Comparison of incumbent user privacy preserving technologies in database driven dynamic spectrum access systems

He Li, Yaling Yang, Yanzhi Dou, Chang Lu, Doug Zabransky, and Jung-Min (Jerry) Park

Virgina Tech, Blacksburg, VA, USA
{heli, yyang8, yzdou, changl7, dmz5e, jungmin}@vt.edu

Abstract. Database driven dynamic spectrum sharing is one of the most promising dynamic spectrum access (DSA) solution to address the spectrum scarcity issue. In such a database driven DSA system, the centralized spectrum management infrastructure, called spectrum access system (SAS), makes its spectrum allocation decisions to secondary users (SUs) according to sensitive operational data of incumbent users (IUs). Since both SAS and SUs are not necessarily fully trusted, privacy protection against untrusted SAS and SUs become critical for IUs that have high operational privacy requirements. To address this problem, many IU privacy preserving solutions emerge recently. However, there is a lack of understanding and comparison of capability in protecting IU operational privacy under these existing approaches. In this paper, thus, we fill in the void by providing a comparative study that investigates existing solutions and explores several existing metrics to evaluate the strength of privacy protection. Moreover, we propose two general metrics to evaluate privacy preserving level and evaluate existing works with them.

Keywords: Dynamic spectrum access · Privacy preserving technology.

1 Introduction

Using geolocation databases is one of the most practical approaches for enabling spectrum sharing. For example, to achieve dynamic spectrum access between Citizens Broadband Radio Service (CBRS) and government and non-government incumbents in 3.5 GHz band, a Spectrum Access System (SAS) is required to coordinate CBRS devices (CBSDs). Under SAS's coordination, CBSDs can satisfy the varying interference protection requirements of incumbent users (IUs), while maximizing the utilization of spectrum.

The operational privacy of IUs is crucial in this DSA paradigm, especially when IUs are federal government and military systems [9]. The Federal Communications Commission (FCC) and wireless innovation forum (WINNF) have regulatory requirements that the retention and disclosure of information related to IU operational privacy should be limited.

To satisfy these regulations of IU operational privacy, a few IU privacy preserving schemes have been proposed recently. These schemes can be divided into two categories. The first category, including [2–4, 11, 12], achieve their goals by obfuscating IUs' inputs to SAS. The second category achieves provable security through secure multi-party computation (MPC) protocols [7, 8], where IU inputs are encrypted before being sent to SAS and SAS performs spectrum computation on ciphertext domain without seeing the plaintext of IU operational data.

In this paper, we present a comparative study on the two existing categories of proposals, and we explore different existing security metrics for evaluating these existing works. Furthermore, we propose two new and generic metrics, named *minimum adversarial estimation error* and *indistinguishable input*, to evaluate IU privacy preserving level that can be applied across different schemes.

Through simulation study, we show that data obfuscation-based solutions provide better protection against adversarial SUs, yet offer worse spectrum utilization. Secure MPC-based solutions provides better protection against untrusted SAS and offer worse protection against adversarial SUs.

The rest of the paper is organized as follows: Section 2 presents the general system model and attack model. Section 3 introduces existing works. Section 4 proposes our security metrics evaluating IU privacy protection strength. Section 5 presents the comparison on privacy preserving strength for existing works and section 6 concludes the paper.

2 System model

In this section, we introduce the general system model and attack model for an IU privacy preserving DSA system.

2.1 Model of Database driven dynamic spectrum access system

In this paper, we assume a general DSA service model, which consists of three entities: incumbent users (IUs, also known as "primary users" in some literature), Spectrum Access System (SAS), and secondary users (SUs). IUs update their operational status to SAS. SAS handles spectrum request from SUs by running a spectrum computation functionality $f(\cdot)$ that performs admission control for SUs. $f(\cdot)$ may also include channel assignment and/or power assignment operations. This system model summarizes the system models used in all existing privacy-protection works, including [2–4, 7, 8, 11, 12].

