Practical Privacy-Preserving Spectrum Query Schemes for Database-Driven CRNs with Multiple Service Providers

Jiajun Xin*, Ming Li*, Linke Guo†, Pan Li‡
* Department of Computer Science and Engineering, University of Nevada, Reno, NV 89577, USA
† Department of Electrical and Computer Engineering, Binghamton University, Binghamton, NY 13902, USA
‡ Department of Electrical Engineering and Computer Science, Case Western Reserve University, Cleveland, OH 44106, USA

***Abstract*—The database-driven CRN has emerged as a promising solution for the spectrum scarcity issue. However, it also raises severe privacy concerns. Although there are some existing works on this topic, they are far from practical due to their restrict on particular database structures or extremely heavy computation and communication overhead.**

To address these issues, in this paper we develop two practical privacy-preserving spectrum query schemes. A basic scheme is first proposed based on private equality test (PET) technique. In order to enhance its efficiency, an advanced scheme is further devised by integrating the Locality Sensitive Hash (LSH). More importantly, both of them are applicable to multi-SP scenarios, which have never been discussed previously.

***Index Terms*—Spectrum query, database-driven cognitive radio networks, user's operational parameter privacy**

I. Introduction

The exploding growth and popularity of wireless devices and services have exacerbated the spectrum deficiency in wireless networks. Recent studies show that this issue is also largely attributed to inefficient spectrum utilization due to the current static spectrum policies, by which spectrums are exclusively used by their licensed holders, and cannot be accessed by other users even if they are not in use. To address this artificial spectrum scarcity problem, cognitive radio networks (CRNs) have been proposed allowing primary users (PUs) to lease their unused spectrums to secondary users (SUs) who do not have licensed spectrums. More recently, as an important branch of CRNs, database-driven CRNs have been receiving increasing attention from both academia and industry due to its management efficiency for dynamic spectrum access. Several commercial entities, such as Cellular South, Google Inc. and Wi-Fi Alliance, have been actively involved in the database-driven CRNs protocol design and administration.

The work of M. Li was supported by the U.S. National Science Foundation under grants CNS-1566634, ECCS-1711991 and DGE-1516724. The work of L. Guo was partially supported by National Science Foundation under grants ECCS-1710996 and CNS-1744261. The work of P. Li was partially supported by the U.S. National Science Foundation under grants CNS-1602172 and CNS-1566479.

In database-driven CRNs, each service provider (SP), including primary service provider (PSP) and secondary service provider (SSP), maintains a database to store the spectrum available information (SAI) so as to facilitate the spectrum management. When an SU has data to transmit, it queries its home SSP for available spectrums. According to the FCC Release [1], an SU should report its location, service time duration, maximum transmission power, interference threshold and etc. during its spectrum query. Only with these operational parameters, can the home SSP depict this SU's interference relations with other incumbent users and thus decide its available spectrums. The home SSP first checks if there is collision between the query SU and SUs that it serves. As there may be other colocated users, including SUs and PUs, served by other SPs, the home SSP needs further check the spectrum availability with these SPs as well. For this purpose, the home SSP has to send them the query SU's operational parameters.

However, all these parameters contain rich information of an SU. For instance, the coordinate tells where this SU locates. The service time duration can be used to explore the SU's behavior patterns, e.g., when it is active throughout a day. Besides, the maximum transmission power can help to identify which mobile device the SU uses. Thus, an adversary, who illegally accesses these data, can easily infer an SU's private information, such as commute routes, residence, habits, and even its identity. When the SU is a federal government, possibly military, user, the information revealed during spectrum query may result in more severe threats. Therefore, all its operational parameters should be properly protected.

Only a handful existing works discuss SU's privacy protection during spectrum query in database-driven CRNs. Some private SAI retrieval schemes are developed in [2]–[4] based on private information retrieval (PIR) techniques. They allow SUs obtain SAI without revealing their locations to the database. However, these schemes heavily rely on some specific database structure and are impractical in the sense that the database has to be updated entirely whenever any

978-1-5386-0683-4/17/$31.00

user joins or leaves the system. Although the work [5] does not impose any constraint over the database structure, it involves tedious cryptographic operations and intense interactions among system entities, rendering the scheme unfavorable for practical use. More importantly, all the above works only consider a single SP, i.e., all the incumbent users together with the query SU are all subscribed to this SP. And none of the proposed schemes are extensible to multi-SP scenarios.

With these in mind, in this work we develop two practical privacy-preserving spectrum query schemes for database-driven CRNs with multi-SPs. The core requirement is to allow two SPs to determine if any pair of their served users (each served by one SP) cause conflict with each other, that is, if the spectrum usage of any two users overlap in both spatial and temporal domains. In the case that one of them is a query SU and the other as an incumbent user, then the query SU cannot be allocated with the same spectrum occupied by the incumbent user. More importantly, their operational parameters should be protected. Notice that our problem shares some similarities of the private equality test (PET) [6], [7]. However, PET can only perform over discrete values, while the conflict check in our problem is conducted over continuous values in both spatial and temporal domains, e.g., if any one locates in the interference range of the other; and if their service time durations overlap. To address this issue, we map each user's spectrum usage into grids in the spatial domain and time slots in the temporal domain. Then, the PET is conducted over two users' corresponding grids and slots. Meanwhile, in order to guarantee performance accuracy, the size of a unit grid/slot should be as granular as possible. However, this may lead to considerable computation and communication overhead, especially when there are many users and SPs in the system. Hence, as a step further, an advanced scheme is also developed. Locality Sensitive Hashing (LSH) [8] is integrated, by exploring its dimension reduction property. As we show in the simulation, the advanced scheme demonstrates a much better computation efficiency.

The contribution of this paper is summarized as follows.

- According to our knowledge, this is the first work discussing privacy-preserving spectrum query for database-driven CRNs with multiple SPs.
- The proposed schemes are much more practical than existing ones, in terms of no special structure requirement over the database and a much lower computation and communication overhead.
- We novelly apply PET and its combination with LSH in the privacy-preserving spectrum query scheme design.

The rest of this paper is organized as follow. Section II describes preliminaries of this paper. The system overview is given in Section III. We elaborate our basic scheme in section IV, followed by our advanced scheme in Section V. We conduct privacy and performance analysis the security and privacy in VI. Section VII concludes the paper.

II. Preliminaries

A. Locality Sensitive Hashing

Locality Sensitive Hashing (LSH) is a hashing scheme with the property that close nodes will collide with a higher probability than distant ones. For a given metric space $\mathcal{M} = (M, d)$, where M represents a set and $d(\cdot,\cdot)$ represents a distance measure, an LSH family $\mathcal{H}$ is (r_1, r_2, p_1, p_2)-*sensitive* if it satisfies the following conditions for any hash function $h_i \in \mathcal{H}$ and any two nodes $a, b \in \mathcal{M}$:

$$\begin{cases} P\big[h_i(a) = h_i(b)\big] \geq p_1, \text{ if } d(a,b) \leq r_1, \\ \\ P\big[h_i(a) = h_i(b)\big] \leq p_2, \text{ if } d(a,b) \geq r_2 \end{cases}$$

where thresholds $r_2 > r_1$ and probabilities $p_1 > p_2$. This tells that if the distance between two nodes is no larger than r_1, then the probability of these two nodes having the same LSH value is at least p_1; if the distance between two nodes is no smaller than r_2, the probability of these two nodes having the same LSH value is at most p_2.

