Preserving the Incumbent Users' Location Privacy in the 3.5 GHz Band

He Li, Yanzhi Dou, Chang Lu, Doug Zabransky, Yaling Yang, Jung-Min (Jerry) Park
Virgina Tech, Blacksburg, VA, USA
Email: {heli, yzdou, changl7, dmz5e, yyang8, jungmin}@vt.edu

***Abstract*—In dynamic spectrum sharing (DSS) ecosystem with non-informing incumbent users (IUs), Environmental Sensing Capability (ESC) system has been proposed to detect IU activity information for a geolocation database-driven spectrum access system (SAS). SAS then allocates unused spectrum left by IUs to secondary users (SUs). However, IU location information is often highly sensitive and thus it is preferable to avoid storing ESC sensing data on a SAS, especially if the SAS is a potential target of cyber attacks. None of existing works studied the IU location privacy protection problem in such an ESC-based dynamic spectrum access (DSA) system. In this paper, we fill in the void by proposing novel privacy-preserving ESC-based dynamic spectrum access (PriDSA) schemes. We designed two versions of PriDSA that preserve IU privacy to different extent under two different adversary models, namely non-colluding honest but curious SAS model and colluding malicious SAS model. Evaluation results show that PriDSA is efficient in terms of communication and computation overhead and accurately serves SU spectrum access requests while preserving location privacy of IUs.**

***Index Terms*—Dynamic spectrum access; Location privacy; Environmental Sensing Capability.**

I. Introduction

The Federal Communications Commission (FCC) has prescribed the creation of a Citizens Broadband Radio Service (CBRS) in the 3.5 GHz band (3500 - 3700 MHz) to enable spectrum sharing between federal and commercial systems [1]. In the scenario of 3.5 GHz CBRS along U.S coastal areas, Environmental Sensing Capability(ESC) systems are setup to detect the presence of federal incumbent users (IUs). ESC systems inform the presence of IUs to a Spectrum Access System (SAS) which coordinates CBRS devices' (CBSDs') access to the 3.5 GHz band. Meanwhile, SAS and ESC have to guarantee that CBSDs, essentially the Secondary Users (SUs), do not generate harmful interference to IUs.

One of the critical concerns of the above ESC-based DSA system is the IUs' location privacy issue. IUs in 3.5GHz band are often military systems, like shipborne radars. Location of these IUs are part of their operational characteristics. So, breaking location privacy of IUs directly leads to the failure of CBRS operational security. The wireless innovation forum(WINNF) has been developing requirements for *CBRS operational security* in [2], which aims at preventing adversaries from leaning information about IUs.

Existing works that attempt to address the IU location privacy protection problem can be divided into two categories. The first category [3][4][5] adds noise or distortion on IU location data before the data is sent to SAS. The second category [6][7][8] encrypts IU location data using homomorphic cryptosystem, so that SAS can homomorphically perform spectrum allocation computation on ciphertext domain without needing to see the underlying plaintext location data. Both categories of works, however, assume that IU must actively participate in the spectrum allocation process. The first category relies on IUs to add noise to their data according to their privacy needs and true location. The second category depends on IUs to encrypt its true location data.

None of these existing work can handle the non-informing IU cases in 3.5 GHz band, where IUs do not directly interact with the DSA system. In 3.5 GHz paradigm, SAS obtains information related to IU presence from ESC. The inputs from ESC to the SAS are IU signal detection events, not IU location information as in existing works. Thus, distortion logics used in category one of existing work cannot be applied on ESC input and the homomorphic computation over IU location inputs in category two of existing work also are not applicable.

To fill in the void of existing work, in this paper, we focus on preserving IU privacy under untrusted SAS scenario for ESC-based DSA systems. We consider two different attack models with different assumptions about attacker capability: non-colluding honest but curious (HBC) SAS model, and colluding malicious SAS model. We designed two schemes, called PriDSA-v1 and PriDSA-v2, to tackle these two different cases. We leverage the partial homomorphic feature of a proxy re-encryption scheme to preserve IU privacy and achieve the goal of dynamic spectrum sharing at the same time. In PriDSA-v2, we additionally blind IU inputs to prevent malicious colluding SAS from extracting information from any single ESC input; spectrum allocation is achieved by leverage a commitment system, where only the overall blinding of data can be removed. We provide formal proofs to show the level of privacy that each PriDSA scheme provides.

Our contributions can be summarized as follows:

1) We propose PriDSA, a framework for ESC-based DSA system to address the IU location privacy issue with untrusted SAS. Both PriDSA-v1 and PriDSA-v2 achieve guaranteed IU location privacy under non-colluding honest but curious SAS assumptions, and PriDSA-v2 can further reduce IU privacy degradation caused by colluding and malicious SAS.
2) We propose the concept of individual ESC operational security in ESC-based DSA systems, which provides a

novel approach to protect IU privacy under colluding SAS and SUs.

3) We provide evaluations to show that PriDSA is efficient and scalable, and show that PriDSA does not sacrifice spectrum allocation accuracy for a higher level of privacy.

The remainder of the paper is organized as follows. Section II reviews related works. Section III introduces the system model and the design objective. Section IV provides background information and Section V, VI present technical details on PriDSA-v1 and PriDSA-v2, respectively. Formal security definitions and corresponding analysis are presented in Section VII. Evaluations are provided in section VIII. Conclusions and discussion of future work are offered in Section IX.

II. Related Work

In [6],[8] and [7], efficient secure multi-party computation protocols are proposed, where partial homomorphic features of Paillier cryptosystem are leveraged for IU privacy protection. These solutions are based on non-colluding honest but curious adversary model. These schemes provide no privacy protection when SAS can collude with an SU.

Another group of approaches [3][4][5] focus on designing data obfuscation techniques. Assuming IU locations are known, these schemes add obfuscation noises on IU Ezone information to protect IU location privacy. Their assumption that IU locations are known makes them not applicable to DSA systems that are based on ESC and have non-informing IUs.

