97]	W. Wang preserved CR sensing privacy leakage attacks via differential privacy in multi-service provider scenarios.
2017	[10]	Mohamed wrote a detailed survey article on the issue of location privacy leakage in cognition cycle of CRN.
2018	[53]	X. Dong introduced a differentially private notion to protect operation time privacy of primary users.
2019	[98]	F. Hu worked over development of differentially private matching-based double auction in spectrum trading.

user, either for getting private information of CR nodes, or to inject falsified information in the network.

SUs Acting as Adversary

Alongside external adversaries, sometimes SUs can also act as adversaries and can play the role in compromising privacy of other CR participants. Similar to the intruding attack discussed in the above section, sometimes legitimate SUs can also act as adversaries and try to leak into the privacy of other SUs, PUs, and FC by collecting unnecessary data during cognitive cycle [10]. Nowadays there is a trend of decentralized sensing via blockchain, and all SUs try to reach a consensus in a decentralized manner [41]. This decentralized consensus is a great way to remove FCs, but it can also cause privacy issues because information reported by SUs is publicly visible to all other SUs, which can lead to harmful effects.

PUs Acting as Adversary

Apart from SUs, sometimes, PUs can also act as adversaries. This rarely occurring case cannot be ignored especially in the case of spectrum auction and trading. Since PUs are the authorities having excessive spectrum to sell, they also have objectives to enhance their revenue. Some PUs therefore try to analyse the bids of SUs and try to take certain actions through which they could increase their revenue in a tactical way [42].

Service/Fusion Centre Acting as Adversary

The fourth type of adversary in our CRN modelling is centralized data centre-based adversary, which are also known as FCs. These FCs are usually trusted central entities and are designed to collect information from SUs during SS process to get the best spectrum. However, in some cases these FCs become adversaries. For example, FCs can sell the private data of their associated SUs and PUs to advertising organizations to earn extra profit. Similarly, these FCs can also analyse the data in a malicious way, which can even lead to the development of certain policies that may impact a certain group of participants.

This discussion concludes that efficient privacy preserving mechanisms are required to protect CRN from these types of adversaries. In this perspective, differential privacy provides a strong privacy guarantee, which can be used to protect the privacy of CR users.

Motivation of Using Differential Privacy in CRN

Privacy preservation in wireless systems is a well-established field, and extensive research has been carried out in this regard [43]. In this section, a comparative analysis of these privacy preservation strategies with differential privacy has been presented.

Encryption-Based Privacy Protection

Since the advent of cryptography, encryption is being used to protect information in almost all fields of life [44]. Therefore, it will not be wrong to state that encryption-based privacy is the most traditional means to protect the privacy of any network/application. Encryption works over the phenomenon of key-based cryptography, in which a message is encrypted by a CR sender and then it is sent to CR receiver [45]. The receiver has the key which is used to decrypt the message. The message in its encrypted form is known as ciphertext, which is unreadable and can only be decrypted by the person having the secret key. In this way, the message is protected from external intruders who cannot tap into the private communication of CR users.

Although, encryption provides strong privacy against external adversaries, but it is not an efficient privacy protection mechanism when internal participants become adversaries. According to our already discussed adversary models, encryption will only be helpful against external adversaries, but will not be much useful against the other three adversaries. There are certain encryption mechanisms which require strong computational power and a specific architecture for encryption [46]. Such computational efficiency is hard to obtain in small CR nodes. Contrarily, differential privacy provides both these features, as it provides privacy protection from internal adversaries and is computationally less-expensive as compared to encryption.

Oblivious Transfer-Based Privacy

Oblivious transfer (OT) is also a popular means to protect privacy of CR nodes nowadays because it allows CR senders to send a message in multiple patches [10]. In this mechanism, a message is broken down into multiple segments during transmission, which are then received and reassembled at the receiver as a single message. This approach is being used as a viable approach to carry out SS tasks in order to find out available spectrum without compromising communication privacy. However, this mechanism suffers from similar issues of encryption-based privacy.

Firstly, OT can only preserve privacy against external intruders, but cannot protect it from internal intruders. Secondly, the computational and communication overhead of this mechanism is quite high as compared to other mechanisms because multiple messages are transmitted at the same time, which incur high communication overhead due to collision, cohesion, and redundant rebroadcasts. Differential privacy is, however, free from these issues, because the

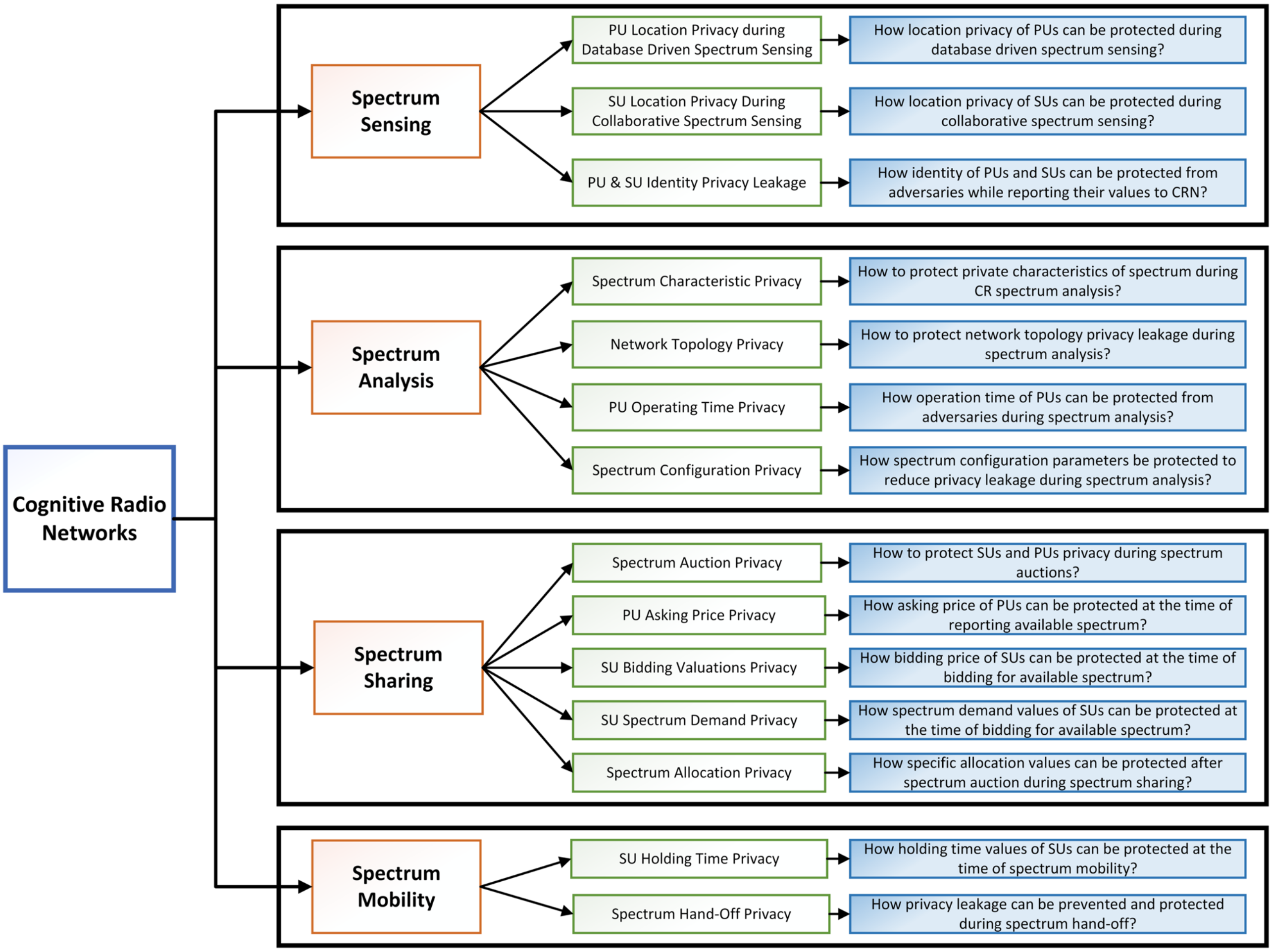
Cognitive Radio Networks
Spectrum Sensing
PU Location Privacy during Database Driven Spectrum Sensing
How location privacy of PUs can be protected during database driven spectrum sensing?
SU Location Privacy During Collaborative Spectrum Sensing
How location privacy of SUs can be protected during collaborative spectrum sensing?
PU & SU Identity Privacy Leakage
How identity of PUs and SUs can be protected from adversaries while reporting their values to CRN?
Spectrum Analysis
Spectrum Characteristic Privacy
How to protect private characteristics of spectrum during CR spectrum analysis?
Network Topology Privacy
How to protect network topology privacy leakage during spectrum analysis?
PU Operating Time Privacy
How operation time of PUs can be protected from adversaries during spectrum analysis?
Spectrum Configuration Privacy
How spectrum configuration parameters be protected to reduce privacy leakage during spectrum analysis?
Spectrum Sharing
Spectrum Auction Privacy
How to protect SUs and PUs privacy during spectrum auctions?
PU Asking Price Privacy
How asking price of PUs can be protected at the time of reporting available spectrum?
SU Bidding Valuations Privacy
How bidding price of SUs can be protected at the time of bidding for available spectrum?
SU Spectrum Demand Privacy
How spectrum demand values of SUs can be protected at the time of bidding for available spectrum?
Spectrum Allocation Privacy
How specific allocation values can be protected after spectrum auction during spectrum sharing?
Spectrum Mobility
SU Holding Time Privacy
How holding time values of SUs can be protected at the time of spectrum mobility?
Spectrum Hand-Off Privacy
How privacy leakage can be prevented and protected during spectrum hand-off?

Fig. 3 Graphical Illustration of Sources of Privacy Leakage in Cognitive Cycle of Cognitive Radio Networks

computational and communication overhead of differentially private messages is quite minimal, and it also provides protection from internal intruders.

Data Anonymization-Based Privacy

Data anonymization is also a famous privacy preservation strategy which is being used to protect privacy during query evaluation of CR nodes [47]. In anonymization-based privacy, a dataset is anonymized by removing pseudoidentifiable information from data before making it available for query evaluation. For instance, in CRN, FC can remove names and IDs of PUs before making the dataset available to SUs for database drive spectrum access.

This mechanism provides an effective solution for certain internal adversaries, but continuous experimentations have revealed that anonymized datasets can also be deanonymized by carrying out various linking attacks [48, 49]. Similarly, finding the best combination to remove from the dataset is also difficult, e.g. for some participants, coverage area could be confidential but not for others. Therefore, developing a consensus among participants on pseudoidentifiable information is also tough. A major drawback of anonymization in CRN is that it requires a large database to operate, and in case if the database is not significantly big, then it can leak privacy. Contrary to all these aspects, differential privacy provides a dynamic mechanism which can be used to provide efficient privacy in these scenarios. Firstly, it is hard to identify the data protected via differential privacy due to its strong privacy guarantee. Secondly, differential privacy does not always require a large database, because pointwise differential privacy mechanism can also protect a single entity generated by CR nodes.

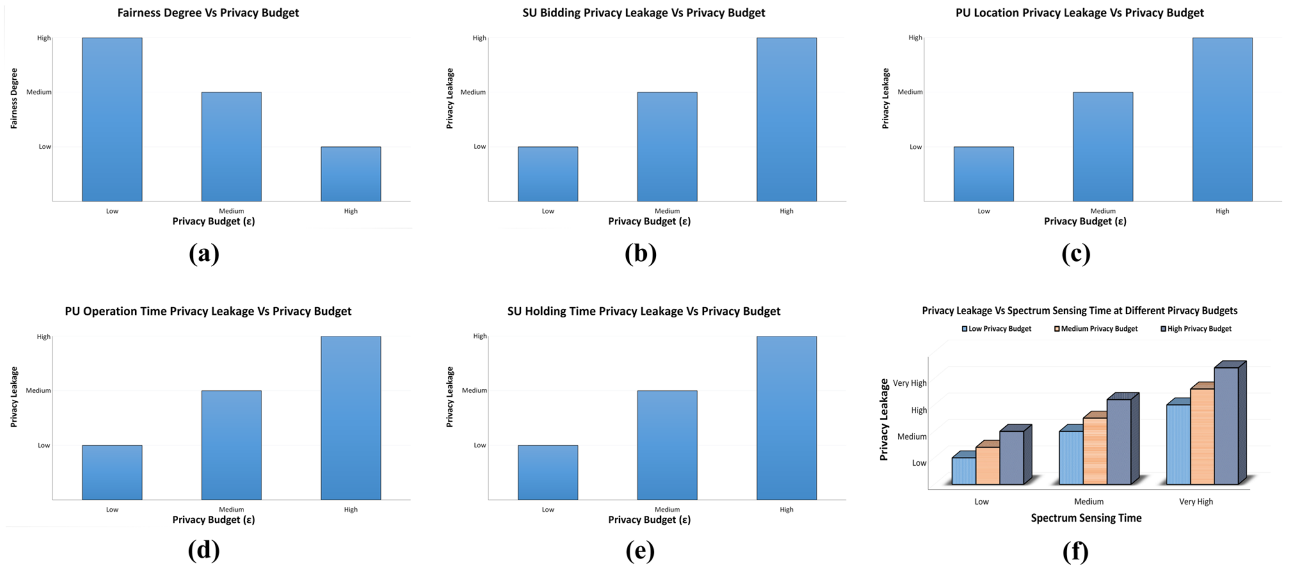

Fig. 4 Intuitive Analysis of Privacy Leakage in Various CR Scenarios at Different Privacy Budget (ε) Values. (**a**) Fairness Degree Vs Privacy Budget (adapted from [50]) (**b**) SU Bidding Privacy Leakage Vs Privacy Budget (adapted from [51]) (**c**) PU Location Privacy Leakage Vs Privacy Budget (adapted from [52]) (**d**) PU Operation Time Privacy Leakage Vs Privacy Budget (adapted from [53]) (**e**) SU Holding Time Privacy Leakage Vs Privacy Budget (adapted from [54]) (**f**) Privacy Leakage Vs Spectrum Sensing Time at Different Epsilon (adapted from [55])

Scenarios of Privacy Leakage During Cognitive Cycle and Prospective Role of Differential Privacy

In the previous section, a thorough discussion regarding the importance of privacy preservation in CRN from the perspective of SUs, PUs, and other involved participants is provided. Moving further to classification, we discuss major sources of privacy leakage in CRN alongside an in-depth analysis of how differential privacy can play its role in preserving privacy. The sources are further categorized into four subtypes on the basis of four major steps of cognitive cycle. An illustration of sources is also provided in Fig. 3. Moreover, in order to provide our readers an intuitive overview of privacy leakage with respect to various prominent CR scenarios (such as fairness degree, SU bidding privacy, PU location privacy, PU operation time privacy, SU holding time privacy, and privacy in spectrum sensing time), we develop certain intuitive graphs, which have been presented in Fig. 4.

Privacy Leakage Scenarios During Spectrum Sensing

SS is considered as a key functionality of CRN, as it provides information about available spectrum, which is the core for Dynamic Spectrum Access (DSA). SS in CR is performed by SUs in order to detect spectrum holes which they use to carry out cognitive communication. The CRN environment is highly mobile and at certain times immediate decisions need to be taken in order to utilize the spectrum in the most efficient manner. Therefore, the aspects of accuracy, efficiency, timeliness, and decision making cannot be ignored [56]. In order to make quick decisions, a fine-grained data of participating nodes in CRN which provides efficiency on one hand, but on the other leaks the privacy of participants at multiple standpoints [57]. In this section, possible scenarios that can leak privacy during SS of CRN are discussed.

PU Location Privacy from Databases-Driven Access

According to General Data Protection Regulation (GDPR), location is a personal information and location of any participant/node cannot be traced without their approval [58]. Similarly, Federal Communications Commission (FCC) has also made it mandatory to preserve location privacy of PU nodes while designing CRN sensing techniques [59]. Database-driven CRN works over the phenomenon of query evaluation-based spectrum access. It can easily be analysed that multiple queries from FC database can leak privacy of PUs who are involved in SS. For instance, an adversary can try to launch multiple queries from database which collectively form a location inference attack. For example, if there is a single PU with name ‘X’ in a region ‘Y’, then the first query could be to find the number of PUs operating under a specific band (this will be done to find out the availability of spectrum). Similarly, the second query could be to find out the number of PUs in this specific region. Afterwards, the next query could be, for example, to find out the name of PU organization by saying ‘how many PUs have ‘X’ in their name’. In this way, via multiple queries one can easily identify the presence and availability of a PU in a region. This can lead to harmful consequences because other attacks can be launched to exploit such identified PUs. Therefore, location privacy of PUs during database-driven DSA should be protected.