Typically, a sufficient gap between p_1 and p_2 is desirable. To enlarge this gap, three amplification methods could be further adopted, i.e., AND, OR, and the combination of these two.

Specifically, given K_1 hash functions $\{h_1, \ldots, h_{K_1}\}$ randomly selected from $\mathcal{H}$, AND method defines a new LSH family $\mathcal{F}$, which is a family of functions f, by setting $f(a) = f(b)$ if and only if all $h_{k_1}(a) = h_{k_1}(b)$ $(1 \leq k_1 \leq K_1)$. Since the members of $\mathcal{H}$ are independently chosen, $\mathcal{F}$ is a $(r_1, r_2, p_1^{k_1}, p_2^{k_1})$-$sensitive$ family.

Given K_2 hash functions $\{h_1, \ldots, h_{K_2}\}$ randomly selected from $\mathcal{H}$, OR method defines a new LSH family $\mathcal{F}'$, which is a family of functions f', by setting $f'(a) = f'(b)$, if any $h_{k_2}(a) = h_{k_2}(b)$ $(1 \leq k_2 \leq K_2)$. Since the members of $\mathcal{H}$ are independently chosen, $\mathcal{F}'$ is a $(r_1, r_2, 1-(1-p_1)^{k_2}, 1-(1-p_2)^{k_2})$-$sensitive$ family.

In an AND-OR combination method, given K_2 hash functions $\{f_1, \ldots, f_{K_2}\}$ randomly selected from $\mathcal{F}$ (generated by AND-method), we define a new LSH family $\mathcal{F}''$, which is a family of functions f'', by setting $f''(a) = f''(b)$ if any $f_{k_2}(a) = f_{k_2}(b)$ $(1 \leq k_2 \leq K_2)$. Since the members of $\mathcal{F}$ are independently chosen, $\mathcal{F}''$ is a $(r_1, r_2, 1-(1-p_1^{k_1})^{k_2}, 1-(1-p_2^{k_1})^{k_2})$-$sensitive$ family.

B. Interference Model

Based on a widely used model [9]–[11], power propagation gain g between two arbitrary wireless users a and b can be expressed by $g = C \cdot d(a,b)^{-\gamma_0}$ where $d(a,b)$ refers to their Euclidean distance, γ_0 is the path loss factor, and C is a constant related to the antenna profiles of the transmitter and the receiver, wavelength, and so on.

In this work we adopt the *protocol model* [12] to analyze the interference relations among users, which considers one interfering neighbour at a time. When a and b operate on the same spectrum, b's transmission can be carried out successfully if its received signal strength from a is lower than a threshold

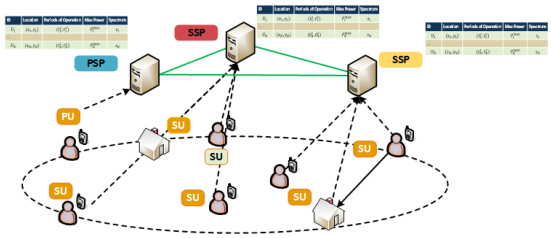


Fig. 1. System model.

δ_b, i.e., $P_a \cdot g = P_a \cdot Cd(a,b)^{-\gamma_0} < \delta_b$, where P_a stands for a's transmission power. Therefore, a's interference range is calculated by $\Gamma_a = (CP_a/\delta_b)^{1/\gamma_0}$, i.e., b's transmission can be carried out successfully if it falls outside the interference range of a, i.e., $d(a,b) > \Gamma_a$. In this work, we assume that the all users share the same interference threshold δ.

C. Cryptographic Assumptions

Decisional Diffie-Hellman (DDH) Problem: Consider a cyclic group G of order p and with the generator g. It is computationally intractable to differentiate the value g^{ab} from a random element in G, given g^a and g^b for uniformly and independently chosen $a, b \in \mathbb{Z}_p$.

III. System Overview

A. System Model

As shown in Fig. 1, the system consists of four types of entities, i.e., primary users (PUs), secondary users (SUs), primary service providers (PSPs) and secondary service providers (SSPs). We also call PSPs and SSPs as service providers (SPs) and PUs and SUs as users. In this work we consider multiple PSPs (e.g., AT&T, Verizon, and T-mobile) and SSPs (e.g., Google and Huawei) coexist, operating over the same geographic area. Each of them maintains its own database regarding the spectrum available information (SAI) of its served users and manages their spectrum allocation.

According to Protocol to Access White-Space (PAWS) Databases specified by FCC [1], a typical work flow of the system (without considering privacy protection) can be described as follows. To acquire spectrum for data transmission, an SU queries its home SSP. The query message contains this SU's location (x, y), period of operation $[t^s, t^e]$, and the maximum transmission power $P^{\max}$ it may adopt[1]. Based on them, the home SSP determines a set of available spectrums for this SU in collaborating with other SPs according to their stored SAI. Finally, the home SSP randomly picks a spectrum band from the available spectrum set and allocates it to SU, who then operates on this spectrum following the operational parameters it claimed in query. Meanwhile, the home SSP adds a new entry for this SU in its database accordingly.

[1]In practical, more information is contained in a spectrum query message, such as antenna height, transmitter's call sign and etc. We do not list them here as they are irrelevant to the scheme design in this work.

ID	Location	Periods of operation	Max power	Spectrum
U_1	(x_1, y_1)	(t_1^s, t_1^e)	P_1^{max}	s_1
...	...	...	...	...
U_N	(x_N, y_N)	(t_N^s, t_N^e)	P_N^{max}	s_N
U_{N+1}	(x_{N+1}, y_{N+1})	(t_{N+1}^s, t_{N+1}^e)	P_{N+1}^{max}	s_{N+1}

Fig. 2. Database structure.

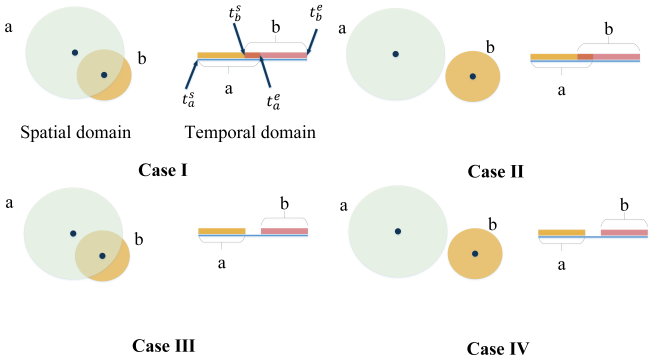


Fig. 3. Illustration of interference.

B. Database Structure

The database structure plays an important role in our scheme design for privacy-preserving spectrum query and retrieval as well as its performance. In this work we adopt a general a database structure shown in Fig. 2. Each entry records an active user's operational parameters, i.e., (x, y), $[t^s, t^e]$, and $P^{\max}$, together with the allocated spectrum s. The database allows each SP to keep track of SAI of its served users and provides necessary information for spectrum management, including spectrum allocation and billing. The SAI update process under our database structure is simple. When an SU joins/leaves, its home SSP just adds to/deletes from the database the corresponding entry for this SU.

C. Problem Formulation and Design Objectives

When allocating spectrum to a query SU, its data transmission on the allocated spectrum should not cause noticeable interference to other incumbents, including both existing PUs and SUs that operate over the same spectrum. Since an in-use spectrum is occupied both in temporal and spatial, interference should be jointly considered in both domains.