2.2 Attack models

There exist several types of attackers focusing on breaking IU operational privacy in a database driven DSA system:

A1: (Intruders) the attacker is an intruder, which is not any entity in the DSA system. It can overhear, intercept, and synthesize any message exchanged across the network. Specifically it may directly extract IU operational status by

looking at the messages sent from IUs to SAS. This threat model is also referred to as "Dolev-Yao model" [6]. Under this threat model, exchanging all messages under secure channels (e.g using TLS) can provide confidentiality, which ensures IU privacy. Thus, existing works are not focusing on proposing countermeasures towards this type of attack.

A2: (Honest but curious SAS, or semi-honest SAS) the adversary is a faithful SAS. While it performs all spectrum computation faithfully, it is also interested in discovering the operational parameters of IUs from the information it receives from IUs. Under this attack model, IU privacy fails if IUs directly send their plain operational status to SAS. Works [3, 4, 7, 8] consider this attack model.

A3: (Adversarial SU network) the adversary controls a group of compromised SUs, so that it can obtain their spectrum request results to infer IUs' operational parameters. This type of attack is also referred to as "database inference attack" [2], which is studied in [2–4, 11].

A4: (Malicious colluding SAS) the adversary controls both a group of compromised SUs and a malicious SAS. The malicious SAS would deviate from the protocol to allure SUs to generate other observations to further infer IUs' operational status. In [7] such kind of attack is discussed.

3 Existing works

In this section, we will introduce existing solutions for IU privacy protection.

3.1 Overview of existing works

Data obfuscation techniques: When we consider attacks that focus on inferring IU operational status, the straightforward countermeasure is to obfuscate the inputs from IUs to SAS by adding noise or distortion to the input data.

For example, in order to prevent adversaries from deriving an IU's location by the radius of its protection zone, [2, 11] propose to replace k IUs' individual protection zones by a super-size protection contour that encloses these k individual protection zones. Thus, IU location privacy protection in terms of k-anonymity can be provided under these schemes.

Another approach is to directly add noise to the actual IU operational parameters before executing spectrum computation functionality $f(\cdot)$. In [3, 4], such strategies are briefly discussed. In [12], a structured noise is added to the true location of IUs, so that differential location privacy is preserved for IUs.

It is also proposed in [3, 4] to add fake IU entries to the database. As a result, both adversarial SAS and SUs will not be able to distinguish those false entries from the true IU entries.

Essentially, applying data obfuscation techniques achieves IU privacy protection at a cost of SU spectrum utility. In [2, 4, 11], simulation results show that data obfuscation techniques can achieve an advantageous trade-off in their simulation setup. However, it is not deeply studied on how to choose proper obfuscation techniques and how to set parameters for them. In [4], an optimization

problem is setup to study this issue, but the authors also claimed it may not be practical to solve this optimization problem at runtime.

Secure multi-party computation based schemes: The basic idea of a secure multi-party computation (MPC) based solution for DSA system is for IUs to first encrypt their operational parameters by homomorphic cryptosystems before sending the encrypted parameters to SAS. SAS then executes spectrum computation functionality $f(\cdot)$ in ciphertext domain by leveraging the homomorphic property of the cryptosystems. The confidentiality properties of the underlying cryptosystems ensure that a semi-honest SAS is not able to extract any information from those encrypted messages.

In [8], such an MPC-based solution is proposed, where SAS is assumed to manage SU interference in "protection zone model", which ensures the aggregated interference generated from SUs to IUs does not exceed certain threshold. In [7], another MPC-based solution is proposed, where SAS is assumed to manage SU interference in "exclusion zone model", which ensures any spectrum request from an SU located in an exclusion zone will be declined.

3.2 Privacy metrics in existing works

A few metrics have been used in existing DSA privacy-preserving works. In this section, we introduce these metrics and discuss whether they are appropriate for comparative studies of multiple privacy-preserving schemes.

Average expected location estimation error [2, 4, 11]: Assume an attacker can obtain a probability density function $A(loc'|\mathcal{O})$ as the guess of an IU location given some observation $\mathcal{O}$. Assuming n_I IUs exist in a target region, the actual IU locations are used to partition the region into n_I subregions using the Voronoi diagram approach. These subregions are denoted as $\mathcal{L}_i$. The *average expected location estimation error* metric is defined as:

$$Pri := \frac{1}{n_I} \sum_{i=1}^{n_I} \sum_{loc \in L_i} d(loc_i, loc) \frac{A(loc|\mathcal{O})}{\sum_{loc' \in \mathcal{L}_i} A(loc'|\mathcal{O})}, \tag{1}$$

where loc_i is the true location of the ith IU, $d(\cdot, \cdot)$ is the distance between two locations. This metric is proposed in [4] and is widely applicable. [2] and [11] use a special case of the metric that assumes $n_I = 1$.