Prospective Role of Differential Privacy: Since database-driven DSA works over the phenomenon of query evaluation, this location privacy issue of PU nodes can easily be protected via differential privacy. As differential privacy was designed to protect privacy of statistical databases [60], it can be applied here to protect location privacy of PUs at the time of query evaluation. For instance, at the time of query from FC, a pseudorandom noise generated from differential privacy distribution can be added into query output to ensure the randomness in the query output. However, the utility can also be maintained by controlling the privacy budget (ε) to a desired range [61]. Therefore, integration of differential privacy during query evaluation of database-driven DSA can effectively protect location privacy of PU nodes.

SU Location Privacy During Collaborative Sensing

SS is not only harmful for the privacy of PUs, but also poses a risk to the privacy of SUs location [62]. In CSS, all SU nodes have to report the sensed values to centralized FC. This collaboration results in an efficient and trustworthy sensing, but this also poses a high risk to the location privacy of SU nodes. For instance, untrusted, or compromised SUs can act as adversaries to locate the exact location of other SUs on the basis of the values received for SS [63]. For instance, location leakage of an SU can result in tracking of daily life activities of a particular SU. Therefore, considering the catastrophic outcomes of location privacy leakage, SUs are also concerned about their privacy protection. Considering this discussion, it can be concluded that privacy of SUs should be protected during CSS.

Prospective Role of Differential Privacy: Since SS in a collaborative manner is a critical aspect of CRN, it cannot be ignored. Therefore, protecting privacy during CSS is pretty important. Differential privacy is a randomization technique which can protect privacy from statistical databases to real-time reporting and it can be protected using pointwise differential privacy. Pointwise differential privacy means that any individual instance of data can be protected by adding pseudorandom noise from differential privacy distribution [64]. Usually, Laplace and Gaussian distributions are used to carry out pointwise perturbation of differential privacy. Similarly, if one adds a pseudorandom noise to protect location privacy of CR node at the time of SS, its privacy can easily be preserved. Plenty of research is carried out to integrate the phenomenon of differential privacy in location reporting [65]. The need here is to integrate this dynamic concept in the reporting aspect of SS in CRN.

Identity Privacy Leakage During Crowdsourced Sensing

Alongside location privacy leakage, another significantly important parameter is identity of PU and SUs. We briefly discussed this identity in query evaluation, but it is important to mention it separately as well, especially in the case of crowdsourced SS. Since crowdsourced SS is a combined activity, all CR nodes have to perform their best in order to get optimum results. As all nodes share the information, this may lead to identity theft in case of an adversarial attack. For example, an adversarial node can pretend to be some other node if it gets to know all identity parameters of other nodes. In this way, many malicious acts can be carried out, ranging from adversarial decisions to DoS attacks. Therefore, it is important to protect identity privacy in SS alongside preserving location privacy.

Prospective Role of Differential Privacy: In crowdsourced SS, the most important parameter to protect is identity of the sensing node, because this identity can further be backtracked to locate the specific node. However, at certain phases it is also important to check identity in order to ensure the integrity of the sensing report. Differential privacy is a strong privacy guarantee that can also be used to protect privacy leakage in case of identity theft-based attacks [66]. For instance, differential privacy can be combined with other provable encryption or proofing mechanisms to provide a provable identity alongside preserving the actual values [67]. The similar concept can easily be applied for CR nodes during the aspect of SS. Therefore, we believe adding calibrated differentially private noise with provable security mechanisms can be a viable solution to preserve identity theft privacy during crowdsourced SS.

Privacy Leakage Scenarios During Spectrum Analysis

Spectrum analysis comes after SS and is used to select an available spectrum [68]. Similarly, the decision of bidding/trading for any specific spectrum is also taken on the basis of results from this step [69]. Spectrum analysis is broadly divided into two steps named as characterization and reconfiguration. First, the prospective scenarios in spectrum analysis which can become the source of privacy leakage are discussed and afterwards the role of differential privacy to overcome these leakages have been presented.

PU Privacy in Spectrum Characterization

After successful SS, SUs possess information about PUs and the available spectrum band which they can use to choose the most suitable. The scrutiny process is called spectrum characterization and it works as follows. After collecting all data from the sensing step, a list of spectrum bands is formulated involving various parameters such as path loss, RF environment, holding time, error rate, and switching delay [70]. These parameters are then used by SUs to determine the best available spectrum. This process helps in the in-depth spectrum analysis but also leaks privacy. For example, the fine-grained values, for example error rate and RF environment, can easily be used to identify the private characteristics of PUs. Thus, privacy of PUs during characterization needs to be protected.

Prospective Role of Differential Privacy: Differential privacy is an advanced privacy protection mechanism which can be used to protect privacy during the characterization process. Firstly, differential privacy can be used to obfuscate the identity values so that the identity does not get leaked during characterization. Secondly, differential privacy obfuscation can further be applied to parametric values on the basis of requirement. For example, a margin of error can be ignored in error rate or a margin of error in path loss can also be tolerated. So, the dynamic differential privacy algorithm can take advantage of this marginal error and can perturb data within this range in order to ensure privacy along with significant utility.

Privacy Leakage in Learning Network Topology

Similar to spectrum characteristics, network topology also carries private information in it. For instance, the geolocation of nodes can easily be inferred in case of unprotected network topology. In case of an adversarial attack on CRN, the adversary node may try to infer and collect all possible information collected via sensing, and after this inferring, the adversarial opponent may try to get much deeper insights about network topology [71]. This is done in order to find out the exact location of all PU nodes in the network. In case if the adversary successfully gets this personal information, then it can launch all attacks associated with location privacy, as discussed above. Therefore, it is important to protect privacy of network topology before publishing data during spectrum analysis.

Prospective Role of Differential Privacy: Since network topology depends upon multiple aspects, such as geo-location and signal strength, they are combined together to form a complete topology. To protect privacy during network topology formation, one therefore needs to protect individual parameters. The obfuscation of differential privacy can efficiently protect this by adding pseudorandom pointwise noise to all parameters individually while considering the overall network utility [72].

PU Operation Time Privacy

During spectrum characterization, an aspect of operation time cannot be ignored from a privacy viewpoint. Operation time is the total activity time of primary user, which is also known as primary user activity time [73]. Usually, during development of CR mechanisms researchers use various PU activity models to analyse the mechanism behaviour [74]. These PU models are used to determine the presence, absence, and functioning of PU nodes. However, in real-life scenarios, if one has this much fine-grained information about activity and presence of any node, then it can cause serious consequences to its privacy. For instance, if an adversary has fine-grained information about PU activity, it can easily infer a daily schedule. For example, if an adversary is active then it means it is at a particular place, and if the spectrum band is unused, then the licensed user must be sleeping or doing other tasks. This data is fed into machine/deep learning models, which further train themselves and try to predict the accurate lifestyle. Therefore, privacy of PU operation time needs to be protected before sharing this information to SU nodes.

Prospective Role of Differential Privacy: Protecting real-time lifestyle privacy is one of the key roles of differential privacy. Due to this advantage, differential privacy is being used by researchers in multiple aspects, for example, protecting privacy real-time smart metering data, protecting privacy of real-time EVs data [36]. Similarly, this aspect can also be applied to protect PU operation time privacy. For example, PU operation time values can be perturbed using differentially private noise from the distribution, and this noise can be calibrated according to privacy budget and data sensitivity.

Spectrum Reconfiguration Parameter Privacy

After successful categorization of desired channel, the step of spectrum reconfiguration arises in which parameters of the transceiver of SU are configured according to the given condition [75]. This involves configuration of power, bandwidth, frequency, and other communication technologies. Although these are important parameters, which need to be configured properly, they in return can also leak privacy. For example, power control parameters can be used to figure out signal-to-interference ratio (SINR), which can further be used to geo-locate the particular SU. Therefore, it is important to protect privacy of these parameters as well at the time of system reconfiguration.

Prospective Role of Differential Privacy: Differential privacy is a viable solution to protect the configuration data. Since certain configuration parameters, for example frequency and values, are pretty strict and cannot be changed, thus, in such cases differential privacy can be combined with some provable mechanism to ensure privacy [66]. Furthermore, in case of parameters which can bear some noise or error, pointwise differential privacy can be integrated to protect their privacy.

Privacy Leakage Scenarios During Spectrum Sharing

Spectrum sharing/decision is the third step after spectrum analysis, this step is further divided into three major steps involving allocation of resources, accessing of spectrum, and trading of spectrum [76]. To demonstrate it further, after spectrum analysis, CR nodes have the choice to choose the best available spectrum, and in order to do so, they first participate in spectrum trading to win the best available spectrum slot. Afterwards, the desired resource is allocated to them by FC or by some other server, and after completion of these two steps, they can access the spectrum for communication. These steps involve plenty of informational parameter exchange, which can lead to CR users. In this section, various cases of privacy leakage in scenarios involving spectrum sharing have been discussed.

Privacy Leakage in Spectrum Auctions

Spectrum auction is a whole new world involving mathematical models. For instance, game theory has been applied to it to achieve better results during auctions [77]. Similarly, for the majority of auctions, equilibrium is usually evaluated to get best results [78]. Alongside this, machine learning is also being applied to spectrum auctions to predict best outcomes [79]. Since this step has been explored a lot, the risk of privacy leakage has also increased a lot, and plenty of attacks on auction mechanisms have been developed in the past. In this section, we also discuss certain sub aspects of auctions such as BP.

Prospective Role of Differential Privacy: Since spectrum auctions are vulnerable to privacy attacks, privacy preservation is required during this process. To preserve auction privacy, differential privacy obfuscation is a viable solution because with differentially private auctions, one can still enhance social welfare of auction alongside preserving differential privacy. Similarly, in case of spectrum auctions, differential privacy can be used to protect privacy of both SUs and PUs acting as spectrum sellers and buyers, respectively. (A detailed discussion about these mechanisms is given in "Differential Privacy Approaches for Cognitive Radio Networks".)

PU Asking Price Privacy

Submitting available spectrum slots alongside asking prices is one of the first step of the auction process. In this step PU node submits the available spectrum value alongside its asking price to FC or centralized server, which is further displayed to CR nodes to collect bids [80]. However, these values are critical, as they contain information about PU spectrum usage, and an adversary can get insights that when a PU is vacant, or occupied. By this analysis, the adversary can plan an adversarial activity or can launch an attack on the basis of previous knowledge. Similarly, an adversary can get insights about financial condition/dependencies of PU on the basis of total spectrum band and the price he asked for it. Therefore, it is important to protect asking price privacy before publicizing these values.

Prospective Role of Differential Privacy: Exponential shuffling, a mechanism of differential privacy can be used to introduce randomness in asking price string [81]. Similarly, the Laplace mechanism of differential privacy can be used to protect the privacy of asking price while managing social welfare of the complete auction process. Similarly, other ways could be to integrate differential privacy with some provable mechanism to protect identity indirectly alongside preserving privacy of PU nodes.

SU Bidding Privacy

Apart from PUs asking price privacy, it is important to protect valuations/bids of buyers during the auction process. Valuations for a specific spectrum band is personal information and the majority of CR buyers do not want their private valuations to get leaked [82]. To overcome this, researchers integrated sealed bid auctions in CRN, but modern machine learning-based attacks have caused privacy leakage even in sealed bid auctions. Therefore, it is important to protect privacy of bidding price alongside preserving privacy of asking price.

Prospective Role of Differential Privacy: Private valuation of auction process can easily be protected using randomized differential privacy mechanism [83]. For SUs, differential privacy works from the perspective of addition of random noise in the set valued data, which plays an important role in hiding the actual valuation. For instance, a randomized valuation within the range of social welfare maximization can be generated for auction with the help of differential privacy. This randomized valuation ensures that the privacy does not get leaked and the social welfare for auction still remains positive.

SU Demand Privacy

Alongside valuations, the amount required by a particular SU is also personal, because no CR node wants to reveal the exact spectrum usage to any adversary [84]. This is because these spectrum usage values can further be used to carry out burglaries or other attacks at non-usage/idle times. Similarly, the demand of a particular SU does also signify the financial situation and other similar aspects. Therefore, SUs usually try not to reveal their actual demand to auction places where there is a chance of adversarial attacks. Considering this discussion, it can be claimed that if the demand of SUs can be protected, a large gain in spectrum trading can be seen because SUs will be able to participate in auction without the risk of losing their private information.

Prospective Role of Differential Privacy: Demand by a particular SU is a personalized information, which it needs to be protected [85]. This value can easily be protected by dynamic differential privacy mechanisms. Differential privacy can be integrated at multiple steps during this demand protection process. The most significant way to overcome this issue is to integrate differential privacy with some provable mechanism. By doing this, one will be able to show perturbed demand alongside having a protected demand at the backend for verification and allocation. Another way could be to collect variable demand from SUs and then find out the finalized value via an obfuscation mechanism. Third way could be to use the Exponential obfuscation mechanism in a way that does not harm the utility but introduces a selection randomness. All these mechanisms can be used to protect demand privacy in a viable manner.

Privacy Leakage in Spectrum Allocation

After careful collection of asking price and bids, the next step is the allocation of spectrum. This step is usually carried out via some game-theoretic auction model. Some prominent auctions used in CRN include double auction, VCG auction, Dutch auction [86]. These auction models analyse all collected values and find the auction winner according to the prescribed process. Although highest bidder wins the best spectrum in these auctions, this can cause privacy leakage at various levels. For instance, the identity privacy of the winner can be leaked by analysing the auction result [87]. Similarly, the identity privacy of sellers gets leaked and it can be analysed that which seller has a specified amount of available spectrum. Alongside this, the financial situation of PU and SU nodes can be analysed by adversaries as a result of this spectrum. Similarly, the number of available channels involved in auctions can also be leaked during allocation. Therefore, designing a privacy preserving spectrum allocation model should be considered while developing CR auctions.

Prospective Role of Differential Privacy: Significant research on integration of differential privacy in auction allocation have been carried out and these research works have showed that differential privacy protection is a suitable method to protect privacy during auctions allocation [88]. From CRN perspective, there is a need to design certain works which ensure truthful and private allocation alongside enhancing social welfare. In this way, the Laplace mechanism of differential privacy can play a significant role to ensure identity and multi-channel privacy at the time of allocation by integrating controlled randomized obfuscation.

Privacy Leakage Scenarios During Spectrum Mobility

The fourth and final step in the cognitive cycle revolves around movement of SU nodes at the time of PU arrival called as spectrum mobility [89]. In this step, first of all, PU tries to access the licensed spectrum back, which in return forces SU nodes to leave the spectrum immediately. Then SU vacates the spectrum and stops communication on it. SUs then looks for another available spectrum or waits for the PU to stop the communication again in order to resume their communication [76]. In both cases, privacy gets leaked at multiple events ranging from request to hand-off. Let’s discuss that how differential privacy can play its role to mitigate these privacy risks.

SU Holding Time Privacy

When a SU occupies a spectrum, it holds the spectrum until the PU arrives, or it holds the spectrum until the required communication need is fulfilled [54]. In both cases, SU does not want other adversaries to know the exact amount of time the spectrum was held by it. For instance, if the specific time gets leaked, then the adversary can find out that the particular SU held the spectrum on a particular place for an ‘X’ amount of time which can further lead to harmful events. Therefore, protecting privacy of SUs holding time is important and specific privacy preserving mechanisms should be designed for this purpose.

Prospective Role of Differential Privacy: Channel holding time can be used to infer private information of SU, it should therefore be protected by designing privacy preserving mechanisms. In this case, differential privacy can play an active role by integrating Laplace-based obfuscation in values of holding time [90]. This obfuscation ensures that adversaries will not be able to predict with confidence about the presence or absence of a specific SU on a spectrum. Similarly, at the time of sharing holding time, the exponential randomness can be used to ensure randomized response in order to protect privacy of SU.

Privacy Leakage During Spectrum Hand-Off

When PU arrives, SUs are forced to leave the spectrum causing privacy leakage at multiple levels. Firstly, PU may know that a particular SU is within its specified region. Secondly, SUs might have to carry out SS again to find the new appropriate spectrum, which again opens the door for all privacy leakage scenarios during SS. Thirdly, alongside SU, the identity privacy of PU is also at risk, because SU can infer the presence of PU in its region by visualizing the request [10]. Therefore, it is important to integrate a privacy preserving mechanism at the time of spectrum hand-off.