Take Fig. 3 as an example. Assume that user a and b are allocated with the same spectrum. They conflict with each other in Case I, because their transmission duration overlaps and b locates in the interference range of a. To have a and b carry out their data transmission successfully, they should be assigned with different spectrums. For the rest three cases, a and b do not conflict.

Apparently, the operational parameters (x, y), $[t^s, t^e]$, $P^{\max}$ are indispensable for SPs to determine interference relations between the query SU and incumbents and thus spectrum allocation. However, all these parameters contain rich information

of an SU. For instance, (x, y) tells where it locates. $[t^s, t^e]$ can be used to explore its behavior patterns, e.g., when it is active throughout a day. Besides, $P^{\max}$ can help to identify which mobile device the SU uses. In addition, as discussed in [2], the knowledge of k, i.e., SU's allocated spectrum, can also be leveraged to reveal this SU's location. Thus, an adversary, who illegally accesses these data, can easily infer an SU's private information, such as commute routes, residence, habits, and even her identity. When the SU is a federal government, possibly military, user, the information revealed during spectrum query may result in more severe threats. Therefore, all its operational parameters should be properly protected.

In this work we assume that SPs work under semi-honest mode, i.e., they behave honestly in following spectrum allocation protocols, but are curious in finding out operational parameters of SUs *that they do not directly serve*. SUs trust their home SSP for not disclosing their operational parameters, but not other SPs, who may sell them to adversaries for illegal benefits. Note that we are not protecting an SU's operational parameters from its home SSP, as they are easily obtainable at the home SSP. For instance, the home SSP can analyze the received signal strength and its arrival angle from the SU to estimate her location during data transmission.

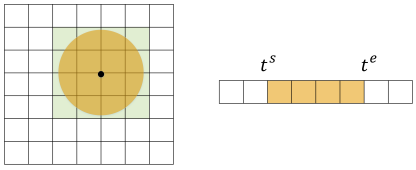
We list the design objectives of this work as follows.

- **Privacy.** Except the home SSP, no other SP can infer any operational parameter of an SU during spectrum query and retrieval process.
- **Accuracy.** The spectrum allocation result when applying our proposed schemes should be closely the same with the one when privacy is not considered.

To achieve these design goals, the challenge is apparent. As mentioned above, query SUs' operational parameters are critical in determining their spectrum allocation. Besides, since multiple SPs coexist in the same geographic area, they have to exchange these parameters to make the decision. How to carry out spectrum allocation accurately with concealed operational parameters is a nontrivial task.

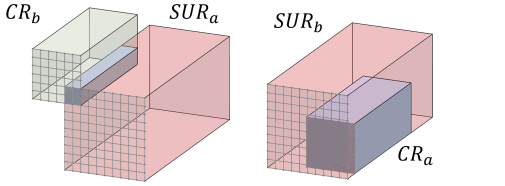
IV. Basic Scheme

In our basic scheme, the geographic area is first divided into small square grids, each with the same size of $L \times L$. Under this model, an SU's transmission/interference range becomes the minimum set of grids that cover it (as shown in Fig. 4). Besides, the time is divided into non-overlapping and fixed-size time slots. The service duration $[t^s, t^e]$ is then represented by the minimum set of consecutive time slots that cover it. As a result, an SU's spectrum usage is transformed into a set of cubes, which we call spectrum-usage-range (SUR), indicating the spatial-temporal domain that an SU occupies over a certain spectrum. Its spatial occupancy is the SU's transmission range. We further define SU's conflict range (CR) under the same spatial-temporal domain. It shares the same duration of SU's SUR in temporal, but spans across its interference range in spatial.



(a) Spatial domain (b) Temporal domain

Fig. 4. User's spectrum usage in spatial and temporal domains.



(a) SUR_a conflicts with CR_b (b) SUR_b conflicts with CR_a

Fig. 5. Two cases that user a and b conflict with each other.

For user a (b), denote by $SUR_a = \{a_1, \ldots, a_M\}$ ($SUR_b = \{b_1, \ldots, b_Q\}$) its SUR and $CR_a = \{a'_1, \ldots, a'_{M'}\}$ ($CR_b = \{b'_1, \ldots, b'_{Q'}\}$) its CR, respectively. Here, M and M' (Q and Q') stand for the total number of cubes in a's (b's) SUR and CR, respectively. According to the discussion in Section III-C, a and b conflict with each other if they use the same spectrum and either of the following conditions holds

$$SUR_a \cap CR_b = \{a_1, \ldots, a_M\} \cap \{b'_1, \ldots, b'_{Q'}\} \neq \emptyset$$
$$SUR_b \cap CR_a = \{b_1, \ldots, b_Q\} \cap \{a'_1, \ldots, a'_{M'}\} \neq \emptyset,$$

i.e., SUR_a overlaps with CR_b (as shown in Fig. 5 (a)) or SUR_b overlaps with CR_a (as shown in Fig. 5 (b)).

In the following, we elaborate our proposed scheme under a simplified scenario, where there are only two SPs. One is the query SU's home SSP which is denoted by SSP_A, and the other could be either an SSP or a PSP which is denoted by SP_B. Note that our scheme can be easily extended to the case where multiple SPs coexist.

A. System Setup

1) General Setup: Given the security parameter ξ, a trusted authority (TA) generates the ElGamal encryption parameters (p, g, G), where G is a cyclic group of prime order p and g is its generator. TA then publishes them to SSP_A and SP_B. TA also generates a field $\mathbb{Z}_p$ of order p.

2) Service Provider Registration: During SP registration, TA assigns SSP_A an ElGamal encryption/decryption key pair ($\texttt{pk}_A$,$\texttt{sk}_A$). Specifically, $\texttt{sk}_A = \mu$ with μ randomly chosen from $\mathbb{Z}_p$ and $\texttt{pk}_A = h = g^{\mu}$. Similarly, TA assigns SP_B an ElGamal encryption/decryption key pair ($\texttt{pk}_B$,$\texttt{sk}_B$), where $\texttt{sk}_B = \mu'$ with μ' randomly selected from $\mathbb{Z}_p$ and $\texttt{pk}_B = g^{\mu'}$.

B. Request and Computation

Once receiving a spectrum query $\{(x,y),[t^s,t^e],P^{\max}\}$ from SU a, its home SSP (SSP$_A$) first estimates a's interference range by $\Gamma=(CP^{\max}/\delta)^{1/\gamma_0}$, where δ stands for the minimal interference threshold of all the other SUs that also subscribe to SSP$_A$. It further generates SU a's $SUR_a=\{a_1,\ldots,a_M\}$ and $CR_a=\{a'_1,\ldots,a'_{M'}\}$ based on (x,y), $[t^s,t^e]$, $P^{\max}$, and Γ. SSP$_A$ picks a set of random numbers $r_m, r'_{m'}\in\mathbb{Z}_p$ ($m\in[1,M]$, $m'\in[1,M']$) and encrypts SUR_a and CR_a using the ElGamal encryption with its public key $\mathtt{pk}_A$ as

$$\begin{aligned}&\boldsymbol{\theta}_a=\{\theta_{a_1},\ldots,\theta_{a_m},\ldots,\theta_{a_M}\}\\&\boldsymbol{\gamma}_a=\{\gamma_{a'_1},\ldots,\gamma_{a'_{m'}},\ldots,\gamma_{a'_{M'}}\}\\&\theta_{a_m}=(g^{r_m},h^{a_m+r_m}),\quad \gamma_{a'_{m'}}=(g^{r'_{m'}},h^{a'_{m'}+r'_{m'}}).\end{aligned}$$

$\boldsymbol{\theta}_a$, $\boldsymbol{\gamma}_a$ together with $\mathtt{pk}_A$ are then sent to SP$_B$.