All of the above schemes require IUs to actively exchange messages with SAS and perform some computation based on accurate knowledge of IU operational data. Thus, they cannot handle the non-informing IU case, where IU does not interact with SAS and SU, and IU information can only be partially sensed by ESC.

III. System Model and Security Properties

A. System Model

We consider 3.5 GHz spectrum sharing paradigm, consisting of a spectrum access system (SAS), IUs, environmental sensing capability (ESC) system distributed in the service area of SAS, and SUs. We assume that IUs are non-informing. In the ESC-based SAS system, the ESC sensors are deployed in the vicinity of the predefined exclusion zones, which conservatively protects IUs from harmful interference. The ESC system converts part of exclusion zones to protection zones, where ESC detects the existence of IUs through spectrum sensing and SUs can get their spectrum requests approved in those areas based on the sensing result.

B. Inputs from ESC to SAS

In this paper, we assume an ESC system firstly identifies areas where an SU does not violate the spectrum access rules and hence can operate. We call such areas as safe zones. ESC determines safe zones based on its sensing results and default parameters of IUs. Protection zones are essentially areas outside of the safe zones.

Note that WINNF requires that the information relevant to federal activity passed from an ESC to a SAS shall be limited to protection area, channel, effective time, allowed retention time, and protection level [9]. The concept of safe zone indicates the protection level and area and hence fulfills the requirement in [9]. In the following subsection, we give an example on how an ESC sensor determines safe zones.

C. Example of determining safe zone

Figure 1 illustrates our example of determining safe zone. The black dot at the center of Figure 1 (a) and (b) is an ESC sensor. $\mathcal{R}_{max}$, which is marked by the dashed line, is the maximum sensing area of the ESC sensor. An IU located outside of $\mathcal{R}_{max}$ cannot be sensed by the ESC. An IU inside $\mathcal{R}_{max}$ can be detected by ESC and its distance to the ESC, denoted as d_0, can be computed based on ESC sensing result as follows.

Set the ESC sensor's location to be the origin of a 2-dimensional polar coordination system. Denote the path loss between any other polar location (d, θ) and the origin as $G_f(d, \theta)$ in dBm, where θ is the polar angle, d is the radical distance, f is the center frequency and $G_f(d, \theta)$ can be obtained from any radio propagation model or software. Assume that the ESC sensor senses that the received signal strength of an IU at frequency f is ψ dBm. The ESC sensor can calculate its possible distance to the IU, denoted as d_0, by

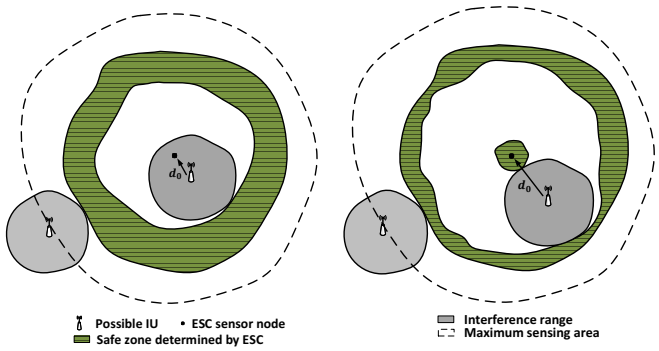
$$P_{IU} - \psi = G_f(\theta, d_0) \Longrightarrow d_0(\theta) = G_f^{-1}(\theta, P_{IU} - \psi), \quad (1)$$

where $G_f^{-1}(\theta, \cdot)$ is the inverse function of $G_f(\theta, \cdot)$, and P_{IU} is the default transmission power of IU, which is assumed to be known by ESC.

For each possible IU location (d, θ), ESC can obtain an interference range, which is the area where an operating SU would impose harmful interference on this possible IU location. We denote the interference area as $O_f(d, \theta)$ and show it as a gray area in Figure 1. The aggregation of all such gray areas over all possible IU positions (i.e. $\mathcal{O} = \cup_{\theta \in [0, 2\pi), d \in \{d_0, radius(\mathcal{R}_{max}, \theta)\}} O_f(d, \theta)$) form the non-safe zone and is colored white in figure 1. The safe zone that can be determined by the ESC sensor, hence, can be defined as $\mathcal{T} = \mathcal{R}_{max} - \mathcal{O}$ and is shown as the green area in figure 1. If an ESC sensor senses multiple IUs operating on the same frequency in its sensing range, it firstly computes the safe zone for each sensed IU signal, and then computes the intersection of all safe zones as the final sensing result passed to SAS.

It is important to note that the safe zones discovered by a single ESC are determined in a conservative way: those safe zones do not have intersection with any possible interference ranges. Hence, other ESC's sensing result will not change their safe zone status.

SAS then integrates all ESC input by taking the union of all ESC sensors' final safe zone sensing results. Figure 2 shows an example of aggregated safe zone information from multiple ESC sensors across a $20km \times 20km$ area. The white areas in the map are areas that no ESC is capable of defining them as the safe zone and are essentially the protection zones.



(a) when ESC detects a strong IU signal (b) When ESC detects a relatively weak IU signal

Fig. 1: Example of ESC determining safe zones.

SAS then performs DSA spectrum allocation according to this integration results, such that SAS will not allow SUs to access spectrum in protection zone areas.

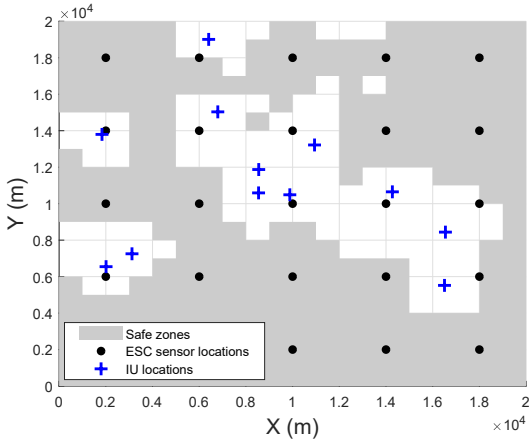


Fig. 2: Safe zone determined by ESC over $20km \times 20km$ area

D. Attack Model

In this paper, we assume that SAS is not trustworthy/can be compromised and our goal is to protect IU location privacy from untrustworthy SAS. As shown in figure 1, SAS can violate IU location privacy by examining the safe zone information submitted by ESC sensors. This is because the inner radius of the safe zone, denoted as d_0, is the distance between an ESC sensor and an IU whose signal is sensed by the ESC. When an IU's signal is detected by three ESC sensors, the three safe zones submitted by the three ESC sensors can lead to three such d_0 estimations. A trilateration localization algorithm then can be used to pinpoint the location of the IU. This observation shows that the safe zone information from ESC sensors can be a significant threat to IU privacy when SAS operator is not trusted.