Privacy time [3]: Privacy time is a widely applicable metric that measures the degradation of location privacy level over time. It is the expected time that it takes for IU location estimation error to fall lower than a certain threshold.

Size of search space [4]: This is the size of search space of possible IU parameters. After collecting some observations, an adversarial SAS or SU can exclude some locations as possible IU locations, which means the search space of true

IU locations is reduced. This metric is essentially equivalent with a special case of the "expected location estimation error" metric where $A(loc'|\mathcal{O})$ is set to be a uniform distribution in the search space area.

ϵ-Differential privacy [12] : When an attacker obtain observation $\mathcal{O}$ and attempts to distinguish the true location of an IU between l_0 and l_1 within a circle with radius r, ϵ-differential privacy requires the likelihood ratio is lower than $e^{\epsilon r}$, where ϵ is the parameter of differential privacy and r can be any radius value smaller than the radius of service area.

The formal definition is given as follows[1]:

$$\frac{P(\mathcal{O}|l_1)}{P(\mathcal{O}|l_0)} \leq e^{\epsilon r} \qquad \forall r > 0 \; \forall l_1, l_0 : d(l_1, l_0) \leq r. \tag{2}$$

This metric, however, cannot be applied in DSA systems where the interference management policy of SAS protects IUs from harmful interference. For example, when $\mathcal{O}$ is a positive response for an SU query at location l_0 and l_0 is extremely close to an IU at the same time, it is easy to see that the denominator $P(\mathcal{O}|l_0)$ in equation (2) must be 0, which makes differential privacy unachievable. Since most of the existing privacy-preserving works [2–4, 7, 8, 11] except [12] are designed for systems where harmful interference to IUs is strictly prohibited, ϵ-differential is not a suitable metric for comparative study of DSA privacy schemes.

Provable security with the cryptographic setting [7, 8]: By defining provable security with the cryptographic setting for a privacy preserving DSA system, we attempt to abstract the attack model and formulate any attacker under this model as an adversarial algorithm $\mathcal{A}$. When the provable security is achieved, we expect that any probabilistic polynomial time (PPT) adversarial algorithm $\mathcal{A}$ cannot achieve its goal at a non-negligible probability. Note that we call these security features "provable" because usually we attempt to prove that it is at least harder for an adversary to achieve its goal, compared to breaking a secure cryptosystem or other underlying hard problems.

In [7, 8], provable security feature on IU operational privacy protection is proposed and proved. However, security definitions in [7, 8] are also tailored definitions towards a specific interference management policy ("protection zone" and "exclusion zone" respectively). We hereby propose a general definition of "indistinguishable input" in section 4 to ensure wider applicability.

4 Proposed security metric

In this section, we propose two additional metrics to evaluate the level of IU operational privacy. These two metrics are named *minimum adversarial estimation error* and *indistinguishable input*.

[1] There are three equivalent definitions proposed in [1], and in this paper we show the third one.

4.1 Minimum adversarial estimation error

Suppose M IUs are operating with parameter sets $P_1^*, \cdots, P_M^* \in \mathcal{P}$, where $\mathcal{P}$ is the set of parameters with all possible values. An adversary $\mathcal{A}$ can obtain a posterior distribution of IUs' true parameters through its observations $\mathcal{O}$, which are obtained from compromised SAS or SUs. We denote $p_{\mathcal{A}}(\mathcal{P})$ as the posterior probability and

$$p_{\mathcal{A}}(\mathcal{P}) := \Pr[\text{IUs' operational parameter set}= \mathcal{P} | \mathcal{A} \text{ observes } \mathcal{O}], \tag{3}$$

where $\mathcal{P} := \{P_j\}_{j=1}^{M}$.