Similarly, SP$_B$ generates SUR and CR for each user it serves. Denote by K the total number of spectrums for the entire system and N_k the number of users served by SP$_B$ using spectrum k ($k\in[1,K]$). User j's ($j\in[1,N_k]$) SUR and CR are represented by $SUR_{j,b}=\{b_{j,1},\ldots,b_{j,Q}\}$ and $CR_{j,b}=\{b'_{j,1},\ldots,b'_{j,Q'}\}$, respectively. For each $SUR_{j,b}$ and $CR_{j,b}$, SP$_B$ encrypts them using the ElGamal encryption scheme with SSP$_A$'s public key $\mathtt{pk}_A$ and gets the ciphertext of $SUR_{j,b}$ and $CR_{j,b}$ as

$$\begin{aligned}&\boldsymbol{\theta}_{j,b}=\{\theta_{j,b_1},\ldots,\theta_{j,b_q},\ldots,\theta_{j,b_Q}\}\\&\boldsymbol{\gamma}_{j,b}=\{\gamma_{j,b'_1},\ldots,\gamma_{j,b'_{q'}},\ldots,\gamma_{j,b'_{Q'}}\}\\&\theta_{j,b_q}=(g^{\rho_{j,q}},h^{\rho_{j,q}-\nu_{j,q}b_{j,q}}),\gamma_{j,b'_{q'}}=(g^{\rho'_{j,q'}},h^{\rho'_{j,q'}-\nu'_{j,q'}b'_{j,q'}}).\end{aligned}$$

where $\rho_{j,q},\rho'_{j,q'}$ are randomly chosen from $\mathbb{Z}_p$ and $\nu_{j,q},\nu'_{j,q'}$ are non-zero numbers randomly chosen from $\mathbb{Z}_p$.

Denote by $\boldsymbol{\nu}_j$ the set $\{\nu_{j,1},\ldots,\nu_{j,Q}\}$. For each $\boldsymbol{\theta}_{j,b}$ ($j\in[1,N_k]$), SP$_B$ computes $\boldsymbol{\eta}_j$ as

$$\begin{aligned}\boldsymbol{\eta}_j=&(\boldsymbol{\gamma}_a)^{\boldsymbol{\nu}_j}\times\boldsymbol{\theta}_{j,b}\\=&\Big\{\gamma_{a'_1}^{\nu_{j,1}}\times\theta_{b_{j,1}},\ldots,\gamma_{a'_1}^{\nu_{j,q}}\times\theta_{b_{j,q}},\ldots,\gamma_{a'_1}^{\nu_Q}\times\theta_{b_{j,Q}}\\&\gamma_{a'_2}^{\nu_{j,1}}\times\theta_{b_{j,1}},\ldots,\gamma_{a'_2}^{\nu_{j,q}}\times\theta_{b_{j,q}},\ldots,\gamma_{a'_2}^{\nu_Q}\times\theta_{b_{j,Q}}\\&\qquad\ldots\\&\gamma_{a'_{M'}}^{\nu_{j,1}}\times\theta_{b_{j,1}},\ldots,\gamma_{a'_{M'}}^{\nu_{j,q}}\times\theta_{b_{j,q}},\ldots,\gamma_{a'_{M'}}^{\nu_Q}\times\theta_{b_{j,Q}}\Big\}\end{aligned}$$

where

$$\begin{aligned}&\gamma_{a'_{m'}}^{\nu_{j,q}}\times\theta_{b_{j,q}}\\=&\big((g^{r'_{m'}})^{\nu_{j,q}}\cdot g^{\rho_{j,q}},(h^{a'_{m'}+r'_{m'}})^{\nu_{j,q}}\cdot h^{\rho_{j,q}-\nu_{j,q}b_{j,q}}\big)\\=&\big(g^{r'_{m'}\nu_{j,q}+\rho_{j,q}},h^{(a'_{m'}-b_{j,q})\nu_{j,q}+r'_{m'}\nu_{j,q}+\rho_{j,q}}\big).\end{aligned}$$

Denote by $\boldsymbol{\nu}'_j$ the set $\{\nu'_{j,1},\ldots,\nu'_{j,Q}\}$. Similarly, for each $\boldsymbol{\gamma}_{j,b}$ ($j\in[1,N_k]$), SP$_B$ computes $\boldsymbol{\eta}'_j$ as

$$\begin{aligned}\boldsymbol{\eta}'_j=&(\boldsymbol{\theta}_a)^{\boldsymbol{\nu}'_j}\times\boldsymbol{\gamma}_{j,b}\\=&\Big\{\theta_{a'_1}^{\nu'_{j,1}}\times\gamma_{b'_{j,1}},\ldots,\theta_{a'_1}^{\nu'_{j,q'}}\times\gamma_{b'_{j,q'}},\ldots,\theta_{a'_1}^{\nu'_{j,Q'}}\times\gamma_{b'_{j,Q'}}\\&\theta_{a'_2}^{\nu'_{j,1}}\times\gamma_{b'_{j,1}},\ldots,\theta_{a'_2}^{\nu'_{j,q'}}\times\gamma_{b'_{j,q'}},\ldots,\theta_{a'_2}^{\nu'_{j,Q'}}\times\gamma_{b'_{j,Q'}}\\&\qquad\ldots\\&\theta_{a'_{M'}}^{\nu'_{j,1}}\times\gamma_{b'_{j,1}},\ldots,\theta_{a'_{M'}}^{\nu'_{j,q'}}\times\gamma_{b'_{j,q'}},\ldots,\theta_{a'_{M'}}^{\nu'_{j,Q'}}\times\gamma_{b'_{j,Q'}}\Big\}\end{aligned}$$

where

$$\theta_{a'_m}^{\nu'_{j,q'}}\times\gamma_{b'_{j,q'}}=\big(g^{r_m\nu'_{j,q'}+\rho'_{j,q'}},h^{(a_m-b'_{j,q'})\nu'_{j,q'}+r_m\nu'_{j,q'}+\rho'_{j,q'}}\big).$$

Finally, SP$_B$ generates $\boldsymbol{\eta}=\{\boldsymbol{\eta}_j|j\in[1,N_k],k\in[1,K]\}$, $\boldsymbol{\eta}'=\{\boldsymbol{\eta}'_j|j\in[1,N_k],k\in[1,K]\}$ and sends them to SSP$_A$.