We study two attack models with ascendantly more powerful attacker capability and designed two different countermeasure schemes for these models.

- **Honest but curious (HBC) SAS Model:** This model assumes that SAS does not collude with SUs and follows protocols faithfully. Yet, it may attempt to derive sensitive IU location data from information that it receives. Our PriDSA-v1 scheme tackles this attack model.
- **Colluding malicious SAS Model:** This model assumes that SAS may collude with a small number of SUs in order to break the location privacy of IUs. SAS may also deviate from the spectrum allocation computation process to corrupt the spectrum allocation decisions. Our PriDSA-v2 scheme tackles this attack model.

In both models, we assume that ESC nodes are honest in their sensing report.

E. Security properties

The following is an overview of the security properties of PriDSA. Formal definitions will be presented after introducing details of the system.

Correctness: This property requires that when an SU's operation location can impose interference to some IU, its spectrum request cannot be approved. i.e. SU can not receive a valid spectrum license in this case.

Location privacy for IUs: We assume SAS as the adversary, which is curious on IU locations. SAS can attempt to derive IU location by examining the safe zone information submitted by ESC nodes.

We expect that in PriDSA (both versions), when SAS is non-colluding and honest but curious, IUs have location privacy guarantee. This guarantee ensures that SAS is unable to identify any safe zone information, which could be used by the adversary to determine the location of IUs.

Moreover, we expect PriDSA-v2 can still provide certain level of IU privacy protection under the colluding malicious SAS model. Specifically, individual ESC privacy is proposed in this case, which requires that SAS is not able to identify the safe zone information of any single ESC's data report, so as to reduce the likelihood of inferring the accurate locations of IUs.

Soundness: Soundness property requires that the denial or grant of spectrum access permissions to SUs must be strictly and correctly based on ESC sensing inputs.

IV. Background

In this section, we introduce the features of AFGH cryptosystem that is leveraged in PriDSA design.

A. Overview of AFGH cryptosystem

The design of PriDSA heavily leverages the homomorphic properties of AFGH cryptosystem [10], which is a widely used proxy re-encryption scheme.

AFGH cryptosystem is defined over a type 1 bilinear groups $(\mathbb{G}_1, \mathbb{G}_T)$, where a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ exists with the following properties:

1) $\mathbb{G}_1$ and $\mathbb{G}_T$ are multiplicative cyclic groups of prime order p; g is a generator of $\mathbb{G}_1$.

2) e is an efficiently computable bilinear map with the following properties:
   - Bilinear: $e(u^a, v^b) = e(u, v)^{ab}$, $\forall u, v \in \mathbb{G}_1$, $a, b \in \mathbb{Z}_p^*$;
   - Non-degenerate: $e(g, g) \neq 1$.

The following describes the construction of the AFGH scheme, which is "the third attempt" in [10].

System parameters: To setup the system, a Type 1 bilinear pairing system is required. Denote g as the generator of $\mathbb{G}_1$, and set $Z = e(g, g)$. Denote p as the order of group $\mathbb{G}_1$ and let $\mathbb{Z}_p^* = \{1, \cdots p-1\}$.

Key Generation($\mathsf{KG}(a_1, a_2)$): For two inputs $a_1, a_2 \in \mathbb{Z}_p^*$, set secret key $\mathtt{sk} = (a_1, a_2)$, compute public key $\mathtt{pk} := (Z^{a_1}, g^{a_2})$.

Re-Encryption Key Generation ($\mathsf{RG}(\mathtt{sk}_a, \mathtt{pk}_b)$): taking private key $\mathtt{sk}_a = (a_1, a_2)$ of user A and public key $\mathtt{pk}_b = (Z^{b_1}, g^{b_2})$ of user B, the re-encryption key is computed by $\mathtt{rk}_{A\to B} := (g^{b_2})^{a_1} = g^{a_1 b_2}$.

First-Level Encryption ($\mathsf{E}_I(M, \mathtt{pk}_a)$): for a message $M \in \mathbb{G}_T$ and public key $\mathtt{pk}_a = (Z^{a_1}, g^{a_2})$, select a random nonce $r \leftarrow_\$ \mathbb{Z}_p^*$, and compute $c_1 = Z^r \cdot M$, $c_2 = Z^{ra_2}$. The ciphertext is $C := (c_1, c_2)$.

Second-Level Encryption ($\mathsf{E}_{II}(M, \mathtt{pk}_a)$): for a message $M \in \mathbb{G}_T$ and public key $\mathtt{pk}_a = (Z^{a_1}, g^{a_2})$, select $r \leftarrow_\$ \mathbb{Z}_p^*$, and compute $c_1 = Z^{ra_1} \cdot M$, $c_2 = g^r$. The ciphertext is $C := (c_1, c_2)$.

First-Level Decryption ($\mathsf{D}_I(C_r, \mathtt{sk}_b)$): for a first-level ciphertext $C_r = (c_1, c_2)$ and its corresponding private key $\mathtt{sk}_b = (b_1, b_2)$, the plaintext is obtained by computing $M^* := \frac{c_1}{c_2^{1/b_2}}$.

Second-Level Decryption ($\mathsf{D}_{II}(C_r, \mathtt{sk}_a)$): for a second-level ciphertext $C_r = (c_1, c_2)$ and its corresponding private key $\mathtt{sk}_a = (a_1, a_2)$, the plaintext is obtained by computing $M^* := \frac{c_1}{e(g^{a_1}, c_2)}$.