Prospective Role of Differential Privacy: Spectrum hand-off comprises multiple steps, so a simple obfuscation mechanism will not be enough to protect privacy as it will only cover a single aspect. Therefore, there is a need to design such differential privacy mechanisms which protect the privacy of multiple parallel events to ensure a trustworthy CRN. For instance, a Laplace-based location privacy mechanism can be used to protect the privacy of SUs location [90]. In this mechanism, differential privacy can be used to introduce randomness in the location reporting to PU. Secondly, the sensing request should be done in a randomized way to protect this request privacy [91]. Afterwards, from the perspective of PU, an Exponential mechanism can be used to show randomized PU to SU instead of accurate identity. Similarly, the location privacy of PU at hand-off can also be protected by integrating Laplace obfuscation at the time of hand-off request.

Summary

In this section, we analysed privacy leakage scenarios during cognitive cycle which can be exploited by adversaries to infer privacy of CR participating users. We analysed all four steps involved in cognitive cycle ranging from sensing, and analysis to sharing and mobility. In SS, majority of sources are linked with location privacy. For instance, location privacy of SUs and PUs during collection of their values. Contrary to this, the sources in spectrum analysis step are more related identical threats such as characteristics privacy and network topology privacy. Moving further to spectrum sharing, it can be visualized that literature is more titled towards privacy leakage during different steps of trading. Finally, in spectrum mobility, the privacy leakage is discussed from the perspective of hand-off, which involves both identity and location privacy.

Moving further to the mitigation of these privacy issues, we also provide an in-depth discussion about each possible scenario that how differential privacy can play its role in overcoming privacy issues at different steps. We have provided a detailed discussion from the perspective of integration of both Laplace and Exponential mechanisms of differential privacy in CRN. From the discussion it can be deduced that differential privacy is a dynamic privacy preservation strategy that can play a significant role in all four cognitive cycle steps. And it can be used by researchers in multiple CR scenarios, where there is a risk of privacy leakage.

Performance Matrices for Evaluating Differentially Private CRN Mechanisms

In the previous sections, we highlight significance of differential privacy in preserving privacy of CRN. This section highlights performance parameters that should be taken care of while developing of differentially private CR mechanisms. This section divides performance matrices into three categories, first are the matrices which are required while designing differential privacy techniques; second are those matrices which should be taken care of to avoid attacks; and third are those matrices which should be focused in CR applications.

From the Perspective of Privacy Preservation

There are three important parameters which need to be considered while developing of differentially private CRN works. These are discussed below.

Degree of Privacy

While designing any privacy preservation mechanism it is important to figure out the degree of privacy required by application. For example, some applications might need a high level of privacy, but they can compromise on utility, for example, EV battery status reporting [92]. Contrarily, some applications might need a high level of utility but can compromise a little bit on privacy, for example, industrial manufacturing. Similar is the case in CRN, where some aspects in the cognitive cycle might require a higher level of privacy. For example, location reporting during SS might need a high level of privacy due to involved location inference risks. However, some aspects might require a high level of utility, such as available frequency values from a particular PU. Considering this discussion, it is important that one should determine the degree of privacy before designing and evaluating the privacy preserving model for CRN. Due to differential privacy noise addition, the degree of privacy can be further divided into: (a) degree of privacy due to noise, and (b) degree of privacy due to anonymity. The detailed discussion on these parameters is given below.

Degree of Privacy due to Noise: While designing a differential privacy mechanism, it is important to figure out the level of required noise for the specific cycle. In differential privacy, two factors actively contribute in determination of noise, first one is privacy budget (ε), while second is sensitivity (δ). In a differentially private CR mechanism, ε is used to determine the value of noise which is going to add in the output result. This ε is chosen after careful consideration and is usually backed by a strong theoretical guarantee. For instance, specific theoretical contributions have been carried out to choose the appropriate ε value [93]. This ε is inversely proportional to noise level, which means the higher value of ε provides less privacy and low values of ε provides high privacy values. Similarly, in different CR scenarios different ε values are required, which is determined at the time of mechanism design. For instance, in case of location reporting during SS, the desired ε value is pretty low, which ensures that the chances of location value getting leaked are pretty less. On the other hand, if one is determining final price of spectrum band during auction, only a minor level of noise can play the required role. Therefore, in such cases even the high value of ε can fulfil the requirement.

Similarly, the sensitivity Δ value of a differentially private mechanism is usually determined on the basis of data.

Formally, sensitivity is defined as maximum possible impact of one record in accordance with all neighbouring datasets. This value is used in the noise addition and plays a significant role in determining the noise value. For instance, a CR database in which the participants have such values which differ a lot with each other might have high sensitivity value. On the other hand, a CR database in which the difference is pretty small, will have low sensitivity. Therefore, it is important to determine the sensitivity of model before implementing it. Certain works also highlighted dynamic varying sensitivity on the basis of dynamic data, but even in that case a predetermined method to choose appropriate sensitivity is required.

Degree of Privacy due to Anonymity: Another parameter similar to noise level is anonymity level, which basically is the level of privacy/anonymity after noise addition. This level is determined by comparing the anonymized dataset with original dataset. Similarly, certain works also mentioned it as degree of privacy leakage. In differentially private CRN, it can be termed as the difference between sanitized and non-sanitized CR dataset whether it is in case of sensing, analysis, sharing, or mobility. For instance, if one requests a sensing query from a dataset, then the level of privacy that an observer will see is the actual anonymity of that privacy preservation mechanism. Considering this discussion, it can be concluded that one needs to take care of anonymity level as well during development of differentially private CR mechanisms.

Computational Complexity

Computational complexity is a very important parameter in designing a privacy preservation strategy [94]. Among all privacy preservation mechanisms (such as anonymization, encryption, information-theoretic privacy.) differential privacy has minimum computational complexity due to its light-weight nature [36]. However, even during development of differentially private CR mechanisms, the aspect of computational complexity cannot be ignored. This is because of the fact that sometimes, CR nodes are pretty minute, and they cannot handle large computations. For instance, let us take the case of a low-powered agricultural sensor which is measuring crop parametric values and is carrying out communication through CR. In this case, multiple sensors taking these readings will be pretty minute and will not have enough computational complexity to carry out heavy tasks. And if one thinks of integrating local differential privacy with these nodes, then it will need such a local differential privacy mechanism which is computationally efficient and can be supported by these nodes. Therefore, it is important to ensure that the complexity of differentially private CR mechanisms is well suited for the concerned application.

Utility Evaluation

Utility is one of the most considered factors during the development of privacy preservation models because it determines the usefulness of the mechanism. Similar is the case with differential privacy models, where utility plays a very important role in determining privacy budget and anonymity level [99]. Similarly, in differentially private CRN models the utility also plays a very important role because this factor is responsible for smooth functioning of the network. For instance, if the utility of SS values is low, then CR nodes shall not be able to access spectrum in the best way, which in turn shall impact the spectrum utilization. Similarly, if utility is not considered during spectrum trading then the social welfare being of auction may go negative. Similarly, the possibility of auction being in non-equilibrium state is also there if auction utility is not considered properly. Therefore, during development of differentially private CRN models, utility needs to be considered in detail. In order to do so, researchers specifically evaluate utility parameters in their experimental evaluation to ensure that the utility of the proposed mechanism is up to a specific level, and noise addition has not disturbed utility much.

Attack Resilience

Preventing adversarial attack is one of the most prominent features of a privacy model. Different privacy mechanisms provide resilience to different types of attacks. Similarly, the differential privacy model also provides strong resilience to a lot of privacy attacks [100]. Nevertheless, differential privacy provides resilience to a number of attacks. There are some attacks which need special consideration while developing differentially private CR models due to the nature of the adversary involved. In this section, three major attacks that are of sheer importance in preserving CRN privacy are discussed.

Inference Attack

The first attack that requires special consideration is inference attack in CRN. As the name suggests, the adversary tries to infer private data of participants by carrying out various statistical analysis [101]. Similarly, in certain cases, the adversary tries to use various machine/deep learning tools as well to find out more about the participants involved in the dataset. In CRN, this inference attack is usually carried out by an external adversary who tries to find out more information from a centralized server by asking unethical queries or by gaining maximum possible access to the database. For instance, the adversary can try to ask multiple queries related to a single person in a database to find more about that particular individual. Therefore, while developing differentially private CRN models, it is important to evaluate and check the effect of inference attacks on databases. This is usually done by asking multiple queries and evaluating the privacy leakage effect through differentially private answers. In this way, one can analyse if the proposed differentially private model is resilient to inference attack or not.

Disclosure Attack

Disclosure attack is more related to leakage of private information about a particular individual, spectrum band, or an organization [102]. In certain cases, the organizations/FCs have to share the dataset to observers in order to perform certain statistical tasks. But they do not share the dataset directly, they first anonymize the database through a privacy preservation mechanism and then share the dataset for statistical tasks. Indeed, FCs try their best to make the private information protected, but if the data analysing observer is an adversary then it tries to carry out a disclosure attack in order to infer private information. To overcome this, researchers are now integrating the phenomenon of differential privacy before publicizing databases. Therefore, disclosure attack analysis is pretty important in cases where the possibility of publishing anonymized data is high. Differential privacy mechanism provides strong resilience to this attack, as it randomizes databases in a manner that the presence/absence of a particular individual cannot be guessed with confidence. Because the value of noise always keeps the observer in ambiguity, it cannot predict anything with confidence.

Correlation Attack

Another critical attack that needs to be considered while developing differentially private CR models is correlation attack. A correlation attack is usually used after query evaluation. For example, after query evaluation, the data of queries is stored at the adversary side, and then the adversary tries to carry out machine/deep learning-based analysis over the collected information. The adversary combines the collected information with other publicly available datasets to find out links and correlation between participants [103]. This correlation analysis can further be used to infer into private information of participating CR users, whether they are the corresponding PUs/SUs or not. Therefore, while developing differentially private CR protocols it is important for researchers to analyse the effect of correlation attack in order to show resilience to it.

From the Perspective of Cognitive Radio

Alongside privacy and other matrices, certain parameters from CR perspective do also need careful analysis and evaluation while designing differentially private CR matrices. Usually, a networking protocol is evaluated on the basis of enhancement in throughput, communication overhead, and communication delay [104]. However, in the case of CRN, it is also important to figure out that the proposed model also analyses the effect of PU activity in the proposed model. In this section, we provide a thorough discussion of why the evaluation of these parameters is important while designing a differentially private CR model.

Incorporating PU Activity

The most important parameter from the CR perspective of incorporation of PU activity in the proposed model. CR is known for its dynamic capability of allowing CR nodes to carry out communication in the presence of PUs. Therefore, evaluating the proposed model with certain PU activity is important. PU activity can simply be defined as the usage of spectrum by primary nodes. This usage can be of different types and various PU activity patterns have been developed by researchers called as long-term, high, low, and intermittent. Each of these models has their own significance and cause different types of inference to CR usage. A detailed discussion about these models can be found in [74]. Since these models pose different types of inferences to utility, usability, and privacy of the network, while developing differentially private CR models, it is important to incorporate these activities to show a broader perspective.

Throughput Enhancement

Throughput is another critical parameter that is used by researchers to evaluate effectiveness of CR protocols [105]. Generally, throughput in wireless networks is considered as the total number of messages transmitted in a particular time interval [106]. However, in CRN, throughput analysis is pretty vast and a number of scenarios come under throughput enhancement and analysis. For instance, the sensing of spectrum and PU nodes around CR nodes also comes under throughput, as the faster the sensing works, the faster will the throughput of the network [105]. Similarly, the spectrum hand-off speed at the time of mobility of CR nodes is also considered as throughput. However, the important thing is that, if one wants to integrate differential privacy in these aspects then it is important to ensure that the throughput of CRN should enhance or at least do not decrease by addition of external noise. Therefore, while developing differential privacy CR models, authors are suggested to evaluate throughput aspect to ensure the speed of the network.

Delay Enhancement

Delay is usually taken in terms of the time taken to carry out some operation; however, in wireless networks it is the time that a packet takes from source to destination [107]. This parameter is being considered by approximately every second work in the field of CRN because they want to ensure that their model is efficient enough to carry out seamless communication. But when we talk about integration of differential privacy in CRN, it becomes a more critical parameter. Because the communication is now obfuscated, and in order to get beneficial output, one has to take special care of delay caused due to perturbation. Therefore, while evaluating differentially private CR models, researchers are usually advised to evaluate this delay parameter alongside.

Communication Overhead Analysis

Overhead caused by communication cannot be neglected while developing differentially private CR mechanisms because it plays an important role to carry out smooth communication between nodes [108]. Typically, differential privacy works over noise, but this noise addition should not contribute overhead. If the overhead increases because of noise addition, then the overall network performance will be reduced. Therefore, during development of differentially private CR models, researchers perform overhead analysis and compare the overhead of the proposed model with previous models without differential privacy. In this way, the proposed model is analysed and approved efficiently enough for practical implementation in CRN.

Summary

In this section, a comprehensive analysis of all matrices that can play a critical role during design and development of differentially private CRN protocols have been presented. Overall, we divide parameters in three categories from the perspective of privacy, attacks, and CR. We then subdivide each category further to provide a much clearer picture for our readers. Firstly, from the perspective of privacy preservation, we first discuss how noise level and anonymity level can play the role in determining the degree of privacy. Afterwards, we highlight that how computational complexity should be evaluated at the time of designing differentially private models, and finally we provide insights about utility evaluation of differentially private CR models.

Secondly, from the perspective of attack resilience, we gave a thorough investigation about top three attacks which are important to be prevented in differentially private CR models. First attack is inference attack which is caused due to harmful inference of adversary on centralized data centres or communication links. Second attack we discuss is data disclosure attack, which is more linked to data sharing, while the third attack we analysed is correlation attack in which strong machine/deep learning models are used to find out correlation between other databases and CR databases. Finally, in the third parametric category, we analyse parameters from CR perspective and provide discussion about four CR parameters which should be discussed in technical works. Firstly, we discuss primary user incorporation; then we provide discussion about throughput enhancement; afterwards, we analyse delay and overhead of CRN. Overall, it can be concluded that if one is designing a differential privacy-based CR protocol, then analysing and evaluating these parameters will help shape the work in the best manner.

Differential Privacy Approaches for Cognitive Radio Networks

In previous sections, we discussed how differential privacy can play its role in developing private CRN models, and that parameters should be considered while developing differentially private CR protocols. In this section, an extensive literature review that involves integration of differential privacy with CRN at different models is discussed. Based on the cognitive cycle, the technical work has been divided into three categories, that is differential privacy in: (i) SS, (ii) spectrum analysis, and (iii) spectrum sharing. Evaluation of the technical work is given in Table 4, whereas classification of the technical work is given in Fig. 5.

Differential Privacy in Spectrum Sensing

Spectrum sensing involves carrying out measurement and observations for efficient utilization of spectrum bands [121]. In SS, SUs sense their surroundings and develop a radio environment map by sharing these values with each other to get better results [122]. The sensing could be through centralized FC (which is also known as database-driven SS) or it could be through collaborative or crowdsourced approach in which all CR nodes collaborate to figure out the optimal environment. No matter which approach is used; the risk of privacy leakage still exists. For instance, location privacy, identity privacy, and behavioural privacy of PUs, SUs, and FC are always at risk when multiple parties are involved. Therefore, it is important to integrate a privacy preservation mechanism in order to protect privacy in an efficient manner. We now discuss technical approaches which propose this integration and develop their models.