C. Result Retrieval and Filtering

Once receiving $\boldsymbol{\eta},\boldsymbol{\eta}'$ from SP$_B$, SSP$_A$ decrypts $\boldsymbol{\eta}_j$ with its private key $\mathtt{sk}_A$. Specifically, for an element $\gamma_{a'_{m'}}^{\nu_{j,q}}\times\theta_{b_{j,q}}$, it is decrypted by

$$\begin{aligned}&D(\gamma_{a'_{m'}}^{\nu_{j,q}}\times\theta_{b_{j,q}})\\=&\big(g^{r'_{m'}\nu_{j,q}+\rho_{j,q}}\big)^{-\mu}\cdot h^{(a'_{m'}-b_{j,q})\nu_{j,q}+r'_{m'}\nu_{j,q}+\rho_{j,q}}\\=&h^{-r'_{m'}\nu_{j,q}-\rho_{j,q}}\cdot h^{(a'_{m'}-b_{j,q})\nu_{j,q}+r'_{m'}\nu_{j,q}+\rho_{j,q}}\\=&h^{(a'_{m'}-b_{j,q})\nu_{j,q}}.\end{aligned}$$

Similarly, SSP$_A$ decrypts each element $\theta_{a'_m}^{\nu'_{j,q'}}\times\gamma_{b'_{j,q'}}$ of $\boldsymbol{\eta}'_j$ by

$$\begin{aligned}&D(\theta_{a'_m}^{\nu'_{j,q'}}\times\gamma_{b'_{j,q'}})\\=&\big(g^{r_m\nu'_{j,q'}+\rho'_{j,q'}}\big)^{-\mu}\cdot h^{(a_m-b'_{j,q'})\nu'_{j,q'}+r_m\nu'_{j,q'}+\rho'_{j,q'}}\\=&h^{-r_m\nu'_{j,q'}-\rho'_{j,q'}}\cdot h^{(a_m-b'_{j,q'})\nu'_{j,q'}+r_m\nu'_{j,q'}+\rho'_{j,q'}}\\=&h^{(a_m-b'_{j,q'})\nu'_{j,q'}}.\end{aligned}$$

For each spectrum k, SSP$_A$ checks if the following equations hold for all $j\in[1,N_k]$

$$\begin{aligned}&D(\gamma_{a'_{m'}}^{\nu_{j,q}}\times\theta_{b_{j,q}})\stackrel{?}{=}1\quad\exists\ m'\in[1,M'],q\in[1,Q]\\&D(\theta_{a'_m}^{\nu'_{j,q'}}\times\gamma_{b'_{j,q'}})\stackrel{?}{=}1\quad\exists\ m\in[1,M],q'\in[1,Q']\end{aligned}$$

If the decryption of any element of $\boldsymbol{\eta}_j$ or $\boldsymbol{\eta}'_j$ ($j\in[1,N_k]$) is equal to 1 as list above, it indicates that SU a conflicts with the incumbents served by SP$_B$ on spectrum k; otherwise, it does not.

After deriving the available spectrum set for SU a from the perspective of SP$_B$, SSP$_A$ needs further filter out the spectrums that cause conflict to its other served SUs. This process can simply be carried out by SSP$_A$ checking the SAI stored at its own side. Finally, SSP$_A$ picks an available spectrum (if there is any), allocates it to SU a, and updates its database accordingly, i.e., adding a new entry for SU a as shown in Fig. 2. SU a then operates over this spectrum

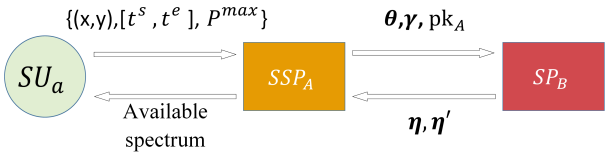


Fig. 6. Workflow for the basic scheme.

following the operational parameters it claims in query. The workflow of our scheme is summarized in Fig. 6.

Remark. In the scheme, the filtering process is conducted at SSP_A after deriving the available spectrum set for SU a from SP_B. If these two processes are performed in a reverse order, i.e., SSP_A only sends to SP_B a subset of spectrums that are available to SU a based on SAI stored at SSP_A, the decreased size of spectrums allows SP_B to correctly guess a's final allocated spectrum with a higher probability.

V. Advanced Scheme

Apparently, the computation complexity of the basic scheme increases quickly as the number of cubes contained in users' SURs and CRs grows. It becomes severe especially when there are a large number of users and SPs in the system. Therefore, in this section we propose an advanced scheme, aiming at accelerating the performance efficiency. For this purpose, we integrate LSH into the scheme design. This idea is inspired by the property of LSH, i.e., it can hash similar input items to the same value with high probability. When applying LSH over users' coordinates, it is very likely that the nearby users, which cause interference to each other over the same spectrum, have the same LSH values. Then, rather than applying the PET over a user's high-dimensional SUR and CR, we apply it over this user's single (low-dimensional) LSH value(s). In such a way, the computation complexity will be largely reduced.

A. Generation of LSH Functions

To facilitate the employment of LSH, the advanced scheme adopts a slightly different model to evaluate the interference relations between users. Specifically, we no longer transform continuous spatial domain into discrete grids. But the temporal domain is still divided into time slots as in the basic scheme. Under the new model, two users interfere with each other if a) any one of them locates in the interference range of the other; b) their service duration time slots overlap; and c) they are allocated with the same spectrum.

Denote by Γ_a and Γ_b user a's and b's interference range, respectively, and $d(a,b)$ their Euclidean distance. Our design goal for LSH function h_i is to have

$$\begin{cases} P\big[h_i(a)=h_i(b)\big] \geq p_1, \text{ if } d(a,b) \leq \max\{\Gamma_a,\Gamma_b\}, \\ P\big[h_i(a)=h_i(b)\big] \leq p_2, \text{ if } d(a,b) \geq \delta\cdot\max\{\Gamma_a,\Gamma_b\}. \end{cases} \tag{1}$$

where δ is an approximation factor slightly larger than 1.

To construct an LSH family $\mathcal{H}$ with each member satisfying the above requirement, we follow the idea described in [8]. Specifically, each hash function $h_{\boldsymbol{\alpha},\beta}(\boldsymbol{v}):\mathcal{R}^D\rightarrow\mathcal{N}$ maps a D-dimensional vector $\boldsymbol{v}$ to the set of integers. In our scheme, $\boldsymbol{v}$ is the coordinate of a user and thus $D=2$. Each hash function in the family is indexed by a choice of random $\boldsymbol{\alpha}$ and β where $\boldsymbol{\alpha}$ is a 2-dimensional vector with entries chosen independently from a p-stable distribution and β is a real number chosen uniformly from the range $[0,r]$, where r is a fixed parameter of $\mathcal{H}$. The selection of r is discussed with details in [8]. For a pair of $\boldsymbol{\alpha}$ and β, the hash function $h_{\boldsymbol{\alpha},\beta}(\boldsymbol{v})$ is given by $h_{\boldsymbol{\alpha},\beta}(\boldsymbol{v})=\left\lfloor\frac{\boldsymbol{\alpha}\cdot\boldsymbol{v}+\beta}{r}\right\rfloor$. Following the result from [8], we have

$$P\big[h_{\boldsymbol{\alpha},\beta}(a)=h_{\boldsymbol{\alpha},\beta}(b)\big]=\int_0^r\frac{1}{d}f_p(\frac{t}{d})(1-\frac{t}{r})dt$$

where $f_p(t)$ denotes the probability density function of the absolute value of the p-stable distribution and d is the Euclidean distance between a and b.

In this paper, we adopt the Cauchy distribution as the 1-stable distribution as suggested in [8] (with $p=1$). It calculates that

$$p_i=2\frac{tan^{-1}(r/c_i)}{\pi}-\frac{1}{\pi(r/c_i)}\ln(1+(r/c_i)^2),\ i=1,2$$

where $c_1=\max\{\Gamma_a,\Gamma_b\}$ and $c_2=\delta\cdot\max\{\Gamma_a,\Gamma_b\}$.

B. Advanced Scheme

We consider the same scenario as our basic scheme, where there are only two SPs, SSP_A and SP_B. SU a queries SSP_A for SAI.