Re-Encryption ($\mathsf{R}(C, \mathtt{rk}_{A\to B})$): for a message M encrypted by public key (Z^{a_1}, g^{a_2}), its second-level ciphertext $C = (c_1, c_2)$ can be re-encrypted to be a first-level ciphertext encrypted by public key $\mathtt{pk}_b = (Z^{b_1}, g^{b_2})$ by computing $c_2^* := e(c_2, \mathtt{rk}_{A\to B}) = Z^{(ra_1)b_2}$. The re-encrypted first level ciphertext is $C_r := (c_1, c_2^*)$.

1) Homomorphic property of AFGH scheme: AFGH cryptosystem inherently supports homomorphic multiplication and homomorphic inverse operations, which are defined as follows:

Proposition 1. ***Homomorphic multiplication****: Given an AFGH public and private key pair* $(\mathtt{pk}, \mathtt{sk})$*, consider two AFGH second-level encrypted ciphertexts* $C = \mathsf{E}_{II}(M, \mathtt{pk}) = (c_1, c_2)$ *and* $C' = \mathsf{E}_{II}(M', \mathtt{pk}) = (c_1', c_2')$*. The homomorphic multiplication operation* $C \otimes C' := (c_1 c_1', c_2 c_2')$ *produces a ciphertext of* MM'*. In another word,* $\mathsf{D}_{II}(C \otimes C') = MM'$*.*

Homomorphic inverse*: Given an AFGH public and private key pair* $(\mathtt{pk}, \mathtt{sk})$*, consider an AFGH second-level encrypted ciphertext* $C = \mathsf{E}_{II}(M, \mathtt{pk}) = (c_1, c_2)$*. The homomorphic inverse operation* $\mathsf{inv}(C) := (c_1^{-1}, c_2^{-1})$ *produces a ciphertext of* M^{-1}*. In another word,* $\mathsf{D}_{II}(\mathsf{inv}(C)) = M^{-1}$*.*

We omit the proof since the homomorphic feature of AFGH has already been discussed in [11].

B. Cryptographic Assumptions

The security of AFGH scheme is preserved under the extended decisional bilinear Diffie-Hellman (EDBDH) assumption, Decision Linear (DLIN) and discrete logarithm (DL) assumption [10].

V. PriDSA-v1: Secure DSA under HBC model

In this section, we present the design of PriDSA-v1, which preserves IU location privacy under the assumption that SAS does not collude with SUs and follows protocols faithfully.

A. Overview

As shown in Figure 3, there are four parties in PriDSA-v1: (1) ESC nodes, (2) a SAS server for spectrum management, (3) SUs, and (4) a trusted Key Issuer. In a high level, SAS realizes two functions:

1) maintaining the database of encrypted safe zone maps. Periodically, from each ESC sensor, SAS receives its safe zone information that is encrypted by level-2 AFGH. The encrypted safe zone information is denoted as $[\![\mathbf{X}]\!]_{II}$, where $[\![x]\!]_{II}$ denotes the level-2 AFGH encryption on a message x. SAS aggregates all ESCs' $[\![\mathbf{X}]\!]_{II}$ inputs by leveraging the homomorphic property of AFGH cryptosystem. The aggregated safe zone map is denoted as $[\![\mathbf{D}]\!]_{II}$ and is stored at SAS.
2) spectrum allocation based on the encrypted maps. To handle a spectrum request from an SU, SAS computes a potential spectrum license $\mathtt{cred}$ and generate a safe zone token based on $[\![\mathbf{D}]\!]_{II}$, and then sends $\mathtt{cred}$ and the safe zone token to the SU. Only when the SU is located in a safe zone, can the SU be able to successfully generate the permission proof based on the safe zone token.

In the following, we will describe the details of each step in PriDSA-v1 design.

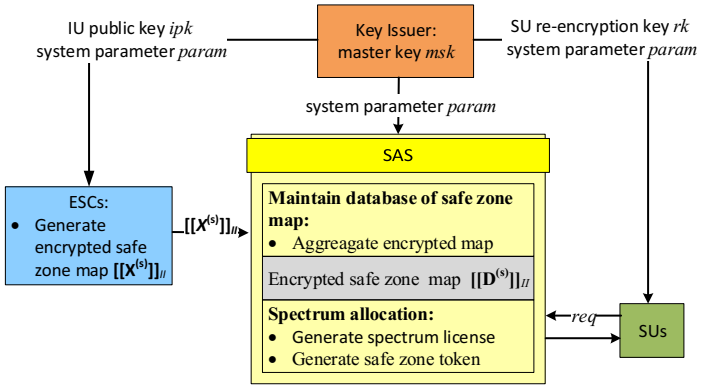


Fig. 3: System Framework

B. System Setup

To initialize the system, the following three steps are executed by the Key Issuer, which is trusted by the IUs (e.g. it can be operated by IU operator):

1) Set up the AFGH scheme: Let the symmetric bilinear group pair be $\mathbb{G}_1, \mathbb{G}_T$ of prime order p, the corresponding bilinear mapping function be $e : \mathbb{G}_1 \times \mathbb{G}_1 \mapsto \mathbb{G}_T$, and AFGH system parameters be $g \in \mathbb{G}_1$, $Z = e(g, g)$.
2) Select $a_1, a_2 \leftarrow_{\$} \mathbb{Z}_p^*$, where $\mathbb{Z}_p^*$ is the multiplicative group modulo p. Compute an AFGH key pair $(\mathtt{sk}, \mathtt{pk}) = \mathsf{KG}(a_1, a_2)$. Let the master secret key $\mathtt{msk} = \mathtt{sk}$ and IU's group public key $\mathtt{ipk} = \mathtt{pk}$. Select $f_1, h \leftarrow_{\$} \mathbb{G}_1$, $H \leftarrow_{\$} \mathbb{G}_T$ and compute $Y := e(f_1, h)$. Let system parameters $\mathtt{params} = (\mathbb{G}_1, \mathbb{G}_T, p, e, g, Z, f_1, h, Y)$.
3) Publish $\mathtt{ipk}$ and $\mathtt{params}$.