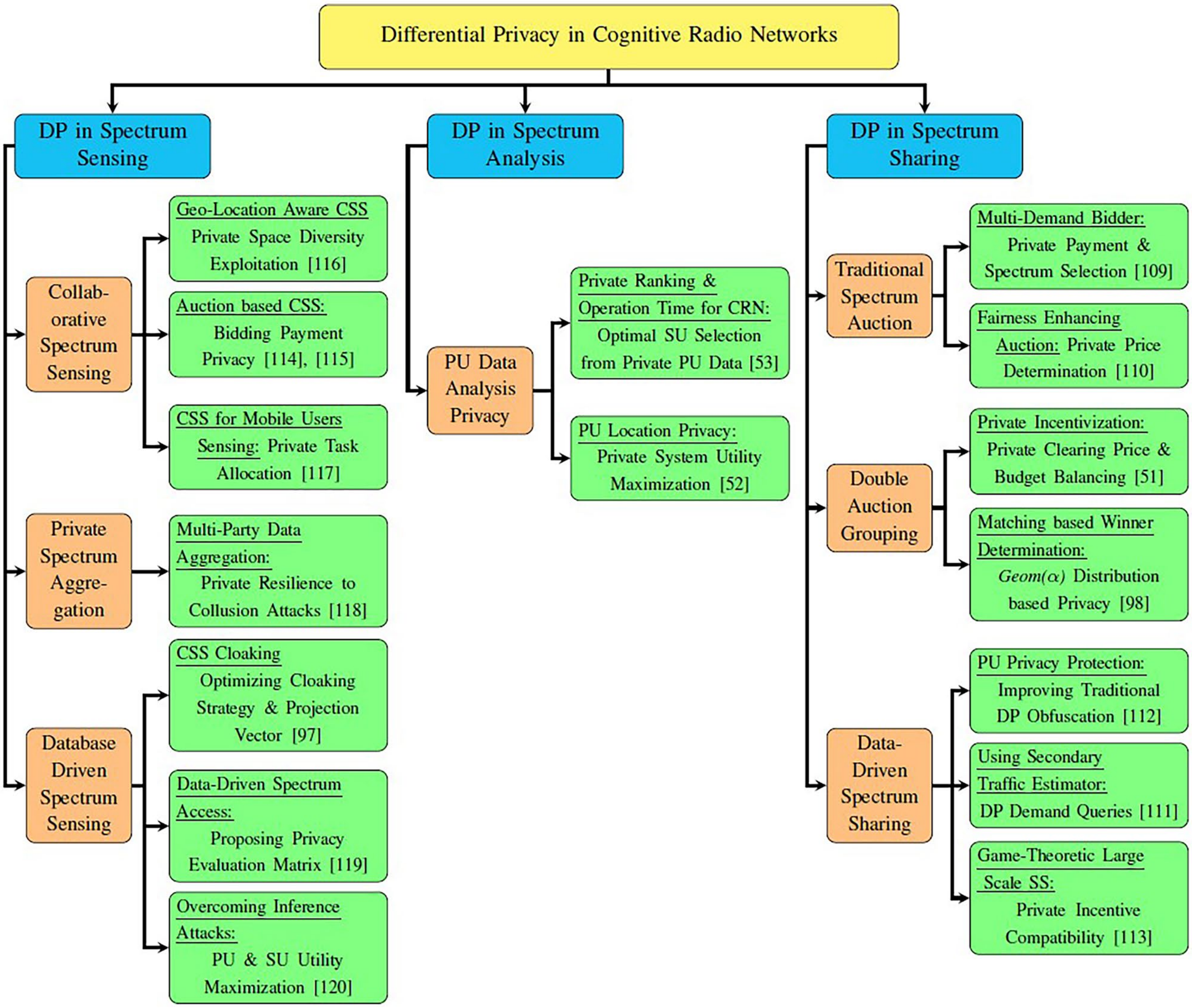
Differential Privacy in Cognitive Radio Networks
DP in Spectrum Sensing
DP in Spectrum Analysis
DP in Spectrum Sharing
Collab-orative Spectrum Sensing
Geo-Location Aware CSS Private Space Diversity Exploitation [116]
Auction based CSS: Bidding Payment Privacy [114], [115]
CSS for Mobile Users Sensing: Private Task Allocation [117]
Private Spectrum Aggre-gation
Multi-Party Data Aggregation: Private Resilience to Collusion Attacks [118]
Database Driven Spectrum Sensing
CSS Cloaking Optimizing Cloaking Strategy & Projection Vector [97]
Data-Driven Spectrum Access: Proposing Privacy Evaluation Matrix [119]
Overcoming Inference Attacks: PU & SU Utility Maximization [120]
PU Data Analysis Privacy
Private Ranking & Operation Time for CRN: Optimal SU Selection from Private PU Data [53]
PU Location Privacy: Private System Utility Maximization [52]
Traditional Spectrum Auction
Multi-Demand Bidder: Private Payment & Spectrum Selection [109]
Fairness Enhancing Auction: Private Price Determination [110]
Double Auction Grouping
Private Incentivization: Private Clearing Price & Budget Balancing [51]
Matching based Winner Determination: Geom(α) Distribution based Privacy [98]
Data-Driven Spectrum Sharing
PU Privacy Protection: Improving Traditional DP Obfuscation [112]
Using Secondary Traffic Estimator: DP Demand Queries [111]
Game-Theoretic Large Scale SS: Private Incentive Compatibility [113]

Fig. 5 A Detailed Classification of Technical Works Integrating the Concept of Differential Privacy (DP) in Cognitive Radio Networks at Various Cognitive Cycle Scenarios

Collaborative Spectrum Sensing

Sensing spectrum in a collaborative fashion is one of the prominent steps of CRN, as this gives information about surroundings in order to access the most beneficial spectrum. However, this step is vulnerable to privacy leakage as well, and to overcome this privacy leakage, differential privacy can play a viable role. The first work in this direction providing detailed insights about the development of a differentially private incentive mechanism has been presented by Dong et al. [115]. The work developed a CSS model and integrated the concept of differential privacy to protect privacy. Authors developed a multi-bid model which collects bids from sensing participants and selects sensing winners in differentially private manner. In the proposed work, authors ensured that they maximize social welfare alongside enhancing winners' cost efficiency. The work provided extensive theoretical analysis for differential privacy guarantees; however, an analysis from the perspective of welfare maximization is missing in the article. Another work discussing differential privacy for crowdsourced SS of CRN have been carried out by Jin and Zhang [114]. Authors proposed two models named as PriCSS^{+} and PriCSS^{+} and demonstrated that both of the proposed models preserve location privacy using differential privacy protection. Alongside protection, authors also enhanced payment system and proposed a truthful and cost minimizing payment mechanisms of SS participants. From the perspective of evaluation, authors carried out evaluation on multiple PU activities and evaluated utility and network overhead to demonstrate that their proposed model outperforms others in this perspective.

Table 4 A Parameter-based Evaluation of Technical Works Integrating Differential Privacy in Cognitive Radio Networks

Domain	Sub-Domain	Ref.	Major Contribution	System Model	DP Mechanism	Privacy Criterion	Complexity	CRN Parameters				
								PU activity	Throughput	Utility	Delay	Overhead
Spectrum Sensing	Collaborative Spectrum Sensing	[114]	Private location & payment strategy during crowdsensed spectrum sharing.	Centralized	Exponential	ε-dp	–	✓	✗	✓	✗	✓
		[115]	Enhanced bidding privacy for multi-bid CSS users.	Centralized	Exponential	$((e-1)\varepsilon/\delta ln(e\delta^{-1}), \delta)$-dp	–	✗	✗	✓	✗	✓
		[116]	Preserving Geo-location for CRN participants in collaborative network.	Centralized (cluster based)	Manual	(μ, δ)-dp	$\lceil \frac{n}{m} \rceil.(\frac{m+1}{2}).C_{tr}$	✗	✗	✗	✗	✓
		[117]	Private location-aware geocast SS for CRN.	Centralized	Laplace	ε-dp	–	✗	✗	✓	✗	✓
	Private Spectrum Aggregation	[118]	Spectrum aggregation & auction for multi-party CRN.	Centralized	Manual	ε-dp	$O(nn_i)Add$	✗	✗	✓	✗	✓
		[97]	Private collaborative sensing for service providers privacy via Cloaking Time.	Distributed Clusters	Laplace	ε-dp	$O(N^2K)$	✓	✗	✓	✗	✓
	Database Driven Private Sensing	[120]	PU & SU utility maximization via Optimal Private Decisions.	Centralized	Laplace	ε-dp	–	✓	✗	✓	✗	✗
		[119]	Evaluating Collaborative Privacy Protection Models of Spectrum Access Systems and PU.	Centralized	Exponential	ε-dp	–	✗	✗	✓	✓	✓
Spectrum Analysis	PU Data Analysis Privacy	[53]	Selecting Optimal SUs from Private operation-time values for CRN.	Centralized	Exponential	$(2\varepsilon\Delta)$-dp	$O(ln(N))$	✓	✗	✓	✗	✗
		[52]	Protecting PU location privacy optimally.	Centralized	Exponential	(w, ε)-dp	–	✗	✓	✓	✓	✗
Spectrum Sharing	Traditional Spectrum Auction	[109]	Private payment & spectrum selection for multi-demand bidder.	Centralized	Exponential	$(2\varepsilon\Delta)$-dp	–	✗	✗	✓	✗	✗

Table 4 (continued)

Domain	Sub-Domain	Ref.	Major Contribution	System Model	DP Mechanism	Privacy Criterion	Complexity	CRN Parameters				
								PU activity	**Throughput**	**Utility**	**Delay**	**Overhead**
		[110]	Fairness enhancing private auction.	Centralized	Exponential	$(2\varepsilon\Delta q)$-dp	–	✗	✗	✓	✗	✗
––	Double Auction Grouping	[51]	Private incentivization and budget balancing for CRN.	Centralized	Exponential	ε-dp	–	✗	✗	✓	✓	✗
		[98]	Geon(α) distribution-based bid matching privacy.	Centralized	Laplace	ε-dp	$O(KM^2N^2X)$	✗	✗	✓	✗	✗
		[111]	Private demand query modelling using secondary traffic estimator.	Centralized	Laplace	ε-dp	–	✗	✗	✓	✗	✗
	Data-driven Spectrum Sharing	[113]	Truthful game-theoretic aggregation for large scale spectrum sharing.	Centralized (cluster based)	Exponential	ε-dp	–	✗	✗	✓	✓	✗
		[112]	Protecting PU privacy in spectrum sharing.	Centralized	Exponential	(ε, δ)-dp	–	✓	✓	✓	✗	✓

A similar work on location privacy preservation for CSS is presented by Li et al. [116]. Authors proposed a privacy preserving sensing scheme, PPSS. The authors further proposed two private protocols of PPSS for aggregation and injection during sensing called PPRSA and DDRI respectively. Authors evaluated the proposed model on SRLP and DLP attacks by taking values from real-testbed sampling region of CRN. From experimental evaluations, it can be seen that the proposed model successfully protected privacy of model alongside enhancing entropy and fluctuations of received signal strength. The fourth work in the domain of differentially private privacy protection for crowdsourced SS have been carried out by Huang and Gong [117]. The work featured the method of geo-cast for hop by hop message dissemination and broadcast in CRN, and in the article authors demonstrated that how location privacy gets leaked via this type of sensing. The proposed model enhanced privacy protection for geo-cast SS alongside providing enhancement in agents task acceptance, system overhead, and report correlation. In the experimental evaluation, the work analysed correlation in the data; however, the aspect of privacy leakage and error rate is missing, which is one of the critical aspect that should be added in the location reporting works.

Private Spectrum Aggregation

Apart from CSS, a work discussing private sensing aggregation and auction in CRN is presented by Zhou et al. [118]. The work first proposed an efficient data aggregation model for multiparty CRN, and then demonstrated the sources of privacy leakage in this model. Thus, in order to overcome the privacy leakage, the authors further propose a lightweight privacy preserving aggregation strategy using the concept of dynamic differential privacy. And, alongside providing private aggregation, authors also proposed PPSSA for differentially private spectrum auction to enhance revenue of auctioneer. The authors further evaluated their proposed models and experimental evaluation showing that the proposed strategy not only enhances communication cost, but also enhances SUs satisfaction and auctioneers' revenue. Authors provide an in-depth theoretical analysis for the proposed work; however, it is important to mention that the article does not have any algorithm, which is usually helpful in replicating the work for future experiments by new researchers.

Database Driven Spectrum Sensing

In SS for CRN, one cannot ignore the discussion about database driven SS, which is the second most prominent strategy to carry out SS after CSS [89]. This method is dominantly used by SUs to get efficient results, but research has indicated that it can also cause privacy leakage. In order to overcome this privacy leakage, researchers have proposed the usage of differential privacy in database driven SS. The first work in the integration of differential privacy in CSS have been carried out by Wang et al. [97]. It is a privacy preserving framework for SU in CRN on basis of cloaking time and named the framework as PromCos. Authors draw the motivation that in order to carry out efficient sensing, it is important to incentivize and enhance trust of SUs in the network. In order to do so, authors computed differentially private theoretical privacy guarantees for SU, and afterwards, evaluated these guarantees on SP, SU, and collusion attack to ensure privacy. Some other works evaluated database driven private sensing from a differentially private perspective. The first work in enhancing privacy of database driven CRN was carried out by Zhang et al. [120]. The aim of the article is to develop an inference free framework for both SUs and PUs in which both will be able to play their part in SS without the risk of losing their private location and identity data. The authors formulated theoretical bounds for optimal decisions of PUs and SUs, and then evaluated these bounds by carrying out extensive experimental evaluation, which ensured utility of both participating SUs and PUs. The final work for integration of differential privacy in CRN was carried out by Li et al. [119]. The work focused over evaluation of privacy preserving models for SU privacy in database driven CRN. The proposed work analysed four different types of adversaries and then proposed two security matrices called indistinguishable input and adversarial estimation error. Afterwards, the authors evaluated the privacy preservation models and showed the effect of these models with respect to proposed matrices. Overall, it will not be wrong to say that the article is a good piece of literature for a new researcher in the field. But in-depth analysis, evaluation, and experiments from the perspective of the field are lacking in the article.

Differential Privacy in Spectrum Analysis

Analysing spectrum efficiently after getting values from SS devices is the second and one of the most critical steps in cognitive cycle, because this step is used to opt or bid for a specific spectrum or not [68]. It also checks if a specific available spectrum band is suitable for the required communication. Therefore, a careful analysis of spectrum is carried out in this step which involves two major steps named character analysis and parameter configuration. However, careful analysis has shown that the privacy of participants, especially the privacy of PUs gets leaked during this step [123]. Therefore, it is important to protect the privacy of participating nodes alongside providing efficient service. In order to protect the privacy of participating PUs and SUs during spectrum analysis, we believe the obfuscation mechanism of differential privacy can be utilized in an efficient manner.

Primary User Data Analysis Privacy

From the perspective of integration of differential privacy in spectrum analysis, it can be observed that work has only been carried out to protect PU privacy. In this direction, two significant works have been carried out so far. Both focus on preserving privacy of participating PUs during spectrum analysis, as PUs are the most vulnerable participants because their data is being analysed in this step. The first work for protecting operation-time privacy of PU in CRN is carried out by Dong et al. [53]. The authors named the proposed mechanism as PriDSS, in which they carried out a two-fold contribution. First from the perspective of providing efficient selection of SUs for dynamic sharing systems, and secondly from the perspective of providing privacy on operation time of PUs. This work integrated and contributed to multiple aspects of spectrum analysis within a single article. For instance, they worked on a SU selection problem by calling it a utility dependent problem, and then solved it by proposing a utility maximizing model. Afterwards, they explicitly mentioned that the operation-time of participating PUs is not private, and it can be used for various malicious purposes. For instance, detecting presence/absence of a particular PU or channel. After this discussion, they propose the strategy to efficiently select SUs from differentially private operation-time readings. The evaluation results of the proposed model showed that the work efficiently overcome privacy loss alongside providing efficient payments to maximize system utility.

The second and the final work in the domain of differentially private PU privacy protection for CRN is carried out by Liu et al. [52]. The article focused on protecting the privacy of PUs in a real-time environment. The major motivation of the article is the real-time protection, as the authors mentioned that several other works protected privacy in database-driven environments, but the works protecting privacy in real-time are missing. Therefore, authors proposed a PU privacy protection model, which protects location privacy of PUs during spectrum analysis in a real-time environment. The article used the concept of cloaking time optimality to design a differentially private utility optimal model which also enhances spectrum usage efficiency. Alongside this, authors proposed theoretical guarantees to prove that how their proposed model obeys the rules of differential privacy in order to protect PUs from harmful adversarial interference. To demonstrate it further, they developed the notion of ‘expected interference error’ and evaluated and compared this notion with other recent works to show the significance of the proposed model. Nevertheless, there is not much work in the domain of differentially private spectrum analysis, but the two works demonstrated how differential privacy can enhance privacy in this step optimally. Therefore, there is a need for more work from the perspective of differentially private spectrum analysis.

Differential Privacy in Spectrum Sharing

Spectrum sharing is a decisive step in the cognitive cycle because multiple SUs are competing for an available spectrum at this stage. Usually, auctions are carried out to choose the optimal combination of buyer and seller which maximizes utility of auction [80]. These auctions are carried out in multiple different ways. For instance, some research work is carried out on traditional auction styles, while some works proposed crowdsensed auctions. Similarly, certain other works highlighted the use of auction grouping for CRN nodes on the basis of the double auction model. Among all these auctions, it is made sure that the proposed model is rational, truthful, and maximizes social welfare of the network [80]. Apart from auction models, another aspect of data analysis during spectrum sharing cannot be ignored, because it is used to learn and adapt efficient futuristic models of spectrum sharing [10]. Usually, the aspects of game-theory and machine/deep learning are used at this step to find optimal sharing strategies. In all these models, it is important to mention that the risk of privacy leakage cannot be ignored, and in order to overcome this privacy risk, the aspect of differential privacy is being integrated by researchers.

In this section, we highlight the works which integrate the concept of differential privacy in spectrum sharing to produce optimal private results. Differentially private spectrum sharing work can be categorized into three domains from the perspective of auction model and spectrum sharing. The first two categories focus over integration of differential privacy in various types of auction, while the third category focus over integration of differential privacy in other processes involving spectrum sharing.