1) System Setup: The system setup in the advanced scheme is similar to that in the basic scheme. The only difference is that SSP_A and SP_B are further initialized with the LSH family $\mathcal{H}$, with each hash function $h_{\boldsymbol{\alpha},\beta}(\boldsymbol{v})$ constructed following the discussion in Section V-A.

2) Request and Computation: Once receiving a spectrum query $\{(x,y),[t^s,t^e],P^{\max}\}$ from SU a, SSP_A generates a's slotted service duration $SSD_a=\{a_1,\cdots,a_T\}$. It then picks a hash function $h_{\boldsymbol{\alpha},\beta}(\boldsymbol{v})$ from $\mathcal{H}$ and computes $\sigma_a=h_{\boldsymbol{\alpha},\beta}((x,y))$. It further encrypts SSD_a into $\boldsymbol{\theta}_a=\{\theta_{a_1},\ldots,\theta_{a_t},\ldots,\theta_{a_T}\}$, where $\theta_{a_t}=(g^{r_t},h^{a_t+r_t})$, and σ_a into $\zeta_a=(g^{r_a},h^{\sigma_a+r_a})$, all under ElGammal encryption. Then $\boldsymbol{\theta}_a$, ζ_a, pk_A, and the index of $h_{\boldsymbol{\alpha},\beta}(\boldsymbol{v})$ are sent to SP_B.

Similarly, SP_B generates slotted service duration for each user j it serves as $SSD_{j,b}=\{b_{j,1},\ldots,b_{j,Q}\}$. With the LSH function specified by SSP_A, SP_B calculates $\sigma_{j,b}=h_{\boldsymbol{\alpha},\beta}((x_{j,b},y_{j,b}))$. It further encrypts $SSD_{j,b}$ into $\boldsymbol{\theta}_{j,b}=\{\theta_{j,b_1},\ldots,\theta_{j,b_{t'}},\ldots,\theta_{j,b_{T'}}\}$, where $\theta_{j,b_{t'}}=(g^{\rho_{j,t'}},h^{\rho_{j,t'}-\nu_{j,t'}b_{j,t'}})$, and $\sigma_{j,b}$ into $\zeta_{j,b}=(g^{\rho_{j,b}},h^{\rho_{j,b}+\nu'_{j,b}\sigma_{j,b}})$. Note $\rho_{j,t'}$ and $\rho_{j,b}$ are randomly chosen from $\mathbb{Z}_p$. $\nu_{j,t'}$, $\nu'_{j,b}$ are non-zero numbers randomly chosen from $\mathbb{Z}_p$.

Denote by $\boldsymbol{\nu}_j$ the set $\{\nu_{j,1}, \ldots, \nu_{j,T'}\}$. For each $\boldsymbol{\theta}_{j,b}$ ($j \in [1, N_k]$), SP_B computes $\boldsymbol{\eta}_j$ as $\boldsymbol{\eta}_j = (\boldsymbol{\theta}_a)^{\boldsymbol{\nu}_j} \times \boldsymbol{\theta}_{j,b}$ following the process described in Section IV-B. It also computes η'_j as

$$\begin{aligned}
&\eta'_j = {\zeta_a}^{\nu'_{j,b}} \times \zeta_{j,b} \\
=&\big((g^{r_a})^{\nu'_{j,b}} \cdot g^{\rho_{j,b}}, (h^{\sigma_a + r_a})^{\nu'_{j,b}} \cdot h^{\rho_{j,b} - \nu'_{j,b}\sigma_{j,b}}\big) \\
=&\big(g^{r_a \nu'_{j,b} + \rho_{j,b}}, h^{(\sigma_a - \sigma_{j,b})\nu'_{j,b} + r_a \nu'_{j,b} + \rho_{j,b}}\big).
\end{aligned}$$

Finally, SP_B prepares $\boldsymbol{\eta} = \{\boldsymbol{\eta}_j | j \in [1, N_k], k \in [1, K]\}$, $\boldsymbol{\eta}' = \{\eta'_j | j \in [1, N_k], k \in [1, K]\}$ and sends them to SSP_A.

3) Result Retrieval and Filtering: Once receiving $\boldsymbol{\eta}, \boldsymbol{\eta}'$ from SP_B, SSP_A first decrypts $\boldsymbol{\eta}'$ with its private key $\mathtt{sk}_A$. For an element $\eta'_j \in \boldsymbol{\eta}'$, it is decrypted by

$$\begin{aligned}
&D({\zeta_a}^{\nu'_{j,b}} \times \zeta_{j,b}) \\
=&\big(g^{r_a \nu'_{j,b} + \rho_{j,b}}\big)^{-\mu} \cdot (h^{\sigma_a + r_a})^{\nu'_{j,b}} \cdot h^{\rho_{j,b} - \nu'_{j,b}\sigma_{j,b}} \\
=&h^{-r_a \nu'_{j,b} - \rho_{j,b}} \cdot h^{(\sigma_a - \sigma_{j,b})\nu'_{j,b} + r_a \nu'_{j,b} + \rho_{j,b}} \\
=&h^{(\sigma_a - \sigma_{j,b})\nu'_{j,b}}.
\end{aligned}$$

For each spectrum k, SSP_A checks if $D({\zeta_a}^{\nu'_{j,b}} \times \zeta_{j,b}) \stackrel{?}{=} 1$. If it is not, it's very likely that neither SU a nor user j is within the interference range of the other. Therefore, spectrum k is available to SU a. If $D({\zeta_a}^{\nu'_{j,b}} \times \zeta_{j,b}) = 1$, SSP_A further decrypts $D(\boldsymbol{\eta})$ and checks if any element is 1. If there is, spectrum k is unavailable to SU a, because a interferes with j in the both spatial and temporal domains; otherwise, spectrum k is safe to allocate to a.

After deriving the available spectrum set for SU a from the perspective of SP_B, SSP_A needs further filter out the spectrums that cause interference to its other served SUs following the similar process in the basic scheme.

C. Enhance the Scheme Accuracy

To have (1) accurately capture the interference relation between user a and b, we should have p_1 close to 1 and p_2 close to 0. Otherwise, the chance will be pretty high to mistake interfering users as interference-free ones (i.e., false negative) and interference-free users as interfering ones (i.e., false positive). To enhance the scheme accuracy, a sufficient gap between p_1 and p_2 is desirable. For this purpose, we plan to adopt the AND-OR amplification method described in Section II-A. A new LSH family $\mathcal{F}''$ is generated based on $\mathcal{H}$, with $p'_1 = 1 - (1 - p_1^{k_1})^{k_2}$ and $p'_2 = 1 - (1 - p_2^{k_1})^{k_2})$. Correspondingly, (1) is replaced by

$$\begin{cases}
P\big[f''_i(a) = f''_i(b)\big] \geq p'_1, \text{ if } d(a,b) \leq \max\{\Gamma_a, \Gamma_b\}, \\
P\big[f''_i(a) = f''_i(b)\big] \leq p'_2, \text{ if } d(a,b) \geq \delta \cdot \max\{\Gamma_a, \Gamma_b\}.
\end{cases}$$

With properly chosen k_1 and k_2, p'_1 and p'_2 could be approximate to 1 and 0, respectively. Hence, the false positive and false negative will be greatly decreased[2]. Under the new $\mathcal{F}''$, the advanced scheme is modified slightly. Specifically, when SSP_A picks a hash function f'' from $\mathcal{F}''$, it actually contains $k_1 \times k_2$ $h_{\boldsymbol{\alpha},\beta}$'s. Therefore, $f''((x,y))$ is an LSH vector with $k_1 \times k_2$ elements. Notice that $\sigma_a = h_{\boldsymbol{\alpha},\beta}((x,y))$ is a single value in the advanced scheme. With the introduction of $\mathcal{F}''$, the computation complexity of the scheme thus increases. However, as shown in the simulation result, small values of k_1 and k_2 (≤ 5) will be sufficient to guarantee a satisfying scheme accuracy.