An SU b must register its identity with the Key Issuer before sending any spectrum request. During the registration process, it generates a randomized AFGH key pair $(\mathtt{sk}_b, \mathtt{pk}_b)$ and sends $\mathtt{pk}_b$ to the Key Issuer. The Key Issuer then sends back the corresponding re-encryption key $\mathtt{rk}_b$, which is generated by $\mathtt{rk}_b \leftarrow \mathsf{RG}(\mathtt{msk}, \mathtt{pk}_b)$, through a secure channel.

After the initial setup, the Key Issuer can go off-line without affecting PriDSA-v1's runtime normal operation, which is outlined in the following subsections.

C. Details of maintaining the database of safe zone map

In this subsection, we describes how ESC sends safe zone information to SAS without indirectly exposing IU location information .

1) ESC input data: The input safe zone data from an ESC to SAS is generated by the following procedure. Firstly, PriDSA system's service area is divided into a total of L same size grids and the 3.5 GHz spectrum is divided into F channels. Then, following the process outlined in Section III-C, an ESC derives its own safe zone information and converts the information into a matrix $\mathbf{T} := [\mathbf{T}_{l,f}]_{L \times F}$ of dimension $L \times F$. If the entire grid l at channel f is inside the safe zone, ESC sets $\mathbf{T}_{l,f}$ to be a random non-zero element picked from $\mathbb{Z}_p$; formally,

$$\mathbf{T}_{l,f} \leftarrow_{\$} \mathbb{Z}_p \backslash \{0\}. \tag{2}$$

Otherwise, $\mathbf{T}$'s entry $\mathbf{T}_{l,f}$ is 0; formally,

$$\mathbf{T}_{l,f} \leftarrow 0. \tag{3}$$

Afterwards, ESC creates matrix $\mathbf{X} := [\mathbf{X}_{l,f}]_{L \times F}$ by converting every $\mathbf{T}_{l,f}$ to group $\mathbb{G}_T$ through the exponentiation operation

$$\mathbf{X}_{l,f} \leftarrow Y^{\mathbf{T}_{l,f}}. \tag{4}$$

Then, ESC encrypts every entry of $\mathbf{X}$ using level 2 encryption and public key $\mathtt{ipk}$. Finally, ESC sends the encrypted safe zone report $[\![\mathbf{X}]\!]_{II}$ to SAS. SAS cannot decrypt these encrypted reports since it does not have the decryption key.

2) Aggregate ESC input: Upon receiving the encrypted safe zone maps $\{[\![\mathbf{X}(i)]\!]_{II}\}_{i=1}^{N}$ from all N ESCs, where (i) indicates the input of the ith ESC sensor, SAS integrates them together to form the aggregated safe zone map $[\![\mathbf{D}]\!]_{II} := [[\![\mathbf{D}_{l,f}]\!]]_{L \times F}$ by computing element-wise homomorphic product of all input maps. That is:

$$[\![\mathbf{D}_{l,f}]\!]_{II} \leftarrow \otimes_{i=1}^{N} [\![\mathbf{X}_{l,f}(i)]\!]_{II}. \tag{5}$$

Note that an entry $\mathbf{D}_{l,f} \neq 1_{\mathbb{G}_T}$ indicates grid l is a safe zone grid in channel f.

D. Spectrum computation

Spectrum computation requires an SU to obtain a valid spectrum license from SAS if and only if it is in a safe zone. To realize the above spectrum computation requirements, on a high level, SAS computes a safe zone token using the encrypted safe zone map, which can be further used to generate permission proof by SU. Specifically, the process works as follows.

Let l be the location of an SU b and f be its requested channel. SAS firstly generates a valid license $\mathtt{cred}$ for this request. The license contains the content of authorization for the SU b (i.e. expiration time, location, transmission power, etc), SAS certificate, an safe zone token and a digital signature over the authorization and safe zone token. The safe zone token is computed by using SU b's re-encryption key $\mathtt{rk}_b$ on safe zone map item $[\![\mathbf{D}_{l,f}]\!]_{II}$, namely,

$$[\![\mathbf{D}_{l,f}]\!]_{I,b} \leftarrow \mathsf{R}\left([\![\mathbf{D}_{l,f}]\!]_{II}, \mathtt{rk}_b\right). \tag{6}$$

Note that the safe zone token is a level 1 ciphertext of some random value other than $1_{\mathbb{G}_T}$ over SU b's key, if and only if SU b's location belongs to a safe zone.

Then, SAS sends spectrum license $\mathtt{cred}$ and safe zone token $[\![\mathbf{D}_{l,f}]\!]_{I,b}$ to the SU as the response to the SU's spectrum access request.

E. Operations at SU: safe zone token retrieval

Upon receiving the response to its spectrum access request, the SU b with public key $\mathtt{pk}_b = (p_1, p_2)$ decrypts the safe zone token $[\![\mathbf{D}_{l,f}]\!]_{I,b} := (D_1, D_2)$ in $\mathtt{cred}$, namely $D^* \leftarrow \mathsf{D}_I\left([\![\mathbf{D}_{l,f}]\!]_{I,b}, \mathtt{sk}_b\right)$. If $D^* = 1_{\mathbb{G}_T}$, it means SU is not located in a safe zone. Thus, it should not access the spectrum; otherwise, SU b gains the permission to access channel k at its location l.