Traditional Spectrum Auctions

The first two works in this domain worked over integrating traditional auction models with differential privacy to ensure privacy in the trading. The first work discussing revenue maximization via approximate privacy guarantees is presented by Chen et al. [109]. The work proposed a differentially private revenue maximizing auction and named the proposed strategy as DEAR. The proposed DEAR algorithm is an auction model which protects the privacy of participating entities via the Exponential mechanism of differential privacy. The proposed work introduced differentially private randomness in bidders’ group in a hexagonal formation to ensure maximum privacy. Afterwards, the work also proved fairness enhancing theoretical guarantees of differential privacy to demonstrate that their work supports all theoretical bounds. Authors performed extensive experiments showing that the proposed work enhanced revenue of the auction market; however, it is also significant to mention that the evaluation from the perspective of social welfare of buyers is missing. Another work that evaluated differentially private auction mechanisms in CR settings was carried out by Wu et al. [110]. Authors proposed a private auction model named 'DIARY' and then evaluated and compared the proposed model with four other state of the art models to show effectiveness of the proposed model. It can be seen from experimental results that DIARY outperforms other models from the perspective of seller, and auction revenue. Authors further supported their work by adding extensive theoretical contributions from the perspective of differential privacy and auction-based evaluations such as winner selection and price determination.

Grouping-based Double Auction

Another type of auction that is commonly used in differentially private CRN is grouping-based double auction. From this perspective, Zhu et al. [51] proposed DDSM mechanism which is a double auction scheme for differentially private spectrum grouping. Authors used the Exponential mechanism of differential privacy to select private optimal prices during the double auction process. Afterwards, authors proved using theoretical guarantees that their proposed price selection model provides truthfulness and rationality alongside providing private pricing. The second work in the domain of differentially private auction was carried out by Hu et al. [98]. The authors used $Geom(\alpha)$ distribution to protect bid privacy during the auction process. The new distribution is combined with a differentially private noise addition model to find out the optimal amount of noise for the bid value before encryption. The performance evaluation demonstrated that the proposed model outperforms other similar works in terms of revenue, satisfaction, and privacy of PUs and SUs. The article is a twofold contribution from the perceptive of auction and differential privacy. But the experimental evaluation only shows the evaluation of auction properties, while the evaluation for privacy parameters is missing.

Data-Driven Spectrum Sharing

Apart from auction works, some researchers worked over integration of differential privacy in data-driven aspects of private spectrum sharing. The first work that falls in this category is carried out by Wang et al. [111], which focused on preserving SUs privacy in data-driven spectrum trading. The contributions of the articles are twofold: firstly, authors preserved revenue of PUs by integrating differential privacy in it, and afterwards, authors preserved the demand values of SUs as well through dynamic differential privacy. The work first proposed an architecture in which available spectrum of PUs is aggregated for selling during spectrum sharing. PUs can sell the spectrum to centralized SSP at fixed price or can also sell it directly to SUs at the individual price. However, in both of the cases authors ensured that the privacy of PUs gets protected by adding a specified level of obfuscation in the trading. Alongside this, the centralized PSP also collects values and estimates the demand of SUs, in order to develop an efficient utilization matrix. This is also done in a differentially private manner to protect privacy of SUs. Overall work ensured that the proposed model is optimized with respect to revenue-maximization and risk-minimization. Another work targeting truthful aggregation via game-theoretic perspective is carried out by Zhou et al. [113]. This work introduced a novel game in CRN and called the game as an aggregative game, which is used to carry out large-scale modelling of spectrum sharing in CRN. Authors draw the motivation of proposed game by saying that in large-scale CRN, the information about each other is incomplete, which forms a 'weak mediator', and this weak mediator will not be able to reach Nash equilibrium with this incomplete information. Therefore, they developed an aggregative game to improve the utility of these systems. However, they showed that this type of learning can lead to privacy leakage, which they further eliminated by using the concept of differential privacy and proposed an incentive-compatible and differentially private approximate Nash equilibrium of aggregative game for CRN. The final work focusing over privacy enhancement of PUs in spectrum sharing has been carried out by Clark and Psounis [112]. The work first studied the trade-off between privacy and performance in differentially private CRN, and then proposed a generalized spectrum sharing model to overcome this trade-off. Authors considered this research gap as an optimization problem of privacy in which one measures the level of privacy on the basis of data exposure to possible adversaries. After that, the authors tried to fill this research gap by developing an optimal solution for multi-utility spectrum sharing model in terms of performance and efficiency of using spectrum in the best possible way.

Summary

In this section, a comprehensive overview of integration of differential privacy in CRN from the perspective of technical works is presented. We first categorized all technical works from the perspective of steps involved in cognitive cycle, and afterwards provide in-depth subcategories of these cycle steps on the basis of technical contributions in the article. From the discussion it can be seen that a variety of scenarios in spectrum analysis have been evaluated ranging from CSS to database-drive SS. Similarly, the aspect of differentially privacy spectrum sharing has also been explored a lot from trading and database analysis perspective. But, when we move to spectrum analysis and spectrum mobility, not much work can be seen. For instance, in spectrum analysis, only two technical works have carried out integration of differential privacy, and that too to protect PUs privacy. Similarly, from the perspective of differentially private spectrum mobility, none of the technical work evaluated this aspect in detail. Therefore, we did not provide this cycle step in the classification figure and table. This discussion opens a wide-range of future directions especially from the perspective of spectrum analysis and spectrum mobility in CRN.

Applicability of Differential Privacy in Futuristic Cognitive Radios

Apart from the privacy leakage in traditional usage, the notion of CR is also being applied to various applications. For instance, CRN are being integrated with smart grid and other similar technologies to carry out resource efficient communication [124]. Nevertheless, these integrations provide a vast number of benefits, but they also come with certain drawbacks, and one of the largest among them is the privacy leakage. Therefore, preserving privacy is of sheer importance in futuristic CR-based technologies. In this section, discuss the importance of privacy in these applications, and then we provide an in-depth discussion that how differential privacy can be used to project privacy in these scenarios.

Cognitive Radio-Based Smart Grid

Integration of CR with traditional energy grids is also one of the key features being considered during development of modern smart grid systems [124]. This integration has provided a wide range of benefits ranging from power reduction to low-latency communication between smart meters and grid utilities [125]. For instance, CR-based smart metering nodes can carry out communication over available spectrum bands without having heavy license cost. Similarly, the highly adaptive nature of CR communication is suitable to carry out almost every possible operation of smart grid, whether its real-time reporting, fault monitoring, or meter firmware updates, etc. Nevertheless, CR-based smart grid is a viable communication model for modern smart grid scenarios, but it also comes up with certain privacy-related issues which needs to be tackled. For example, daily lifestyle privacy of residents can be leaked if smart meters report their real-time data to grid utility via dynamic CR channel. Similarly, location privacy of smart meters can be leaked while carrying out spectrum analysis for communication. Therefore, it is important to protect the privacy of CR-based smart grid users before practical application of these scenarios.

Integration of Differential Privacy

In order to protect privacy of CR-based smart grid users, differential privacy can be used as a viable solution because of its dynamic and light-weight nature. For instance, CR-based smart meter nodes reporting their real-time data via unlicensed channels can use a perturbation mechanism of differential privacy to add noise in their values in order to protect their privacy. Similarly, Exponential perturbation of differential privacy can be used during spectrum analysis of CR-based smart meters. Apart from these prominent directions, differential privacy can also be used to protect usage privacy during firmware updates, fault detection, fault reporting, and other similar scenarios where smart grid nodes have to use functionalities of CRN to carry out communication. From the perspective of literature review in this domain, certain works (such as [64, 126]) highlighted the use of differential privacy in smart grid reporting and other analysis. However, a full-fledged work discussing and integrating differential privacy in CR-based smart grid has not been carried out yet. Therefore, we believe that this domain has potential and this integration of differential privacy with CR-based smart grid communication can lead to development of secure and efficient modern energy infrastructures.

Software-Defined Networks-based Cognitive Radio

Since the emergence of CR, it has been incorporated with various technologies, and software-defined network (SDN) is one of them. This integration of CR and SDNs are in discussion for more than a decade due to its tremendous benefits [127]. SDNs provide CR users with an efficient architecture to carry out their communication and networking needs, which in turn will help to improve the efficiency and latency of CRN. Effective network management capabilities of SDN enables CR nodes to carry out efficient communication without worrying about network latency and complexity issues. However, despite these tremendous advantages, it can also be visualized that even SDN-based CR do also suffer with privacy issues because of centrally managed networks. As SDN uses various rules to manage network wide traffic, and all this is happening in a centralized manner; therefore, if an adversary gets control over this central entity or in case of some malicious query evaluation, the privacy of these networks is at risk [128]. Therefore, it is important to protect the privacy of these networks before integrating them with CR and other similar radios.

Integration of Differential Privacy

To overcome this issue of centralized query evaluation for SDN-based CRN, differential privacy serves as one of the most suitable options. Exponential mechanism of differential privacy can be used to protect privacy of CR users during query evaluation, during spectrum analysis, and during other cognition cycle steps. Similarly, critical information of the SDN-based CRN can also be protected via direct data perturbation/Laplace mechanism of differential privacy in order to reduce adversarial risk. For instance, during SS when every CR node transmits their data to a centralized SDN server, then instead of reporting plain-text data, one can report differentially private data in order to protect its location and identity privacy.

Cognitive Radio-Based Internet of Things

IoT is a widespread domain which is playing a very important role in our daily lives ranging from small temperature sensors in homes to massive ubiquitous sensing controllers taking decision of transportation [129]. If one looks around, IoT devices are everywhere around us and are being integrated with almost all major communication technologies to carry out operations in a streamline manner. As a part of this integration, researchers also integrated and used the concept of CR to carry out IoT communication, which has been proved to be beneficial in many ways [130]. For instance, smart in-home applications are being made capable of running over unlicensed spectrum in order to overcome spectrum scarcity due to immense increase in in-home sensors [131]. Similarly, smart cities are being developed with an aim of developing an eco-friendly environment, and one step in them is to carry out communication via CR instead of traditional licensed bands to reduce the excessive use of licensed spectrum [132]. Despite these tremendous benefits, the aspect of privacy leakage from these IoT devices cannot be ignored due to the large amount of data traversing across the network [133].

Integration of Differential Privacy

IoT devices transmit a large amount of data to the network via CR unlicensed channels to carry out various operations for the functioning. If this data is not secured, then this can leak privacy of the device owners, which can lead to catastrophic results [134]. In this perspective, differential privacy can play a key role in both active and passive data protection of CR-based IoT devices. For example, in case if IoT devices are carrying real-time streaming of their data via CRN, then noise addition mechanism of differential privacy can protect data of this real-time streaming by injecting i.i.d noise in it. Similarly, in case of passive data protection for IoT where surveys, learning, and query evaluation is carried out, the randomization mechanism of differential privacy can play a role to produce ambiguity in attackers mind regarding presence or absence of a specific user or IoT node during learning. Therefore, we believe integrating differential privacy with IoT devices operating over CRN can be a viable solution to protect them from external and internal intruders.

Machine/Deep Learning-Based Cognitive Radio Networks

Since the advent of CRN, researchers are continuously trying to develop and integrate novel technologies to enhance its efficiency. One such pathway is integration of machine/deep learning with CRN. CRN by its basic nature is considered to be an artificially intelligent radio which is capable of taking intelligent decisions involving spectrum sharing, hand-off, etc. However, the integration of modern machine/deep learning models with CRN has opened a plethora of research directions via which one can enhance the functioning of CRN in an efficient manner [135]. For example, reinforcement learning provides CR users the functionality to develop their behaviour via interacting with the surrounding environment during the cognition cycle [136]. Apart from reinforcement learning, basic machine learning algorithms such as support vector machine (SVM), homomorphic machine learning, nearest neighbour, ANN, etc., have also aided a lot in development of modern CRN. Similarly, in the modern times, the integration of deep learning models with CRN is paving path for future intelligent radios, e.g. one such example is the integration of deep reinforcement learning with CRN, which enhances the capability of SS a bit further and provides CRN users with an efficient signalling results to choose the best possible option [137]. Similarly, deep neural network (DNN)-based models are also being used to enhance the detection accuracy during spectrum sending [138]. Nevertheless, the research in machine/deep learning-based CRN is improving day by day, and a large amount of data from CR nodes is being collected to enhance the cognition cycle of CRN. This data is basically the feed to machine/deep learning models, and it will not be wrong to say that more data means high detection accuracy. However, on the other hand this data can leak a huge amount of private information of CR users. For example, accurate location information during SS can lead to location privacy leakage. Similarly, spectrum hand-off information can lead to leakage of holding time privacy of nodes. Therefore, alongside collecting this huge amount of data for machine/deep learning models, it is equally important to protect this data from all sorts of adversaries.

Integration of Differential Privacy

Nonetheless, the collected data during the cognition cycle can pose a huge privacy concern for CR users, but on the other hand differential privacy protection can be used to protect this privacy leakage to a large extent. Nowadays, differential privacy is a universally accepted matrix for privacy protection during machine/deep learning scenarios, thus differential privacy is being integrated with almost all state-of-the-art learning models to protect privacy at different levels. For instance, local differential privacy is being used to protect individual privacy before feeding the data to a machine learning model [139]. Similarly, differentially private learning in wireless big data networks is also being employed by researchers to test its efficacy in wireless scenarios [140]. Apart from these, differential privacy have proved its significance in almost all machine learning models, such as naïve bayes, linear regression, linear SVM, logistic regression, kernel SVM, decision tree, k-means clustering, etc. [141]. Thus, one can imply all these differentially private machine learning models in the majority of CR scenarios. For example, during machine learning for SS, local differential privacy can be used to protect user privacy. Similarly, during query evaluation and learning steps of cognition cycle, noise can be calibrated and added to protect individual privacy. Therefore, by keeping in view this discussion, it will not be wrong to say that differential privacy is one of the most viable solutions to protect privacy during machine learning-based CR applications, where users have to share their private data in order to get efficient outcomes.

Cognitive Radio-Based UAV Communication

Nowadays, drone technology (also known as unmanned aerial vehicle (UAV)) is booming, and various different sized drones are being used to carry out multiple applications around us ranging from sports streaming to carrying critical military operations [142]. In order to carry out efficient communication and message exchange between UAVs, researchers are using unlicensed CR-bands for communication [143]. In this way, UAVs can exploit the unused spectrum and can carry out their operations without causing their part in spectrum scarcity. Nonetheless, this integration is fruitful, but research has highlighted that the information exchange via this integration is not completely secure and is prone to many privacy attacks. For example, in autonomous UAVs, route planning is carried out, but this route planning also needs to be reported to neighbouring clusters via CR network to overcome possibility of any collusion. However, if this information gets leaked, it can reveal the complete planning and movement of UAV clusters. Therefore, it is important to protect the privacy of these UAVs in order to carry out seamless operations.

Integration of Differential Privacy

Similar to CR-based IoT devices, CR-based UAVs are also reporting their real-time planning, location, and identity values to the neighbouring nodes, clusters, and managing authorities to carry out operations in a streamline manner. This real-time reporting can cause serious privacy leakage because significant strategic information can be leaked from the reported values. Similarly, while performing steps involved in the cognition cycle, these UAVs also have to carry out SS, analysis, sharing, and mobility, which can also cause privacy leakage to a greater extent. In order to overcome these issues, the notion of differential privacy can play a critical role due to its dynamic nature of privacy protection during a real-time reporting environment. Different from other privacy preserving strategies, differential privacy can perturb values in real-time depending upon the allowed error rate. This real-time perturbation can be integrated with UAV real-time reporting and sensing to protect their private values. For example, if a UAV is reporting its identity in real-time just to show its presence, then its identity can be protected by adding i.i.d noise, which will not affect normal operations of the CR network, but on the other hand it will protect the identity theft of that particular UAV. Therefore, we believe integrating differential privacy with CR-based UAVs can be a good step ahead to develop a secure CR-based drone network.

Cognitive Radio-Based Industrial Internet of Things

Carrying out industrial operations via industrial sensors is a well-developed subfield of IoT which is also known as industrial IoT (IIoT). The sensors involved in IIoT are responsible to carry out decisions on the basis of received input [144]. For example, a sensor in a car manufacturing industry will take input from the buyer and will change the colour of the car according to the requirement. In order to provide seamless communication, these sensors are now being operated over unlicensed CR bands [145]. This integration of CR with IIoT architecture is enabling many industries and organizations to reduce their contribution in spectrum scarcity. However, on the other hand, these IIoT nodes are now more vulnerable to privacy issues because now they have to report their sensing values to the centralized CR moderators in order to perform steps involved in cognition cycle. Therefore, it is important to protect privacy of these CR-based IIoT nodes so that they can carry out their operations without risking them to potential adversaries.