[2]In an ideal case, where $p'_1 = 1$ and $p'_2 = 0$, there is neither false positive nor false negative.

VI. Analysis

A. Privacy Analysis

We now analyze what values are known by SSP_A and SP_B in the basic scheme, and if they can reveal the operational parameters of SU a and user j. The privacy analysis of the advanced scheme similarly follows.

For SP_B, the values it receives from SSP_A regarding SU a's operational parameters include $\boldsymbol{\theta}_a$, $\boldsymbol{\gamma}_a$. Specifically, for an element $\theta_{a_m} \in \boldsymbol{\theta}_a$, it is an ElGamal encryption over a_m. Under the DDH assumption, a_m cannot be inferred by SP_B and thus a's operational parameters. Similarly, SP_B cannot infer a's operational parameters from $\boldsymbol{\gamma}_a$ either.

For SSP_A, the values it receives from SP_B regarding user j's operational parameters include $(a'_{m'} - b_{j,q})\nu_{j,q}$'s and $(a_m - b'_{j,q'})\nu'_{j,q'}$'s. For $(a'_{m'} - b_{j,q})\nu_{j,q}$, it is either 0 if $a'_{m'} = b_{j,q}$ or a random non-zero value in $\mathbb{Z}_p$ if $a'_{m'} \neq b_{j,q}$. When $a'_{m'} \neq b_{j,q}$, this reveals no other information about $b_{j,q}$ and thus j's operational parameters.

B. Performance Analysis

1) Simulation Setup: Simulations are conducted under Windows 10 on a computer with 2.6 GHz CPU and 16 GB RAM. The scheme is implemented based on the Crypto++ Library. The 2048-bit ElGamal encryption is applied.

We consider a square region with the size of 1000m$\times$1000m. There is one query SU and 10 incumbent users, all of which are randomly distributed. We assume all users share the same transmission range as 100m, interference range as 150m, and the service duration of one time slot. Besides, there is only one spectrum in the system. All the simulation results are obtained as the average value of 10^4 times of independent experiments.

2) Efficiency: Fig. 7(a) depicts the computation time of SSP_A and SP_B in the basic scheme under different values of grid length L. First of all, both of them decreases fast as L increases, because the number of cubes contained in SURs and CRs decreases. Accordingly, the number of equality test in the scheme decreases. Second, the computation time at SSP_A and SP_B is quite similar. Specifically, the computation carried out at SSP_A includes the calculation of $\boldsymbol{\theta}_a$, $\boldsymbol{\gamma}_a$, $D(\boldsymbol{\eta}_j)$ and $D(\boldsymbol{\eta}'_j)$, while the computation carried out at SP_B includes $\boldsymbol{\theta}_{j,b}$, $\boldsymbol{\gamma}_{j,b}$, $\boldsymbol{\eta}_j$, $\boldsymbol{\eta}'_j$. Fig. 7(b) compares the computation time of the basic scheme and the advanced scheme. The computation time of the advanced scheme remains at a constant value 193.6ms as L increases. This is because in order to determine if two users conflict with each other in the spatial domain, the

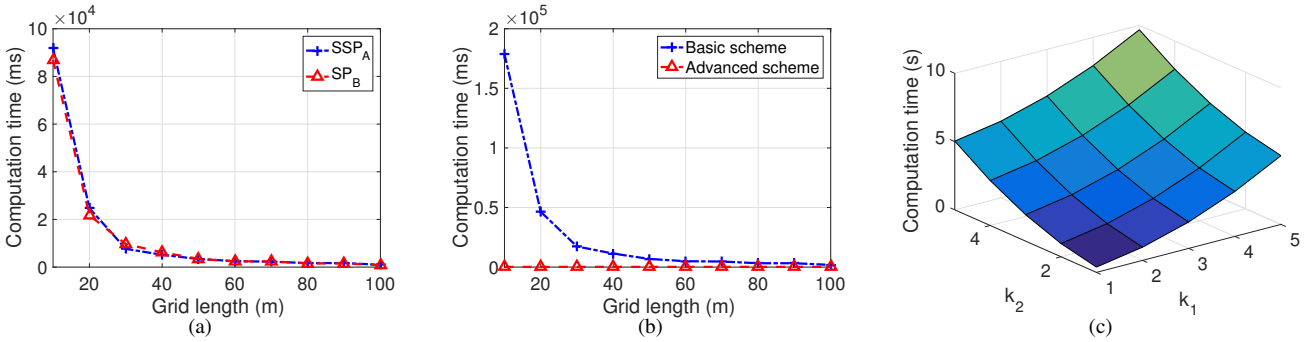


Fig. 7. Scheme performance on computation time.

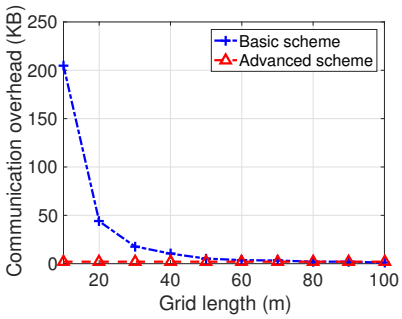


Fig. 8. Communication overhead under different grid lengths.

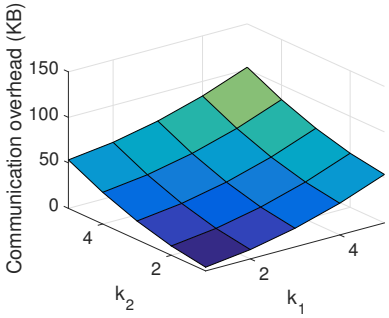


Fig. 9. Communication overhead under different k_1's and k_2's.

advanced scheme compares the LSH values of these users' coordinates, which does not rely on their SURs and CRs. Fig. 7(c) evaluates the computation time of the advanced scheme under different values of k_1 and k_2. Recall that k_1 and k_2 are the numbers of LSH functions included in the new LSH family $\mathcal{F}''$ for amplification. We notice that with a fixed $k_1(k_2)$, the computation time grows quadratically as $k_2(k_1)$ increases.

We further compare the communication overhead of the two schemes in Fig. 8. The value for the basic scheme increases fast when L gets smaller. This is because the number of elements contained in $\boldsymbol{\theta}_a$ and γ_a (transmitted from SSP_A to SP_B) and $\boldsymbol{\eta}$, $\boldsymbol{\eta}'$ (transmitted from SP_B to SSP_A) increases. Fig. 9 shows the communication overhead of the advanced scheme under different values of k_1 and k_2. We have the similar observation with the computation time.