F. Permission Proof

The design of the $\mathtt{cred}$ ensures that an SU can prove to anyone that it indeed got a valid spectrum access permission from SAS. Firstly, the SAS certificate and signature carried in $\mathtt{cred}$ ensure that the content of $\mathtt{cred}$ is not modified and is generated by SAS. Moreover, the design of the safe zone token $[\![\mathbf{D}_{l,f}]\!]_{I,b} := (D_1, D_2)$ in $\mathtt{cred}$ ensures that SU can provide a proof of $D^* \neq 1_{\mathbb{G}_T}$ using zero-knowledge proof. Specifically, to demonstrate $D^* \neq 1_{\mathbb{G}_T}$, an SU b only needs to prove $D_2 \neq D_1^{b_2}, p_2 = g^{b_2}$, where SU b's secret key is $sk_b = (b_1, b_2)$ and public key is $pk_b = (p_1, p_2)$. To achieve this, SU b publishes a tuple $(D_1, D_3, \delta_{b_2}, c)$, which is computed by [12]:

- $D_3 \leftarrow D_1^{b_2}$, $r_{b_2} \leftarrow \mathbb{Z}_p$, $R_1 \leftarrow D_1^{r_{b_2}}$, and $R_2 \leftarrow g^{r_{b_2}}$.
- $c \leftarrow H(D_1, D_3, R_1, R_2)$ and $\delta_{b_2} \leftarrow r_{b_2} + c b_2$.

Anyone can check this zero-knowledge proof by firstly checking $D_3 \neq D_2$ and then checking $c = H(D_1, D_3, \tilde{R_1}, \tilde{R_2})$, where $\tilde{R_1} \leftarrow D_1^{\delta_{b_2}} / D_3^c$, $\tilde{R_2} \leftarrow g^{\delta_{b_2}} / p_2^c$. The proof for the correctness and soundness of this zero-knowledge proof can be found in [12].

VI. PriDSA-v2: IU Privacy protection against colluding malicious SAS

Similar to other existing MPC-based secure DSA schemes on HBC model [6][7][8], PriDSA-v1 is not secure when SAS colludes with some SUs, i.e. PriDSA-v1 and works in [6][7][8] cannot preserve IU privacy in the *colluding malicious SAS model*. To understand this, consider that SAS colludes with an SU b. SAS can use SU b's re-encryption key $\mathtt{rk}_b$ on the encrypted safe zone data $[\![\mathbf{X}_{l,f}]\!]_{II}$, namely, $[\![\mathbf{X}_{l,f}]\!]_{I,b} \leftarrow \mathsf{R}\left([\![\mathbf{X}_{l,f}]\!]_{II}, \mathtt{rk}_b\right)$, which can then be decrypted by SU b to reveal $\mathbf{X}_{l,f}$. When all $\mathbf{X}_{l,f}$ are revealed, all $\mathbf{T}_{l,f}$ are revealed. Essentially, the colluding SU b can reveal the entire Figure 1 of the ESC sensor. With Figure 1 revealed, SAS can easily derive d_0. With d_0s to at least three ESC sensors known, SAS can uniquely identify an IU's location through trilateration and compromise the location privacy of the IU.

Essentially, the failure of PriDSA-v1 in protecting IU privacy in the previous example is due to the fact that under the colluding SAS model, an individual ESC's safe zone report to SAS can be revealed by a colluding SU, which gives very accurate indications of the distance between IUs and their surrounding ESC nodes.

In this section, we introduce PriDSA-v2, which is a modification of PriDSA-v1 that mitigates the threat of SAS-SU collusion to IU location privacy. The spectrum computation function of PriDSA-v2 remains the same as PriDSA-v1, yet it prevents a colluding SAS from obtaining information on an individual ESC's safe zone report by adding a blinding factor on the ESC's protection-zone input data to the SAS. The blinding factor can only be removed after all ESC inputs have been aggregated. Thus, a colluding SAS at most can know the integrated safe zone map (i.e. the shape of the white area in Figure 2), which does not provide enough information to pinpoint individual IU's location.

PriDSA-v2 also includes mechanisms to ensure that a malicious SAS cannot deviate from the proper spectrum allocation computation process to produce incorrect SU spectrum permission. Essentially, PriDSA-v2 includes verifiable computation mechanism so that a SU can verify that SAS's response to its spectrum request is computed following the correct protocol. This ensures that SAS cannot launch denial-of-service attack on selected SUs or treat SUs unfairly.

In the remainder of this section, we introduce the details of PriDSA-v2 design.

A. Blinding of the input data

To blind the safe zone data at each location l and channel f, an ESC sensor picks a random nonce $\mathbf{A}_{l,f}$ in $\mathbb{Z}_p$, and replaces equation (4) by

$$\mathbf{X}_{l,f}^{(b)} \leftarrow Y^{\mathbf{T}_{l,f}+\mathbf{A}_{l,f}}. \tag{7}$$

The above formula adds the nonce to safe zone data $\mathbf{T}_{l,f}$. Note that the blinding factor $\mathbf{A}_{l,f}$ ensures that even when a colluding SU obtains $\mathbf{X}_{l,f}^{(b)}$, it will not be able to see the real safe zone information as it cannot remove the blinding factors.

ESC also computes the Pedersen commitment on $\mathbf{T}_{l,f} + \mathbf{A}_{l,f}$. That is:

$$\mathbf{r}_{l,f} \leftarrow_{\$} \mathbb{Z}_p; \quad \mathbf{C}_{l,f} \leftarrow Y^{\mathbf{T}_{l,f}+\mathbf{A}_{l,f}} H^{\mathbf{r}_{l,f}}. \tag{8}$$

The helper value $\mathbf{B} := [\mathbf{B}_{l,f}]_{L\times F}$ is computed by:

$$\mathbf{B}_{l,f} \leftarrow Y^{\mathbf{A}_{l,f}} \mathbf{C}_{l,f}. \tag{9}$$

Afterwards, this ESC computes $[\![\mathbf{X}_{l,f}^{(b)}]\!]_{II}$ and $[\![\mathbf{B}_{l,f}]\!]_{II}$ using level-2 encryption and sends them as input data to SAS. Meanwhile, ESC also sends all $\mathbf{C}_{l,f}$, $H^{\mathbf{r}_{l,f}}$, and $\mathbf{B}_{l,f}$ to a trusted IU tracker through a secure channel.