We assume that the adversary would sample a parameter set based on the posterior distribution $p_{\mathcal{A}}(\mathcal{P})$ as its guess of the IUs' true operational parameter sets. The privacy preserving level (PPL), thus, can be defined as the expectation of the minimum estimation error, which is the minimum distance between any true IU parameters and any adversarial guess. That is,

$$PPL := E\left[\min_{i\in[M]} \min_{j\in[M]} d(P_i, P_j^*)\right]. \tag{4}$$

The above privacy preserving metric definition extends the "expected location estimation error" concept to privacy protection of any IU operational parameter. In addition, compared to the "average expected location estimation error" discussed in section 3.2, this metric evaluates the minimum estimation error among multiple IUs.

Since different privacy preserving techniques have different format of observations and will result in different posterior distribution of IU parameters from the adversary's point of view, it is not efficient or possible to derive a closed-form math expression of the PPL. Thus, we choose to use numerical method to obtain PPL value. Specifically, note that given the specification of a privacy-preserving system, it is straightforward to generate a large set of possible adversary observations $\mathcal{O}$ for any given IU parameter set P^*. We can therefore employ Markov Chain Monte Carlo(MCMC) [10] method to generate samples of posterior distribution of IU parameters, and use them to obtain an approximate PPL.

4.2 Indistinguishable Input

We introduce the new metric called *indistinguishable input* to extend the concept of provable IU operational security, so that it can be applied on evaluating more privacy preserving DSA solutions under different attack models. Indistinguishable input requires that an adversary is not able to extract much information about an IU's operation parameters (e.g. location, transmit power, etc.) from this IU's input to SAS. In other words, indistinguishable input says that when SAS receives a message from an IU, the likelihoods that the message is generated under two different IU operational parameter settings are *almost* the same.

To formally define this metric, we setup the following guessing game:

- Initialization phase: setup the DSA system faithfully.

- Challenge phase: an adversary (e.g. a compromised SAS) chooses two arbitrary different IU operational parameters P_0 and P_1 on its will. IU picks a random bit $b \leftarrow_{\$} \{0, 1\}$ and sends the corresponding IU input $\mathcal{I}_b$ to the adversary.
- Finalization phase: the adversary attempts to find out the secret bit b and return its guess b^*. We say the adversary wins the game if $b^* = b$.

Indistinguishable input means that any adversary cannot win the above game with an effectively higher probability than randomly guessing. Formally, if for any polynomial time algorithm $\mathcal{A}$ through which the adversary wins the above game at a probability $\epsilon_{\mathcal{A}}(\lambda)$ (λ is the security parameter of underlying cryptosystem), a design that has indistinguishable input property must ensure $\max_{\mathcal{A}} \left|\epsilon_{\mathcal{A}}(\lambda) - \frac{1}{2}\right|$ is negligible. Here, "negligible" means that for any integer c, there exists some λ^* such that $\forall \lambda \geq \lambda^*$,

$$\max_{\mathcal{A}} \left|\epsilon_{\mathcal{A}}(\lambda) - \frac{1}{2}\right| < \frac{1}{\lambda^c}. \tag{5}$$

5 Comparisons on privacy preserving strength

In this section, we compare the security strength for existing works [2–4, 7, 8, 11]. We analyze the indistinguishable input property for all these works, and evaluate the average expected error, minimum adversarial estimation error and privacy time for all of them under attack model **A2** and **A3**.

As we have discussed in section 3.2, "search space size" metric is essentially equivalent to a special case of "expected location estimation error" metric, and ϵ-Differential privacy is not a suitable metric since it is not applicable to most of the existing works. Therefore, we are using these two metrics for evaluation.

Note that as we have discussed in section 2.2, the security threat in attack model **A1** can be thwarted by using secure channel, and the security threats in attack model **A4** has not been deeply studied in existing works. Therefore, we are not evaluating existing works under these two attack models.