3) Accuracy: We demonstrate in Fig. 10 accuracy performance of the advanced scheme under different k_1's and k_2's. Specifically, Fig. 10(a) shows the false positive rate. As in basic scheme, it indicates the probability that two interference-free users are determined as interfering users. Apparently, to achieve a low false positive rate and thus a higher frequency utilization, a large value of k_2 but a small value of k_1 is desirable. Fig. 10(b) shows the false negative rate, which indicates the probability that two interfering users are determined as interference-free users. Apparently, to achieve a low false negative rate and thus a transmission collision (caused by assigning the occupied spectrum to the query SU), a large value of k_1 but a small value of k_2 is desirable. Clearly, there is a tradeoff between these two rates when choosing k_1 and k_2. To evaluate this tradeoff, in Fig. 10(c) we show the overall accuracy, which is defined as 1 - *false positive rate* - *false negative rate*. According to the result, the overall accuracy achieves the highest value when $k_1 = 5, k_2 = 3$.

VII. Related Work

There have been some existing works on privacy-preserving spectrum query in database-driven CRNs. Gao et. al [2] are among the first to work on this problem. They construct the database as a matrix. The information stored in the a-th row and b-th column tells the SAI of location (a, b). Their scheme is developed based on private information retrieval (PIR) technique. Similar to [2], the database in [4] is also constructed as a matrix of SAI. However, the information contained in the a-th row and b-th column tells not only the SAI of location (a, b) but also the nearby locations' SAI for better efficiency. Also built on PIR, our previous work [3] further guarantees the authenticity of query SU's location via location proof. Still, the scheme imposes a special structure of the database. Specifically, the database consists of a stack of matrices. The a-th row and b-th column of a matrix only contains a single bit. The concatenation of all the bits in the a-th row and b-th column from all matrices compose the SAI for location (a, b). Apparently, the functionality of these schemes heavily rely on some particular structures of the database which are impractical. Besides, in these schemes the database has to be

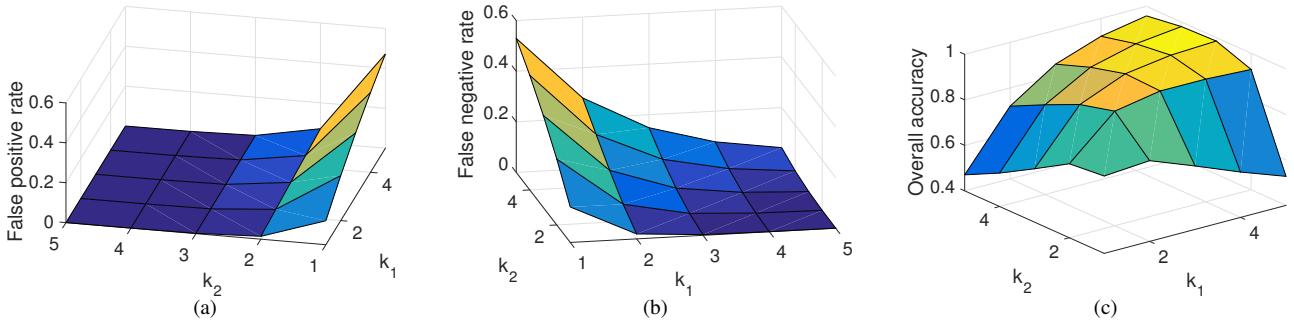


Fig. 10. Accuracy performance of advanced scheme.

updated entirely whenever any user joins or leaves the system. Although the work [5] does not impose any constraint over the database structure, it involves tedious cryptographic operations and intense interactions among system entities, rendering the scheme unfavorable for real applications. Zhang et. al [13] proposed to protect location privacy for both SUs and PUs location privacy. The idea is to add noise to a user's location. Apparently, it impacts spectrum query accuracy. Grissa et. al [14] developed the privacy-preserving scheme by leveraging Cuckoo filter. In addition to protect query SUs' location privacy, [15] also provides a way for the server to verify if the query SU locates at where it claims to be.

Note that all the above works only consider a single SP, i.e., all the incumbent users together with the query SU are all subscribed to this SP. In practical scenarios, however, heterogeneous SPs colocate in the same geographic area, making the privacy-preserving spectrum query a much more challenging task. And none of the proposed schemes has taken this into account.

VIII. Conclusion

In this paper, we discuss how to realize practical and privacy-preserving spectrum query in the database-driven CRNs with multiple service providers. We first develop our basic scheme based on PET. It allows SSP to allocate available spectrums to SUs without disclosing their operational parameters to other SPs. Noticing that the computation and communication cost of the basic scheme becomes heavy when there are many users and SPs in the system, we further develop an advanced scheme by integrating LSH. Finally, the simulation results demonstrate the effectiveness and efficiency of our schemes.

References

[1] "Third memorandum opinion and order," http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0405/FCC-12-36A1.pdf, Federal Communications Commission, May 2012.

[2] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'09)*, Turin, Italy, 2013.

[3] J. Xin, M. Li, C. Luo, and P. Li, "Privacy-preserving spectrum query with location proofs in database-driven crns," in *Proceedings of Global Communications Conference (GLOBECOM'16)*, DC, US.

[4] E. Troja and S. Bakiras, "Efficient location privacy for moving clients in database-driven dynamic spectrum access," in *Proceedings of International Conference on Computer Communication and Networks (ICCCN'15)*, Las vegas, US, 2015.

[5] Y. Dou, K. C. Zeng, H. Li, Y. Yang, B. Gao, C. Guan, K. Ren, and S. Li, "P^2-sas: Preserving users' privacy in centralized dynamic spectrum access systems," *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'16)*, 2016.

[6] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in *Proceedings of 18th Annual Network & Distributed System Security Symposium (NDSS'11)*, San Diego, US, 2011.

[7] G. Zhuo, Q. Jia, L. Guo, M. Li, and Y. Fang, "Privacy-preserving verifiable proximity test for location-based services," in *Proceedings of IEEE Global Communications Conference (GLOBECOM'15)*, San Diego, US, 2015.

[8] M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni, "Locality-sensitive hashing scheme based on p-stable distributions," in *Proceedings of Annual Symposium on Computational geometry (SoCG'04)*, NY, US, 2004.

[9] Z. Feng and Y. Yang, "Joint transport, routing and spectrum sharing optimization for wireless networks with frequency-agile radios," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'09)*, Rio, Brazil, 2009.

[10] Y. T. Hou, Y. Shi, and H. D. Sherali, "Spectrum sharing for multi-hop networking with cognitive radios," *IEEE Journal on selected areas in communications*, vol. 26, no. 1, 2008.

[11] M. Li, S. Salinas, P. Li, X. Huang, Y. Fang, and S. Glisic, "Optimal scheduling for multi-radio multi-channel multi-hop cognitive cellular networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 1, pp. 139–154, 2015.

[12] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on information theory*, vol. 46, no. 2, pp. 388–404, 2000.

[13] Z. Zhang, H. Zhang, S. He, and P. Cheng, "Achieving bilateral utility maximization and location privacy preservation in database-driven cognitive radio networks," in *Proceedings of IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS'15)*, Dallas, US, 2015.

[14] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Cuckoo filter-based location-privacy preservation in database-driven cognitive radio networks," in *Proceedings of IEEE World Symposium on Computer Networks and Information Security (WSCNIS)*, Hammamet, Tunisia, 2015.

[15] Y. Li, L. Zhou, H. Zhu, and L. Sun, "Secure and privacy-preserving location proof in database-driven cognitive radio networks," in *Proceedings of International Conference on Wireless Algorithms, Systems, and Applications (WASA'15)*, Qufu, China, 2015.