Integration of Differential Privacy

The notion of differential privacy has been well researched in literature from the perspective of IIoT [65]. These research works have proved that integration of differential privacy with IIoT sensors and nodes can result in a fruitful outcome. For example, during sharing of mutual information among sensors, differential privacy perturbation can protect sensors and involve user's privacy. Similarly, these concepts can also be applied to CR-based IIoT networks because they share pretty much similar space. For example, if an IIoT node has to carry out SS to choose the most viable spectrum band, then it can perturb its identity and location values to protect itself from network adversaries. Similarly, during information sharing on unlicensed spectrum, these IIoT nodes can add noise to protect information of users being shared via their medium. That is why, we believe that adding differential privacy with a CR-based IIoT network will pave the way for futuristic IIoT systems.

Blockchain-Based Cognitive Radio Networks

Blockchain came into sight as a backbone technology after the sudden boom in the price of Bitcoin since the past decade [146]. Since then, research works are being carried out to integrate blockchain in almost every second aspect of our everyday life [147]. In the quest of this integration, blockchain technology is now being used to perform various CR operations. For example, the steps involved in the cognition cycle are being performed on decentralized distributed blockchain networks in order to enhance trust in the network. This recording of CRN data on blockchain ledger ensures that all participants receive a fair outcome and will prevail a sense of security and trust in the network [148]. However, this decentralized nature also raises various questions, and one of the biggest questions among them is privacy of CR nodes. As mentioned, that the data from CR nodes will be reported and recorded on a tamper-proof decentralized ledger, which means that this data will be visible to all participating nodes in case of a public blockchain to ensure trust, but on the other hand an adversary or a node with adversarial intentions can also misuse this data as well. Similarly, as the data is tamper-proof and will always be there on the chain, then some adversarial node can also learn about past history of a CR node even if the node has left the network. These are certain privacy aspects which need to be addressed in detail before practical deployment of blockchain with CRN.

Integration of Differential Privacy

To preserve privacy of blockchain-based CRN, differential privacy can be a feasible solution because of the diverse adaptability of differential privacy protection. The biggest reason that makes blockchain-based CRN prone to privacy attack is the public availability of plain-text data on decentralized distributed ledger. This issue can be countered by adding pseudorandom noise via differential privacy to the data before reporting/recording it to a decentralized ledger. The noise in differential privacy is controlled by privacy budget, which ensures that the noisy values remain useful to carry out various operations such as statistical analysis, etc. But on the other hand, the strong theoretical guarantee of differential privacy also ensures that the adversary should not be able to get private information of CR nodes from the recorded data. Similarly, in private blockchain networks, certain analyses have been carried out to learn from CR data for futuristic purposes. This analysis can also be secured by introducing a layer of differential privacy between blockchain ledger and observer. Considering this discussion, we believe that differential privacy is one of the critical mechanisms which can play a key role in development of modern blockchain-based CRN.

Cognitive Radio-Based Vehicular Networks

Vehicular communication is not a new topic and it has been in discussion in the scientific community since ages [149]. Similar to other networks, these vehicular networks have also been made capable of running over unlicensed CR spectrum in order to preserve excessive usage of spectrum [150]. A plethora of research has been carried out to perform all operations of vehicular networks via CR so that modern vehicles do not contribute to spectrum shortage [151]. These research works have indicated that this integration of CR with vehicular ad hoc network is a viable solution, and vehicles can achieve low-latency rate and ultra-reliable communication by incorporating CRN during their communication. On the other side of the coin, these CR-based vehicular ad hoc networks (VANETS) are not completely secure and are prone to various privacy attacks because of their real-time reporting. Therefore, protecting privacy of these CR-based VANETS is of sheer importance and this issue needs to be resolved.

Integration of Differential Privacy

To protect privacy of CR-based VANETS, it is important to analyse the type of privacy leakages among these networks. If we analyse, it is evident that the most critical private information among CR-based VANETS is location privacy of vehicles. For example, one does not want to show to others whether he/she visited the hospital at a particular time or not. However, in case of CR-based VANET reporting, sensing, and analysis, this information is prone to adversaries, and any adversary with some background knowledge can get insights of exact values. In order to overcome this, differential privacy can be used to protect location privacy. As discussed in "Scenarios of Privacy Leakage During Cognitive Cycle and Prospective Role of Differential Privacy", one can protect location information pretty easily by just incorporating randomness via differential privacy models. For example, if a vehicle adds differentially private noise to its location coordinated during SS, then the original coordinates will become protected. However, on the other hand the

SS results will not have much effect because of the vehicle being present in the same region. Therefore, we believe integration of differential privacy with CR-based VANETS can serve as a viable step towards development of more secure and private vehicular networks.

Challenges and Future Research Directions

Till now, we provide a detailed overview of how differential privacy can play a critical role in various aspects of the CRN cognition cycle. For instance, we highlight the integration scenarios of differential privacy in SS, analysis, sharing, and mobility. Similarly, we highlight various parameters that need to be taken care of while designing differentially private CRN models. However, apart from all these discussions, there are certain challenges and future directions that need special considerations while designing future differentially private CRN models. In this section, we provide first provide insights about certain prospective integrations that can be beneficial for differentially private CRN, and then we highlight certain challenges that researchers exploring these directions can face during their evaluations.

Integrating Blockchain with Differential Privacy and CRN

During cognition cycle of CRN, SU, and PU nodes suffer with lack of trust due to centralized entities. For instance, during database-drive SS, one has to rely on a centralized database to provide efficient results. Similarly, this centralization is also a part of other steps in the cognition cycle, and it cannot be ignored. Indeed, this centralization provides benefits such as quick response, etc., but on the other hand it also raises serious trust-related issues in the network. Therefore, there is a need to develop decentralized models for modern CRN [152]. In order to provide an efficient alternative to centralization, the notion of blockchain came up as a saviour for CRN. Blockchain is a novel paradigm which is being applied to a large number of daily life domains because of its trust, availability, and tamper-proof nature [153]. Similarly, certain works also discussed and evaluated the integration of blockchain with CRN ranging from SS to other steps of the cognition cycle [41, 154–157]. However, just integrating blockchain with CRN is not a one-in-all solution to every problem as it also suffers from privacy issues due to its public nature [158]. Therefore, it is important to protect privacy of decentralized blockchain CRN.

In order to ensure privacy in decentralized blockchain-based CRN, we believe that differential privacy can play a critical role. A very detailed survey on integration of differential privacy in various layers of blockchain has been presented in [159]. However, the aspect of integration of differential privacy in blockchain-based CRN has not been carried out yet. From the works integrating differential privacy with blockchain, it can be seen that it is an efficient solution to the privacy problem, but it still requires detailed research. For instance, one of the critical challenges for this integration is to choose optimal blockchain type, e.g. there could be scenarios in which public blockchain will perform the best as compared to consortium or private. Contrarily, for some functionalities, private or consortium blockchain will outperform public blockchain. Similarly, choosing an optimal differential privacy budget according to the decentralized nature of blockchain is another challenge that needs to be discussed in future works. Overall, we believe that this integration of blockchain, differential privacy, and CRN have a lot of scope in future but certain aspects require in-depth addressing before practical implementation.

Differential Privacy in Game-Theoretic Spectrum Sharing Models

Since spectrum is a non-renewable resource, it is important to use and allocate the spectrum in the most efficient manner. In order to do so, certain researchers worked over integration of game-theory in various scenarios of the cognition cycle. For instance, some works highlighted use dynamic games to get maximum benefits from CRN [160]. Similarly, certain works highlighted use repeated games for power/spectrum allocation in CRN to maximize spectrum usage efficiency [161]. Alongside this, certain works also highlighted to use game-theory-based auctions for CR spectrum trading [86]. However, the recent studies showed that CRN is vulnerable to certain privacy issues; therefore, it is important to integrate privacy preservation mechanisms with game-theoretic CRN approaches. The dynamic functionality of differential privacy can play a vital role in this integration, e.g. one aspect could be to design game-theoretic differentially private auctions that maximizes revenue alongside preserving privacy. This aspect has been touched by certain research works that we discussed in previous sections. However, it is important to highlight that maximizing revenue while preserving privacy is one of the biggest challenges that these mechanisms face. For instance, in a simple game-theoretic auction revenue can be maximized by proving various equilibriums in the system, such as Nash equilibrium, etc. However, in differentially private auctions, we cannot publicize the bids, which becomes a big hurdle to find optimal values. Certain works focused over approximate social welfare/revenue maximization, but this field still has a lot of potential which needs to be explored further.

Another direction could be to integrate differential privacy with resource allocation of CRN, in which efficient resource allocation/sharing can be carried out in a private manner. This aspect of traditional resource allocation while maintaining equilibrium has been discussed by researchers [162]. However, from the perspective of CRN, this problem is not well addressed, and we need modern differentially private strategies specifically designed for game-theoretic resource allocation by considering dynamic spectrum access capability of CRN. A significant challenge that one can face while designing these differentially private CRN allocation strategies is to perform truthful reporting for any game-theoretic mechanism. Therefore, researchers should focus over this direction in order to get maximum benefit from game-theory for differentially private CRN.

Differentially Private Cognitive Radio Trade-Offs

CR works over the phenomenon of utilization of unused spectrum band when PU is not using the specific band. Thus, in order to utilize the spectrum in the most efficient manner, SUs are continuously sensing the environment to get better opportunities, and they switch to the best available spectrum. However, during this cognition cycle process, a large number of processes are taking place, which sometime can lead to unwilling circumstances, such as false alarm, energy wastage, etc. Thus, in order to eradicate such a phenomenon, SUs try to opt certain strategies to ensure the effectiveness of sensing, e.g. increasing sensing time duration for a specific band/area, etc. These strategies help in efficient detection, but there are certain trade-offs associated with this. For example, one of the most famous trade-offs is sensing-throughput trade-off, in which detection probability and false alarm probability are taken into account in order to figure out the efficiency of the specific CRN [163]. Another famous trade-off for CRN is energy efficiency and spectral efficiency trade-off, where different architectures (such as cooperative, non-cooperative, etc.), links, analyses, and probabilities are considered to figure out efficient balance point among energy and spectral efficiency [164].

From the perspective of relevance of these trade-offs with privacy preservation, we believe that it is important to highlight that majority of these trade-offs can be linked to leakage of privacy in certain aspects. For example, in sensing-throughput trade-off, in order to enhance the throughput, sensing time needs to be increased, which in turn leads into learning a lot more than required about a specific spectrum/coverage area, which directly leads to various privacy leakages. Similarly, in energy related trade-offs, selecting a specific architecture or relay model, etc., also require learning about a specific area, which leads to leakage of privacy. Therefore, it is important to also consider the prospect of privacy preservation while observing these trade-offs. In order to protect privacy during these trade-offs, we believe that differential privacy can play an active role. For example, the location and identity privacy during excessive SS can easily be preserved via Laplacian and Exponential perturbation, in which we perturb the values to ensure that individuals cannot be re-identified, but on the other hand efficiency and accuracy is also taken into consideration in order to enhance throughput. Similarly, differential privacy can also perturb the learnt values for a specific architecture in such a way that privacy is maintained alongside ensuring the accuracy and effectiveness.

Differential Privacy in Spectrum Characterization

Spectrum characterization is the core foundation of the spectrum analysis step during the cognitive cycle. In spectrum characterization, all available spectrum bands and channels are collected and categorized according to the need [165]. This step ensures that characteristics of all available spectrum bands are gathered and grouped in an efficient way to get maximum benefits from available spectrum. In order to achieve this, researchers are also integrating modern machine/deep learning mechanisms to group these values. However, this advancement can also cause privacy leakage during the learning process. As it can be seen from experimental evaluations that machine learning algorithms can be adversely used to learn about characteristics of participants [166]. Same is the case with CRN, that if we integrate machine/deep learning during spectrum characterization, then privacy can be leaked in an adversarial manner.

In order to mitigate this privacy risk, differential privacy can play an active role due to its dynamic nature. For instance, one can develop a differentially private machine learning model to train and group spectrum bands in an efficient manner. This integration of differential privacy ensures that the added noise is pseudorandom, and no one can extract private information of participants by just looking into it. However, this integration is not as simple as it seems because it involves a large number of challenges that needs to be tackled. First of all, one has to choose an optimal machine/deep learning model that matches perfectly with the nature of dynamic differential privacy and CRN. Afterwards, the second big challenge is to figure out parameter training values via which we get both; utility and privacy during characterization. Keeping in view this discussion, it can be said that differentially private spectrum characterization can provide us a lot of benefits, but there are certain challenges that need to be addressed before this fruitful integration.

Differential Privacy in CRN for Smart Grid System

CRN has been integrated with smart grid technology for a long time due to its numerous benefits such as low communication cost [167]. If one analyses this integration, it can be seen that CRN is being used in almost all aspects of smart grid. For instance, certain works analysed integration of CRN in home management, while other works discussed collection of meter reading, pricing, and power outage values via CRN. Similarly, wide area monitoring and power line monitoring is also being carried out through CR-based smart grid. A very detailed survey on the integration of CR with smart grid has been written by Khan et al. [124]. From these integrations it is evident that CR is paving a way for futuristic smart grids. But on the other hand, the privacy issues during this integration cannot be ignored.

Ranging from privacy leakage from real-time energy monitoring to dynamic energy auctions, the communication is vulnerable, and it needs to be protected from adversaries. In order to do so, differential privacy can play a key role because of its randomization mechanisms. Similar to this, differential privacy has been applied with smart grid scenarios since long, such as differentially private smart metering [126]. But the works integrating differential privacy with CRN-based smart grid are not yet covered. Therefore, there is a need to carry out this integration of differential privacy with CRN-based smart grid in order to get maximum possible benefits from these advancing technologies. Nevertheless, this integration is pretty beneficial, but this will raise certain challenges as well, the most important among them will be maintaining the balance between utility and privacy in the protected data. The values reported by smart grid systems involve decisions related to energy; therefore, it is important to take special care of data utility because even a very small mistake can lead to catastrophic events. Therefore, the researchers who are intended to work in differentially private CRN-based smart grids have to deal with the challenge of finding optimal privacy budget, sensitivity, and other parametric values for differential privacy mechanisms.

Integrating Differential Privacy in Federated Learning with CRN

Federated learning is also a novel paradigm which is being used to carry out decentralized learning at users' end without collecting data from them [168]. Federated learning is being applied to various scenarios of cognitive cycle [169]. This concept of federated learning is providing the advantage of decentralized learning in CRN, and now FCs can learn about the characteristics and availability of spectrum without collecting sensitive information from CR nodes. This enhances the security and privacy of the whole CRN because minimal data is being collected at a centralized server.

Research works have shown that this integration can also cause privacy leakage, and even in some worst case scenarios adversarial federated learning models can be used by adversaries to learn private information from users [170, 171]. In order to overcome this risk, the integration of differential privacy with federated learning models can play a key role. For instance, certain works have been developed which have integrated differential privacy with federated learning at the time of model design, and learning. Similarly, a differentially private federated learning model can be designed for the learning environment of CRN, or differential privacy can be integrated with learning outcomes during the runtime. Both of these scenarios can be considered to preserve the privacy of CRN. Although both of these scenarios can be pretty beneficial to preserve privacy, one also has to overcome certain challenges while considering these scenarios. The most important challenge is to figure out the best type of federated learning model. For instance, two most prominent models for federated learning are horizontal federated learning and federated transfer learning. Both of these models have their pros and cons, e.g. if the datasets being used in federated learning share the same feature then horizontal federated learning is the optimal way. Contrarily, if there are not many overlapping features among data, then federated transfer learning needs to be used. Thus, in differentially private CRN, for some scenarios, such as SS, horizontal federated learning could be more suitable, because the shared features are the same, but in some cases this approach might not be feasible. For example, in case of spectrum hand-off, the responses after spectrum mobility can comprise multiple disjoint features. So, in such cases federated transfer learning could be more suitable. Therefore, finding optimal differentially private federated learning models is the key challenge that needs to be resolved before this integration.