5.1 Comparison based on indistinguishable input property

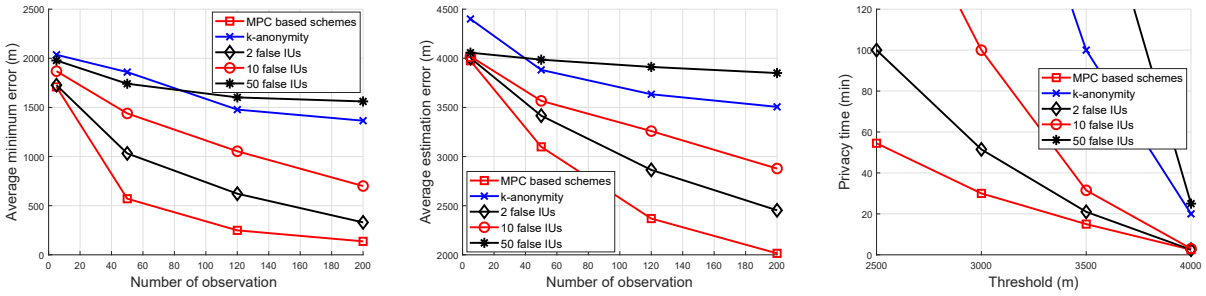
Under attack model **A2**, indistinguishable input property is only achieved for secure MPC protocol based schemes [7, 8]. This is because the obfuscated IU operational status still leaks non-negligible information. In the challenge phase of guessing game, a semi-honest SAS can generate two IU parameter sets that lead to different obfuscated results and directly distinguish them.

Under attack mode **A3**, when adversarial SUs are taken into consideration, indistinguishable input property is not expected to be achieved for all existing schemes. Under this attack model, what an adversary can obtain includes the final spectrum allocation results. Meanwhile under any DSA service model, the spectrum allocation result changes if the IU operational status changes. Hence, by synthesizing the spectrum allocation results, an adversary is able to distinguish IU operational statuses under different scenarios.

5.2 Comparison using adversarial estimation error and privacy time

The comparative study in this subsection is based on simulation. In the simulation setting, IUs are deployed in a 20 km by 20 km rectangular region and there is one channel centered at frequency 3600MHz. The IUs are military radars with 50m height and -80 dBm interference threshold; SUs are assumed to be outdoor CBSD devices and their antenna heights are 6m and transmission powers are 24 dBm. ECC-33 model [5] is used to formulate the path loss. The adversary collects two SU observations per minute.

We firstly compare the privacy preserving strength under attack model **A3**, i.e. attacker is an adversarial SUs network. Figure 1 compares the privacy preserving strength of MPC-based schemes [7, 8], obfuscation-based schemes designed for k-anonymity [2, 11], and obfuscation-based schemes that add false IU entries [3, 4]. MPC-based schemes behave the worst in this case since essentially in the perspective of an adversarial SU network, the secure MPC protocols in [7, 8] do not affect the spectrum computation result and hence introduce no additional confusion for the adversary to infer IU's operational parameters.



(a) Minimum error (b) Average error (c) Privacy time

Fig. 1: Privacy preserving strength evaluation under attack model **A3**.

We then compare the privacy preserving strength under attack model **A2**, i.e. attacker is a semi-honest SAS. Table 1 shows the privacy preserving strength against semi-honest SAS between different approaches. For MPC-based schemes in [7][8], we assume that an adversary cannot break a cryptographic system and can only obtain inferred IU locations by randomly guessing.

In the table, we see that MPC-based schemes provide strong IU privacy protection against semi-honest SAS. Obfuscation schemes designed for k-anonymity do not grant strong privacy protection under attack model **A2**, compared to the same simulation setting under attack model **A3**. This is because when a semi-honest SAS has the full knowledge on k-anonymity algorithm and the equivalent protection zone information, it can estimate the true IU locations with much smaller error. For obfuscation-based schemes that add false IU items, it can be observed that the privacy preserving strength increases with more false IUs. Yet,

intuitively we also expect the spectrum utility will decrease in this case, which will be analyzed in the next subsection.

Table 1: Privacy preserving strength under attack model **A2**.

	Minimum estimation error(m)	Average estimation error(m)
MPC-based schemes	1743.02	4006.33
k-anonymity	509.52	2394.24
Obfuscation(2 false IUs)	0	599.83
Obfuscation(10 false IUs)	71.07	2618.74
Obfuscation(50 false IUs)	701.96	3453.90

5.3 Comparison based on spectrum utilization

In this subsection we compare the spectrum utilization for different privacy-preserving approaches. Table 2 shows the privacy preserving strength measured in minimum estimation error and spectrum utilization between different privacy preserving solutions. We observe that MPC-based schemes provide highest spectrum utilization and they also grant strong privacy protection against semi-honest SAS. For obfuscation-based schemes, we observe a trade-off between privacy protection and spectrum utilization under both **A2** and **A3** attack models. We also observe that schemes designed for k-anonymity sacrifice most spectrum utilization to achieve strong privacy protection under attack model **A3**.