B. Data aggregation and removal of blinding factors

Upon receiving the input from all ESC sensors, SAS follows equation (5) to homomorphically aggregate the blinded encrypted safe zone data report. The aggregation results include the blinding factors and we denote it as $[\![\mathbf{D}^{(b)}]\!]_{II}$. SAS also aggregates helper value $[\![\mathbf{B}]\!]_{II}$ from all ESCs input by computing

$$[\![\mathbf{B'}_{l,f}]\!]_{II} \leftarrow \otimes_{i=1}^{N} [\![\mathbf{B}(i)_{l,f}]\!]_{II}, \tag{10}$$

where i is the index of ESC sensor and N is the number of ESC sensors.

The IU tracker publishes the cumulative commitment value $\mathbf{C}'$, where

$$\mathbf{C'}_{l,f} := \prod_{i=1}^{N} \mathbf{C}_{l,f}(i) \tag{11}$$

for all locations l and channels f.

Using $[\![\mathbf{B'}_{l,f}]\!]_{II}$ and $\mathbf{C}'$, SAS can remove the blinding factors from the aggregated safe zone map as follows:

$$[\![\mathbf{D}_{l,f}]\!]_{II} \leftarrow [\![\mathbf{D}_{l,f}^{(b)}]\!]_{II} \otimes \mathsf{inv}\left([\![\mathbf{B}'_{l,f}]\!]_{II}\right) \otimes [\![\mathbf{C}'_{l,f}]\!]_{II}. \tag{12}$$

$[\![\mathbf{D}_{l,f}]\!]_{II}$ is then used to perform spectrum allocation computation as described in Section V-D and V-E.

C. Preventing SAS from deviating from the protocols

To prevent SAS from deviating from the proper spectrum computation protocol, PriDSA-v2 includes a spectrum enforcer service, which enables an SU to verify that the SAS's response to its spectrum request is computed properly. The enforcer proceeds as follows to verify the integrity of spectrum computation:

Verify the integrity of SU: the enforcer checks the content and signature of the response from SAS to ensure SU is sending the original response.

Fetch data from IU tracker: The enforcer extracts the location l and channel f from the response and gets the corresponding accumulated commitments $\mathbf{C}'_{l,f}$, helper values $\mathbf{B}'_{l,f}$, and commitment nonces $\mathbf{H}'_{l,f}$ from IU tracker.

Soundness check: A faithful response from SAS must satisfy the following condition:

$$\begin{cases} \mathbf{H}'_{l,f}\mathbf{B}'_{l,f} \neq \left(\mathbf{C}'_{l,f}\right)^2, & \text{if the response is approval} \\ \mathbf{H}'_{l,f}\mathbf{B}'_{l,f} = \left(\mathbf{C}'_{l,f}\right)^2, & \text{if the response is denial} \end{cases} \tag{13}$$

The soundness check condition is valid for the following reason. Note that from equation (8)(9):

$$\begin{aligned} &\mathbf{H}_{l,f}\mathbf{B}_{l,f} = \mathbf{H}_{l,f}Y^{\mathbf{A}_{l,f}}\mathbf{C}_{l,f} = \left(\mathbf{C}_{l,f}\right)^2 Y^{-\mathbf{T}_{l,f}} \\ \Rightarrow\ &\mathbf{H}'_{l,f}\mathbf{B}'_{l,f} = \left(\mathbf{C}'_{l,f}\right)^2 Y^{-\sum_{i=1}^{N}\mathbf{T}_{l,f}(i)}. \end{aligned} \tag{14}$$

Since $\mathbf{T}_{l,f}(i)$ is either 0 or some random non-zero element, we have:

- If $\mathbf{H}'_{l,f}\mathbf{B}'_{l,f} = \left(\mathbf{C}'_{l,f}\right)^2$, then $\sum_{i=1}^{N}\mathbf{T}_{l,f}(i) = 0$ and all $\mathbf{T}_{l,f}(i)$ are 0 with probability $1-\epsilon$, where ϵ is some negligibly small probability. Hence, we can conclude that all ESC nodes are **not** marking location l in channel f as safe zone. Therefore, the second condition in equation (13) implies the requested location and channel is not a safe zone, so the expected response should be "decline".
- If $\mathbf{H}'_{l,f}\mathbf{B}'_{l,f} \neq \left(\mathbf{C}'_{l,f}\right)^2$, then $\mathbf{T}_{l,f}(i) \neq 0$ for some i. Hence, we can conclude that at least one ESC node is marking location l in channel f as safe zone. Thus, the expected response from SAS should be "approval".

VII. Security Definitions and Analysis

In this section, we provide formal definitions and proofs of PriDSA's security properties.

A. Correctness

Correctness property requires that when an SU is not located in a safe zone of any ESC, its spectrum request cannot be approved. i.e. SU cannot receive a valid or useful spectrum license in this case. Denote the whole PriDSA functionality as a function f:

$$\texttt{cred}^* := f(\mathcal{T}, \mathcal{B}, \texttt{req}), \tag{15}$$

where $\mathcal{T}$ is the set of all received safe zone reports, $\mathcal{B}$ is its corresponding set of helper value maps.

The formal definition of correctness is given as follows:

Definition 1. *PriDSA is correct if it satisfies the following condition: For any input $(\mathcal{T}, \mathcal{B}, \texttt{req})$ to PriDSA functionality, if the requested location l and channel f is not in any safe zone, the recovered license $\texttt{cred}^* := f(\mathcal{T}, \mathcal{B}, \texttt{req})$ is invalid.*

Theorem 1. *The probability with which PriDSA (both version) is NOT correct is negligible.*

Proof. The correctness follows directly from the specification of the PriDSA protocols. The safe zone data can be correctly aggregated by the homomorphic feature of AFGH cryptosystem, as long as SAS aggregates them faithfully; the unforgeability of the digital signature in the spectrum license ensures SUs that are outside of safe zones cannot recover valid licenses, and the soundness feature of zero-knowledge proof [12] prevents such SUs from forging the permission proof. For PriDSA-v2, the correctness of removing the blinding factors is ensured by the homomorphic feature of AFGH cryptosystem.