Conclusion

Spectrum is a non-renewable resource. It is therefore important to use this precious resource in an efficient manner. In order to carry out efficient utilization of spectrum, scientists developed the notion of CR, which works over the principle of spectrum access at vacant times. CR nodes have the ability to sense the loopholes in the spectrum and then use these loopholes to carry out communication. In this way, CR nodes can play a vital role in overcoming spectrum scarcity. Nevertheless, CRN has a large number of benefits, they are not immune to all threats and one of the most critical ones is the privacy leakage, which causes serious consequences if not handled properly. Certain research works have highlighted the use of various privacy preservation approaches to protect privacy of CRN, and differential privacy is one of them. Differential privacy can play an important role in the design and development of modern, private, and more secure CRN of the future. In this paper, we carried out a comprehensive survey targeting the integration of differential privacy in CRN from various aspects. Firstly, we highlight the importance of privacy preservation in CRN, by discussing the functioning of differential privacy. We then provide an in-depth discussion about the sources of privacy leakage in CRN. Next we provide insights into how differential privacy can play a critical role in protecting this leakage. We then present an analysis of certain parameters that should be taken into account while developing differential privacy-based CRN protocols. Then, an in-depth analysis of technical works integrating differential privacy in various scenarios of CRN. Finally, we provide analysis about prospective future directions alongside highlighting certain challenges that researchers may face.

Funding No funding sources are associated with this article.

Declarations

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. Statista. Number of mobile devices worldwide 2020–2024, [Online]: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/.
2. Sharma RK, Rawat DB. Advances on security threats and countermeasures for cognitive radio networks: A survey. IEEE Comm Surveys Tutor. 2014;17(2):1023–43.
3. Ahmad A, Ahmad S, Rehmani MH, Hassan NU. A survey on radio resource allocation in cognitive radio sensor networks. IEEE Comm Surveys Tutor. 2015;17(2):888–917.
4. Ali A, Kwak KS, Tran NH, Han Z, Niyato D, Zeshan F, Gul MT, Suh DY. Raptorq-based efficient multimedia transmission over cooperative cellular cognitive radio networks. IEEE Trans Veh Technol. 2018;67(8):7275–89.
5. Mitola J, Maguire GQ. Cognitive radio: making software radios more personal. IEEE Pers Commun. 1999;6(4):13–8.
6. Boulogeorgos AAA, Salameh HAB, Karagiannidis GK. Spectrum sensing in full-duplex cognitive radio networks under hardware imperfections. IEEE Trans Veh Technol. 2017;66(3):2072–84.
7. Wei Z, Feng Z, Zhang Q, Li W. Three regions for space-time spectrum sensing and access in cognitive radio networks. IEEE Trans Veh Technol. 2015;64(6):2448–62.
8. Akhtar F, Rehmani MH, Reisslein M. White space: Definitional perspectives and their role in exploiting spectrum opportunities. Telecomm Policy. 2016;40(4):319–31.
9. Sharma SK, Bogale TE, Chatzinotas S, Ottersten B, Le LB, Wang X. Cognitive radio techniques under practical imperfections: A survey. IEEE Commun Surv Tutor. 2015;17(4):1858–84.
10. Grissa M, Hamdaoui B, Yavuza AA. Location privacy in cognitive radio networks: A survey. IEEE Commun Surv Tutor. 2017;19(3):1726–60.
11. Bhattacharjee S, Sengupta S, Chatterjee M. Vulnerabilities in cognitive radio networks: A survey. Comput Commun. 2013;36(13):1387–98.
12. Wang W, Zhang Q. Location privacy preservation in cognitive radio networks. Springer. 2014.
13. Hamamreh JM, Furqan HM, Arslan H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Commun Surv Tutor. 2018;21(2):1773–828.
14. Salahdine F, Kaabouch N. Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey. Physical Commun. 2020;39:101001.
15. Errapotu SM, Wang J, Li X, Lu Z, Li W, Pan M, Han Z. Bid privacy preservation in matching-based multiradio multichannel spectrum trading. IEEE Trans Veh Technol. 2018;67(9):8336–47.
16. Grissa M, Yavuz A, Hamdaoui B. An efficient technique for protecting location privacy of cooperative spectrum sensing users. In IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2016:915–920.
17. Wen T, Zhu Y, Liu T. P2: A location privacy-preserving auction mechanism for mobile crowd sensing. In 2016 IEEE Global Communications Conference (GLOBECOM). 2016:1–6.
18. Grissa M, Yavuz AA, Hamdaoui B. Location privacy in cognitive radios with multi-server private information retrieval. IEEE Trans Cogn Comm Network. 2019;5(4):949–62.
19. Gao Z, Zhu H, Liu Y, Li M, Cao Z. Location privacy in database-driven cognitive radio networks: Attacks and countermeasures. In Proceedings IEEE INFOCOM. 2013:2751–2759.
20. Grissa M, Yavuz AA, Hamdaoui B. When the hammer meets the nail: Multi-server pir for database-driven crn with location privacy assurance. In IEEE Conference on Communications and Network Security (CNS). 2017:1–9.
21. Xin J, Li M, Luo C, Li P. Privacy-preserving spectrum query with location proofs in database-driven crns. in IEEE Global Communications Conference (GLOBECOM). 2016:1–6.
22. Dwork C. Differential privacy: A survey of results. In International conference on theory and applications of models of computation. Springer. 2008:1–19.
23. Amjad M, Rehmani MH, Mao S. Wireless multimedia cognitive radio networks: A comprehensive survey. IEEE Comm Surveys Tutor. 2018;20(2):1056–103.
24. Amjad M, Akhtar F, Rehmani MH, Reisslein M, Umer T. Full-duplex communication in cognitive radio networks: A survey. IEEE Comm Surveys Tutor. 2017;19(4):2158–91.
25. Naeem A, Rehmani MH, Saleem Y, Rashid I, Crespi N. Network coding in cognitive radio networks: A comprehensive survey. IEEE Comm Surveys Tutor. 2017;19(3):1945–73.
26. Palguna DS, Love DJ, Pollak I. Secondary spectrum auctions for markets with communication constraints. IEEE Trans Wireless Commun. 2016;15(1):116–30.
27. Akyildiz IF, Lee W-Y, Vuran MC, Mohanty S. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. Comput Netw. 2006;50(13):2127–59.
28. Martinez Alonso R, Plets D, Deruyck M, Martens L, Guillen Nieto G, Joseph W. Multi-objective optimization of cognitive radio networks. Comput Netw. 2021;184:107651. https://www.sciencedirect.com/science/article/pii/S138912862031269X
29. Ding G, Jiao Y, Wang J, Zou Y, Wu Q, Yao Y-D, Hanzo L. Spectrum inference in cognitive radio networks: Algorithms and applications. IEEE Comm Surveys Tutor. 2017;20(1):150–82.
30. Khalek NA, Hamouda W. From cognitive to intelligent secondary cooperative networks for the future internet: Design, advances, and challenges. IEEE Network in Print. 2020:1–8.

31. Prathima A, Gurjar DS, Nguyen HH, Bhardwaj A. Performance analysis and optimization of bidirectional overlay cognitive radio networks with hybrid-swipt. IEEE Trans Veh Technol. 2020;69(11):13467–81.
32. Martin JH, Dooley LS, Wong KCP. New dynamic spectrum access algorithm for tv white space cognitive radio networks. IET Commun. 2016;10(18):2591–7.
33. Jiang B, Li J, Yue G, Song H. Differential privacy for industrial internet of things: Opportunities, applications and challenges. IEEE Internet Things J. In Print. 2021:1–1.
34. Wang T, Zheng Z, Rehmani MH, Yao S, Huo Z. Privacy preservation in big data from the communication perspective-a survey. IEEE Comm Surveys Tutor. 2018;21(1):753–78.
35. Soria-Comas J, Domingo-Ferrer J, Sanchez D, Meguas D. Individual differential privacy: A utility-preserving formulation of differential privacy guarantees. IEEE Trans Inf Forensics Secur. 2017;12(6):1418–29.
36. Hassan MU, Rehmani MH, Chen J. Differential privacy techniques for cyber physical systems: a survey. IEEE Comm Surveys Tutor. 2020;22(1):746–89.
37. Grissa M, Yavuz AA, Hamdaoui B. Preserving the location privacy of secondary users in cooperative spectrum sensing. IEEE Trans Inf Forensics Secur. 2017;12(2):418–31.
38. Tashman DH, Hamouda W. An overview and future directions on physical-layer security for cognitive radio networks. IEEE Netw. 2020:1–7.
39. Zhang X-G, Yang G-H, Wasly S. Man-in-the-middle attack against cyber-physical systems under random access protocol. Inf Sci. 2021;576:708–24.
40. Clark MA, Psounis K. Trading utility for privacy in shared spectrum access systems. IEEE/ACM Trans Networking. 2018;26(1):259–73.
41. Weiss MBH, Werbach K, Sicker DC, Bastidas CEC. On the application of blockchains to spectrum management. IEEE Trans Cogn Commun Netw. 2019;5(2):193–205.
42. Vakilinia I, Sengupta S. Vulnerability market as a public-good auction with privacy preservation. Comput Secur. 2020;93:101807.
43. Mundhe P, Verma S, Venkatesan S. A comprehensive survey on authentication and privacy-preserving schemes in vanets. Comp Sci Rev. 2021;41:100411.
44. Zhang R, Xue R, Liu L. Searchable encryption for healthcare clouds: A survey. IEEE Trans Serv Comput. 2018;11(6):978–96.
45. Alahmadi A, Abdelhakim M, Ren J, Li T. Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. IEEE Trans Inf Forensics Secur. 2014;9(5):772–81.
46. Cai Y, Chen X, Tian L, Wang Y, Yang H. Enabling secure nvm-based in-memory neural network computing by sparse fast gradient encryption. IEEE Trans Comput. 2020;69(11):1596–610.
47. Kasiri B, Lambadaris I, Yu FR, Tang H. Privacy-preserving distributed cooperative spectrum sensing in multi-channel cognitive radio manets, in. IEEE International Conference on Communications (ICC). 2015;2015:7316–21.
48. Teng Z, Du W. Comparisons of k-anonymization and randomization schemes under linking attacks. In Sixth International Conference on Data Mining (ICDM'06). 2006:1091–1096.
49. Ouafae B, Mariam R, Oumaima L, Abdelouahid L. Data anonymization in social networks state of the art, exposure of shortcomings and discussion of new innovations. In 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET). 2020:1–10.
50. Kalamkar SS, Jeyaraj JP, Banerjee A, Rajawat K. Resource allocation and fairness in wireless powered cooperative cognitive radio networks. IEEE Trans Commun. 2016;64(8):3246–61.
51. Zhu R, Li Z, Wu F, Shin K, Chen G. Differentially private spectrum auction with approximate revenue maximization. In Proceedings of the 15th ACM international symposium on mobile ad hoc networking and computing. 2014:185–194.
52. Liu J, Zhang C, Lorenzo B, Fang Y. DPavatar: a real-time location protection framework for incumbent users in cognitive radio networks. IEEE Trans Mob Comput. 2019;19(3):552–65.
53. 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(7):6561–72.
54. Diruai EM, Sobabe GC, Bai X, Guo B. Spectrum sensing based on channel holding time. In 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). 2017:1–5.
55. Pei Y, Hoang AT, Liang Y-C. Sensing-throughput tradeoff in cognitive radio networks: How frequently should spectrum sensing be carried out? In 18th International Symposium on Personal, Indoor and Mobile Radio Communications. IEEE. 2007:1–5.
56. Zhang Z, Wen X, Xu H, Yuan L. Sensing nodes selective fusion scheme of spectrum sensing in spectrum-heterogeneous cognitive wireless sensor networks. IEEE Sens J. 2018;18(1):436–45.
57. Bhattarai S, Vaka PR, Park J. Thwarting location inference attacks in database-driven spectrum sharing. IEEE Trans Cogn Commun Netw. 2018;4(2):314–27.
58. Georgiadou Y, de By RA, Kounadi O. Location privacy in the wake of the gdpr. ISPRS Int J Geo Inf. 2019;8(3):157.
59. Commission FC et al. Order on reconsideration and second report and order. 2016;FCC-16-55.
60. Asoodeh S, Liao J, Calmon FP, Kosut O, Sankar L. Three variants of differential privacy: Lossless conversion and applications. IEEE J Selected Areas Inf Theory, in Print. 2021.
61. Chen X, Zhang T, Shen S, Zhu T, Xiong P. An optimized differential privacy scheme with reinforcement learning in vanet. Computers & Security. 2021;110:102446.
62. Mao Y, Chen T, Zhang Y, Wang T, Zhong S. Towards privacy-preserving aggregation for collaborative spectrum sensing. IEEE Trans Inf Forensics Secur. 2017;12(6):1483–93.
63. Li S, Zhu H, Gao Z, Guan X, Xing K, Shen X. Location privacy preservation in collaborative spectrum sensing. In Proceedings IEEE INFOCOM. 2012:729–737.
64. Hassan MU, Rehmani MH, Chen J. DEAL: Differentially Private Auction for Blockchain-Based Microgrids Energy Trading. IEEE Trans Serv Comput. 2020;13(2):263–75.
65. Yin C, Xi J, Sun R, Wang J. Location privacy protection based on differential privacy strategy for big data in industrial internet of things. IEEE Trans Industr Inf. 2018;14(8):3628–36.
66. Fan L. Practical Image Obfuscation with Provable Privacy. In IEEE International Conference on Multimedia and Expo (ICME). 2019.
67. Roman N, Corn M, Diaci J. Sharing economy: Implementing decentralized privacy-preserving parking system. In IEEE International Conference on Smart Internet of Things (SmartIoT). 2020:109–116.
68. Xin C, Song M. Analysis of the on-demand spectrum access architecture for cbrs cognitive radio networks. IEEE Trans Wireless Commun. 2020;19(2):970–8.
69. Yang Y, Zhang Q, Wang Y, Emoto T, Akutagawa M, Konaka S. Multi-strategy dynamic spectrum access in cognitive radio networks: Modeling, analysis and optimization. China Communications. 2019;16(3):103–21.
70. Gomez-Cuba F, Asorey-Cacheda R, Gonzalez-Castano FJ, Huang H. Application of cooperative diversity to cognitive radio leasing: Model and analytical characterization of resource gains. IEEE Trans Wireless Commun. 2013;12(1):40–9.
71. Sajid A, Khalid B, Ali M, Mumtaz S, Masud U, Qamar F. Securing cognitive radio networks using blockchains. Futur Gener Comput Syst. 2020;108:816–26.
72. Barthe G, Gaboardi M, Grgoire B, Hsu J, Strub P. Proving differential privacy via probabilistic couplings. In 31st Annual

ACM/IEEE Symposium on Logic in Computer Science (LICS). 2016:1–10.