Table 2: Spectrum utilization and privacy protection.

	Spectrum utilization(%)	Minimum estimation error(m)	
		Attack model **A2**	Attack model **A3**, 120 queries
MPC-based schemes	95.56	1743.02	249.14
k-anonymity	51.68	509.52	1478.35
Obfuscation(2 false IUs)	93.89	0	622.07
Obfuscation(10 false IUs)	87.92	71.07	1054.89
Obfuscation(50 false IUs)	62.67	701.96	1602.70

6 Conclusion and Discussions

In this paper, we present a comparative study on existing solutions that preserves incumbent user's operational privacy. We additionally propose minimum adversarial estimation error metric to evaluate privacy preserving strength, and we propose the indistinguishable input property to generalize the concept of provable security. Our study shows the effectiveness of MPC-based solutions against

attacks from semi-honest SAS, and the trade-off between spectrum utilization and privacy preserving strength for obfuscation-based solutions. We also discover that obfuscation-based scheme provide stronger privacy protection against malicious SUs compared to MPC-based schemes. Combining both MPC-based and obfuscation-based schemes so that both adversarial SAS and SUs can be handled can be an interesting and promising future direction for IU operational privacy protection.

Acknowledgements. This work was partially sponsored by NSF through grants 1547366, 1265886, 1547241, 1563832, and 1642928.

References

1. Andrés, M.E., Bordenabe, N.E., Chatzikokolakis, K., Palamidessi, C.: Geo-indistinguishability: Differential privacy for location-based systems. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. pp. 901–914. CCS '13, ACM, New York, NY, USA (2013)
2. Bahrak, B., Bhattarai, S., Ullah, A., Park, J.M., Reed, J., Gurney, D.: Protecting the primary users' operational privacy in spectrum sharing. In: Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on. pp. 236–247. IEEE (2014)
3. Clark, M., Psounis, K.: Can the privacy of primary networks in shared spectrum be protected? In: Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on. pp. 1–9. IEEE (2016)
4. Clark, M.A., Psounis, K.: Trading utility for privacy in shared spectrum access systems. IEEE/ACM Transactions on Networking (TON) **26**(1), 259–273 (2018)
5. Committee, E.C., et al.: within the european conference of postal and telecommunications administration (cept)," the analysis of the coexistence of fwa cells in the 3.4-3.8 ghz band,". Tech. rep., tech. rep., ECC Report 33 (2003)
6. Dolev, D., Yao, A.: On the security of public key protocols. IEEE Transactions on information theory **29**(2), 198–208 (1983)
7. Dou, Y., Li, H., Zeng, K.C., Liu, J., Yang, Y., Gao, B., Ren, K.: Preserving incumbent users' privacy in exclusion-zone-based spectrum access systems. In: Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. pp. 2486–2493. IEEE (2017)
8. Dou, Y., Zeng, K.C., Li, H., Yang, Y., Gao, B., Guan, C., Ren, K., Li, S.: P 2-sas: preserving users' privacy in centralized dynamic spectrum access systems. In: Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing. pp. 321–330. ACM (2016)
9. the Office of the Federal Register (OFR), the Government Publishing Office.: Title 47: Telecommunication, part 96-citizens broadband radio service., `http://www.ecfr.gov/cgi-bin/text-idx?node=pt47.5.96&rgn=div5`
10. Robert, C.P.: Monte carlo methods. Wiley Online Library (2004)
11. Zhang, L., Fang, C., Li, Y., Zhu, H., Dong, M.: Optimal strategies for defending location inference attack in database-driven crns. In: Communications (ICC), 2015 IEEE International Conference on. pp. 7640–7645
12. Zhang, Z., Zhang, H., He, S., Cheng, P.: Achieving bilateral utility maximization and location privacy preservation in database-driven cognitive radio networks. In: Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on. pp. 181–189. IEEE (2015)