73. Hassan MU, Rehmani MH, Faheem Y. Performance evaluation of broadcasting strategies in cognitive radio networks. Wireless Netw. 2019;25(3):999–1016.
74. Saleem Y, Rehmani MH. Primary radio user activity models for cognitive radio networks: A survey. J Netw Comput Appl. 2014;43:1–16.
75. Bansal T, Li D, Sinha P. Opportunistic channel sharingin cognitive radio networks. IEEE Trans Mob Comput. 2014;13(4):852–65.
76. Tsiropoulos GI, Dobre OA, Ahmed MH, Baddour KE. Radio resource allocation techniques for efficient spectrum access in cognitive radio networks. IEEE Comm Surveys Tutor. 2016;18(1):824–47.
77. Hassan MR, Karmakar GC, Kamruzzaman J, Srinivasan B. Exclusive use spectrum access trading models in cognitive radio networks: A survey. IEEE Comm Surveys Tutor. 2017;19(4):2192–231.
78. Mochaourab R, Holfeld B, Wirth T. Distributed channel assignment in cognitive radio networks: Stable matching and walrasian equilibrium. IEEE Trans Wireless Commun. 2015;14(7):3924–36.
79. Chen Z, Qiu RC. Q-learning based bidding algorithm for spectrum auction in cognitive radio, in. Proceedings of IEEE Southeastcon. 2011;2011:409–12.
80. Yi C, Cai J. Ascending-price progressive spectrum auction for cognitive radio networks with power-constrained multiradio secondary users. IEEE Trans Veh Technol. 2018;67(1):781–94.
81. Wang Z, Li J, Hu J, Ren J, Li Z, Li Y. Towards privacy-preserving incentive for mobile crowdsensing under an untrusted platform. In IEEE INFOCOM 2019 - IEEE Conference on Computer Communications. 2019:2053–2061.
82. Li T, Jung T, Qiu Z, Li H, Cao L, Wang Y. Scalable privacy-preserving participant selection for mobile crowdsensing systems: Participant grouping and secure group bidding. IEEE Trans Netw Sci Eng. 2020;7(2):855–68.
83. Ni T, Chen Z, Xu G, Zhang S, Zhong H. Differentially private double auction with reliability-aware in mobile crowd sensing. Ad Hoc Netw. 2021;114:102450.
84. Grissa M, Yavuz AA, Hamdaoui B. Trustsas: A trustworthy spectrum access system for the 3.5 ghz cbrs band. In IEEE INFOCOM 2019 - IEEE Conference on Computer Communications. 2019:1495–1503.
85. Wang J, Errapotu SM, Gong Y, Qian L, Jantti R, Pan M, Han Z. Data-driven optimization based primary users operational privacy preservation. IEEE Trans Cogn Comm Netw. 2018;4(2):357–67.
86. Zhang Y, Lee C, Niyato D, Wang P. Auction approaches for resource allocation in wireless systems: A survey. IEEE Comm Surveys Tutor. 2013;15(3):1020–41.
87. Kasiri B, Lambadaris I, Yu FR, Tang H. Privacy-preserving distributed cooperative spectrum sensing in multi-channel cognitive radio manets. In IEEE International Conference on Communications (ICC). 2015:7316–7321.
88. Yan Y, Dong A, Zheng H, Sun Y. Privacy-preserving spectrum allocation in cognitive radio networks based on truthful online double auction mechanism. Procedia Comp Sci. 2020;174:304–8.
89. Dai Y, Wu J, Du X. Hierarchical and hybrid: Mobility-compatible database-assisted framework for dynamic spectrum access. IEEE Trans Netw Sci Eng. 2020;7(1):216–26.
90. Kaaniche N, Laurent M, Belguith S. Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. J Netw Comput Appl. 2020:102807
91. Wu D, Wu X, Gao J, Ji G, Wu T, Zhang X, Dou W. A survey of game theoretical privacy preservation for data sharing and publishing. In International Conference on Security and Privacy in Digital Economy. Springer. 2020:205–216.
92. Gunukula S, Sherif AB, Pazos-Revilla M, Ausby B, Mahmoud M, Shen XS. Efficient scheme for secure and privacy-preserving electric vehicle dynamic charging system. In IEEE International Conference on Communications (ICC). 2017:1–6.
93. Tsou Y, Chen H, Chang Y. RoD: evaluating the risk of data disclosure using noise estimation for differential privacy. IEEE Transactions on Big Data. 2019:1–1.
94. Cao Y, Yoshikawa M, Xiao Y, Xiong L. Errata on quantifying differential privacy in continuous data release under temporal correlations. IEEE Trans Knowl Data Eng. 2019;31(11):2234–2234.
95. Celebi H, Arslan H. Utilization of location information in cognitive wireless networks. IEEE Wirel Commun. 2007;14(4):6–13.
96. Prasad NR. Secure cognitive networks, in European Conference on Wireless Technology. IEEE. 2008:107–110.
97. Wang W, Zhang Q. Privacy-preserving collaborative spectrum sensing with multiple service providers. IEEE Trans Wireless Commun. 2014;14(2):1011–9.
98. Hu F, Chen B, Wang J, Li M, Li P, Pan M. MastDP: matching based double auction mechanism for spectrum trading with differential privacy. In IEEE Global Communications Conference (GLOBECOM). 2019:1–6.
99. Yang X, Wang T, Ren X, Yu W. Survey on improving data utility in differentially private sequential data publishing. IEEE Transactions on Big Data. 2017:1–1.
100. Li K, Luo G, Ye Y, Li W, Ji S, Cai Z. Adversarial privacy preserving graph embedding against inference attack. IEEE Internet Things J, in Print. 2020:1–1.
101. Liu J, Zhang C, Fang Y. Epic: A differential privacy framework to defend smart homes against internet traffic analysis. IEEE Internet Things J. 2018;5(2):1206–17.
102. Rassouli B, Rosas FE, Gndz D. Data disclosure under perfect sample privacy. IEEE Trans Inf Forensics Secur. 2020;15:2012–25.
103. Todo Y, Isobe T, Meier W, Aoki K, Zhang B. Fast correlation attack revisited, in Annual International Cryptology Conference. Springer. 2018:129–159.
104. Lu N, Shen XS. Scaling laws for throughput capacity and delay in wireless networks a survey. IEEE Comm Surveys Tutor. 2014;16(2):642–57.
105. Mokhtarzadeh H, Taherpour A, Taherpour A, Gazor S. Throughput maximization in energy limited full-duplex cognitive radio networks. IEEE Trans Commun. 2019;67(8):5287–96.
106. Alsaba Y, Rahim SKA, Leow CY. Beamforming in wireless energy harvesting communications systems: A survey. IEEE Comm Surveys Tutor. 2018;20(2):1329–60.
107. Gopikrishnan S, Priakanth P, Srivastava G. Dedc: Sustainable data communication for cognitive radio sensors in the internet of things. Sustain Comput: Infor Syst. 2020:100471.
108. Karunakaran P, Gerstacker WH. Sensing algorithms and protocol for simultaneous sensing and reception-based cognitive d2d communications in lte-a systems. IEEE Trans Cogn Commun Netw. 2018;4(1):93–107.
109. Chen Z, Ni T, Zhong H, Zhang S, Cui J. Differentially private double spectrum auction with approximate social welfare maximization. IEEE Trans Inf Forensics Secur. 2019;14(11):2805–18.
110. Wu C, Wei Z, Wu F, Chen G, Tang S. Designing differentially private spectrum auction mechanisms. Wireless Netw. 2016;22(1):105–17.
111. Wang J, Zhang X, Zhang Q, Li M, Guo Y, Feng Z, Pan M. Data-driven spectrum trading with secondary users' differential privacy preservation. IEEE Transactions on Dependable and Secure Computing. 2019.
112. Clark M, Psounis K. Optimizing primary user privacy in spectrum sharing systems. IEEE/ACM Trans Networking. 2020;28(2):533–46.

113. Zhou P, Wei W, Bian K, Wu DO, Hu Y, Wang Q. Private and truthful aggregative game for large-scale spectrum sharing. IEEE J Sel Areas Commun. 2017;35(2):463–77.
114. Jin X, Zhang Y. Privacy-preserving crowdsourced spectrum sensing. IEEE/ACM Trans Networking. 2018;26(3):1236–49.
115. Dong X, Li G, Zhang T, Lu D, Shen Y, Ma J. An incentive mechanism with bid privacy protection on multi-bid crowdsourced spectrum sensing. World Wide Web. 2020;23(2):1035–55.
116. Li S, Zhu H, Gao Z, Guan X, Xing K, Shen X. Location privacy preservation in collaborative spectrum sensing. In Proceedings IEEE INFOCOM. 2012:729–737.
117. Huang Z, Gong Y. Differential location privacy for crowdsourced spectrum sensing. In Conference on Communications and Network Security (CNS). IEEE. 2017:1–9.
118. Zhou J, Zhang Y, Cao Z, Dong X. PPSAS: lightweight privacy-preserving spectrum aggregation and auction in cognitive radio networks. In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). 2019:1127–1137.
119. Li H, Yang Y, Dou Y, Lu C, Zabransky D, Park JMJ. Comparison of incumbent user privacy preserving technologies in database driven dynamic spectrum access systems. In International Conference on Cognitive Radio Oriented Wireless Networks. Springer. 2018:55–65.
120. Zhang Z, Zhang H, He S, Cheng P. Bilateral privacy-preserving utility maximization protocol in database-driven cognitive radio networks. IEEE Trans Dependable Secure Comput. 2020;17(2):236–47.
121. Ahmend R, Chen Y, Hassan B, Du L. CR-IoTNet: Machine learning based joint spectrum sensing and allocation for cognitive radio enabled IoT cellular networks. Ad Hoc Netw. 2021;112:102390.
122. Ying X, Roy S, Poovendran R. Pricing mechanisms for crowd-sensed spatial-statistics-based radio mapping. IEEE Trans Cogn Comm Netw. 2017;3(2):242–54.
123. Cheng Q, Nguyen DN, Dutkiewicz E, Mueck M. Preserving honest/dishonest users operational privacy with blind interference calculation in spectrum sharing system. IEEE Trans Mob Comput. 2020;19(12):2874–90.
124. Khan AA, Rehmani MH, Reisslein M. Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols. IEEE Comm Surveys Tutor. 2016;18(1):860–98.
125. Khan AA, Rehmani MH, Reisslein M. Requirements, design challenges, and review of routing and MAC protocols for CR-based smart grid systems. IEEE Commun Mag. 2017 May 12;55(5):206–15. https://doi.org/10.1109/MCOM.2017.1500744.
126. Hassan MU, Rehmani MH, Kotagiri R, Zhang J, Chen J. Differential privacy for renewable energy resources based smart metering. J Parallel Distributed Comp. 2019;131:69–80.
127. Sun G, Liu G, Wang Y. SDN architecture for cognitive radio networks. In 2014 1st International Workshop on Cognitive Cellular Systems (CCS). 2014:1–5.
128. Dacier MC, Knig H, Cwalinski R, Kargl F, Dietrich S. Security challenges and opportunities of software-defined networking. IEEE Security Privacy. 2017;15(2):96–100.
129. Ahmend MS. Designing of internet of things for real time system. Materials Today: Proceedings. 2021.
130. Khan AA, Rehmani MH, Rachedi A. When cognitive radio meets the internet of things? in. International Wireless Communications and Mobile Computing Conference (IWCMC). 2016;2016:469–74.
131. Khan AA, Rehmani MH, Rachedi A. Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions. IEEE wirel commun. 2017 Jun 22;24(3):17–25. https://doi.org/10.1109/MWC.2017.1600404.
132. Somov A, Dupont C, Giaffreda R. Supporting smart-city mobility with cognitive internet of things. In 2013 Future Network & Mobile Summit. IEEE, 2013:1–10.
133. Du M, Wang K, Chen Y, Wang X, Sun Y. Big data privacy preserving in multi-access edge computing for heterogeneous internet of things. IEEE Commun Mag. 2018;56(8):62–7.
134. Awin FA, Alginahi YM, Abdel-Raheem E, Tepe K. Technical issues on cognitive radio-based internet of things systems: A survey. IEEE Access. 2019;7:97887–97908.
135. Bkassiny M, Li Y, Jayaweera SK. A survey on machine-learning techniques in cognitive radios. IEEE Comm Surveys Tutor. 2012;15(3):1136–59.
136. Ding H, Li X, Ma Y, Fang Y. Energy-efficient channel switching in cognitive radio networks: A reinforcement learning approach. IEEE Trans Veh Technol. 2020;69(10):12359–62.
137. Sarikhani R, Keynia F. Cooperative spectrum sensing meets machine learning: Deep reinforcement learning approach. IEEE Commun Lett. 2020;24(7):1459–62.
138. Liu C, Wang J, Liu X, Liang Y-C. Deep cm-cnn for spectrum sensing in cognitive radio. IEEE J Sel Areas Commun. 2019;37(10):2306–21.
139. Zheng H, Hu H, Han Z. Preserving user privacy for machine learning: local differential privacy or federated machine learning? IEEE Intell Syst. 2020;35(4):5–14.
140. Du M, Wang K, Xia Z, Zhang Y. Differential privacy preserving of training model in wireless big data with edge computing. IEEE Transactions on Big Data. 2018;6(2):283–95.
141. Ji Z, Lipton ZC, Elkan C. Differential privacy and machine learning: a survey and review. 2014. arXiv preprint arXiv:1412.7584.
142. ur Rahman S, Kim G-H, Cho Y-Z, Khan A. Positioning of uavs for throughput maximization in software-defined disaster area uav communication networks. J Commun Netw. 2018;20(5):452–463.
143. Mei W, Zhang R. UAV-sensing-assisted cellular interference coordination: A cognitive radio approach. IEEE Wireless Communications Letters. 2020;9(6):799–803.
144. Xu H, Yu W, Griffith D, Golmie N. A survey on industrial internet of things: A cyber-physical systems perspective. IEEE Access. 2018;6:78238–78259.
145. Onumanyi AJ, Abu-Mahfouz AM, Hancke GP. Towards cognitive radio in low power wide area network for industrial iot applications. In 2019 IEEE 17th International Conference on Industrial Informatics (INDIN). 2019;1:947–950.
146. Chan WK, Chin JJ, Goh VT. Simple and scalable blockchain with privacy. J Info Sec Appl. 2021;58:102700.
147. Berdik D, Otoum S, Schmidt N, Porter D, Jararweh Y. A survey on blockchain for information systems management and security. Infor Proc Manag. 2021;58(1):102397.
148. Rehmani MH. Blockchain Systems and Communication Networks: From Concepts to Implementation, T. T. Engineering, Ed. Springer Nature Switzerland AG. 2021.
149. Mekrache A, Bradai A, Moulay E, Dawaliby S. Deep reinforcement learning techniques for vehicular networks: recent advances and future trends towards 6g. Veh Commun. 2021:100398.
150. Daniel A, Paul A, Ahmed A. Queuing model for cognitive radio vehicular network. In IEEE International Conference on Platform Technology and Service. 2015:9–10.
151. Hossain MA, Noor RM, Yau K-LA, Azzuhri SR, Zaba MR, Ahmedy I. Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks. IEEE Access 2020;8:78054–78108.
152. Hasegawa M, Hirai H, Nagano K, Harada H, Aihara K. Optimization for centralized and decentralized cognitive radio networks. Proc IEEE. 2014;102(4):574–84.
153. Qu Y, Pokhrel SR, Garg S, Gao L, Xiang Y. A blockchained federated learning framework for cognitive computing in industry 4.0 networks. IEEE Trans Ind Inf. 2021;17(4):2964–2973.

154. Rathee G, Ahmad F, Kurugollu F, Azad MA, Iqbal R, Imran M. CRT-BIoV: A cognitive radio technique for blockchain-enabled internet of vehicles. IEEE Trans Intell Transp Syst, in Print. 2020:1–11.
155. Luong NC, Anh TT, Binh HTT, Niyato D, Kim DI, Liang Y-C. Joint transaction transmission and channel selection in cognitive radio based blockchain networks: A deep reinforcement learning approach. In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2019:8409–8413.
156. Kotobi K, Bilen SG. Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access. IEEE Veh Technol Mag. 2018;13(1):32–9.
157. Patnaik M, Prabhu G, Rebeiro C, Matyas V, Veezhinathan K. Probless: A proactive blockchain based spectrum sharing protocol against ssdf attacks in cognitive radio iobt networks. IEEE Netw Lett. 2020;2(2):67–70.
158. Hassan MU, Rehmani MH, Chen J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Futur Gener Comput Syst. 2019;97:512–29.
159. Hassan MU, Rehmani MH, Chen J. Differential privacy in blockchain technology: A futuristic approach. J Parallel Distrib Comput. 2020;1(145):50–74.
160. Akkarajitsakul K, Hossain E, Niyato D, Kim DI. Game theoretic approaches for multiple access in wireless networks: A survey. IEEE Comm Surveys Tutor. 2011;13(3):372–95.
161. Xu Y, Anpalagan A, Wu Q, Shen L, Gao Z, Wang J. Decision-theoretic distributed channel selection for opportunistic spectrum access: Strategies, challenges and solutions. IEEE Comm Surveys Tutor. 2013;15(4):1689–713.
162. Roth A. Differential privacy, equilibrium, and efficient allocation of resources. In 2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton). 2013:1593–1597.
163. Liang YC, Zeng Y, Peh EC, Hoang AT. Sensing-throughput tradeoff for cognitive radio networks. IEEE Trans Wireless Commun. 2008;7(4):1326–37.
164. Hong X, Wang J, Wang C-X, Shi J. Cognitive radio in 5g: a perspective on energy-spectral efficiency trade-off. IEEE Commun Mag. 2014;52(7):46–53.
165. Zheleva MZ, Chandra R, Chowdhery A, Garnett P, Gupta A, Kapoor A, Valerio M. Enabling a nationwide radio frequency inventory using the spectrum observatory. IEEE Trans Mob Comput. 2018;17(2):362–75.
166. Nasr M, Shokri R, Houmansadr A. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning, in. IEEE Symposium on Security and Privacy (SP). 2019;2019:739–53.
167. Nghia Le T, Chin W, Chen H. Standardization and security for smart grid communications based on cognitive radio technologies-a comprehensive survey, IEEE Communications Surveys Tutorials. 2017;19(1):423–445.
168. IEEE. Draft guide for architectural framework and application of federated machine learning, IEEE P3652.1/D6, 2020;1–70.
169. Pokhrel SR, Singh S. Compound tcp performance for industry 4.0 wifi: A cognitive federated learning approach. IEEE Transactions on Industrial Informatics. 2021;17(3):2143–2151.
170. Lyu L, Yu J, Nandakumar K, Li Y, Ma X, Jin J, Yu H, Ng KS. Towards fair and privacy-preserving federated deep models. IEEE Trans Parallel Distrib Syst. 2020;31(11):2524–41.
171. Sattler F, Muller KR, Samek W. Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints. IEEE Transactions on Neural Networks and Learning Systems, in Print. 2020:1–13.