Detailed correctness proof is presented in the extended version of this paper [13]. □

B. Security Analysis of PriDSA under non-colluding honest but curious (HBC) SAS model

To formally analyze PriDSA security under the non-colluding HBC model, we setup a security experiment where an adversary tries to distinguish two groups of encrypted (and possibly blinded) safe zone reports as shown in Figure 4. Here, the procedure of generating the encrypted safe zone map report is denoted as algorithm $\mathsf{GenRep}(\cdot)$. The semantic security experiment depicts an adversary who has the messages exchanged between ESC and SU, and aims at distinguishing two different encrypted safe zone reports.

$\mathbf{Exp}_{\mathcal{A}}^{\text{sem-Sec}}(\lambda)$

$(\texttt{msk}, \texttt{ipk}, \texttt{params}) \leftarrow \mathsf{Setup}(2^\lambda)$.

$(\mathcal{T}^{(0)}, \mathcal{T}^{(1)}) \leftarrow \mathcal{A}(\texttt{ipk}, \texttt{params})$, where

$\mathcal{T}^{(0)} := \left\{\mathbf{T}^{(0)}(k)\right\}_{k=1}^{N}$, $\mathcal{T}^{(1)} := \left\{\mathbf{T}^{(1)}(k)\right\}_{k=1}^{N}$;

$b \leftarrow_{\$} \{0,1\}$.

$b' \leftarrow \mathcal{A}\left(\texttt{ipk}, \texttt{params}, \left\{\mathsf{GenRep}(\mathbf{T}^{(b)}(k))\right\}_{k=1}^{N}\right)$.

return 1 if $b = b'$; otherwise **return** 0.

Fig. 4: Definition of semantic security experiment

The formal definition of IU privacy is shown as follows:

Definition 2. *PriDSA is semantically secure for IUs if for all $\lambda \in \mathbb{N}$, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\text{sem-Sec}}(\lambda)$ is negligible in λ for all Probabilistic Polynomial-Time (PPT) Adversaries $\mathcal{A}$, where*

$$\mathsf{Adv}_{\mathcal{A}}^{\text{sem-Sec}}(\lambda) = \left|\Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\text{sem-Sec}}(\lambda) = 1\right] - \frac{1}{2}\right|$$

The definition of semantic security ensures that PriDSA preserving IU privacy under non-colluding HBC SAS model. This is because as long as an HBC SAS achieves non-negligible advantage in the semantic security experiment, it is able to extract information from ESC inputs.

Theorem 2. *If AFGH scheme is semantically secure, PriDSA (both versions) is semantically secure for IUs under the non-colluding HBC SAS model.*

Proof. (Sketch) To prove PriDSA is secure for IUs, we assume that there exists an adversary $\mathcal{A}$ which can break IU security with non-negligible probability. Then, we construct a simulator $\mathcal{S}$ which aims at breaking the semantic security of AFGH scheme by taking advantage of the adversary $\mathcal{A}$. $\mathcal{S}$ plays as the adversary in an given AFGH semantic security experiment, yet meanwhile it sets up a simulated semantic security experiment to interact with $\mathcal{A}$. Finally it can leverage the response from $\mathcal{A}$ to gain a non-negligible advantage in AFGH semantic security experiment.

The full proof is presented in the extended version of this paper [13].

□

Claim 1. *Under EDBDH assumption and the non-colluding HBC SAS model, PriDSA is secure for IUs.*

Proof. According to theorem 3.1 in [10], AFGH is semantically secure under EDBDH assumption, so PriDSA is semantically secure for IUs under EDBDH assumption. □

C. Security Analysis of PriDSA under colluding SAS model

In this section, we prove that PriDSA-v2 can ensure that individual ESC's safe zone input to SAS is secure from colluding SAS and SUs, which is called "individual ESC privacy". In Section VIII-B, we will show how "individual ESC privacy" can mitigate the threat of privacy degradation as a result of colluding SAS and SUs.

To formally define individual ESC privacy, we set up a security experiment, which describes the capability of an adversary and definition of breaking individual privacy. In the privacy experiment, the adversary $\mathcal{A}$ is required to output the safe zone information at one arbitrary location that is sensed by an arbitrary ESC according to the adversary's own choice. To setup the experiment, the challenger $\mathcal{C}$ generates a randomized (yet unknown) safe zone data and send the encrypted inputs following PriDSA-v2 protocol to $\mathcal{A}$, assuming $\mathcal{C}$ is ESC and $\mathcal{A}$ is the SAS. Since SAS may collude with SUs, we allow the adversary $\mathcal{A}$ to query a Reg oracle to simulate the process of SU registration, so that $\mathcal{A}$ can arbitrarily fetch any keys an SU may possess. The details of individual privacy experiment are shown in Figure. 5.

$\mathbf{Exp}_{\mathcal{A}}^{\mathrm{ind-Priv}}(\lambda)$

$(\mathtt{msk}, \mathtt{ipk}, \mathtt{params}) \leftarrow \mathsf{Setup}(2^{\lambda})$.

for $k = 1, \cdots, M$

$\quad \mathbf{T}^{(e)}(k) \leftarrow_{\$} \{0,1\}^{L \times F}, \quad \mathbf{T}(k) \leftarrow_{\$} \{0,1\}^{L \times F}$.

endfor

Send $\mathtt{ipk}, \mathtt{params}, \left\{ \mathsf{GenRep}(\mathbf{T}^{(e)}(k)), \mathsf{GenRep}(\mathbf{T}(k)) \right\}_{k=1}^{M}$ to $\mathcal{A}$

$(k^*, l, f) \leftarrow \mathcal{A}^{\mathsf{Reg}(\cdot)}$.

return 1 if $\mathbf{T}_{l,f}^{(e)}(k^*) = 1$ or $\mathbf{T}_{l,f}(k^*) = 1$; otherwise **return** 0.

$\mathsf{Reg}(\mathtt{pk}_b)$

$\mathtt{rk}_b \leftarrow \mathsf{RG}(\mathtt{msk}, \mathtt{pk}_b)$.

return $\mathtt{rk}_b$.

Fig. 5: Definition of individual privacy experiment

The formal definition of IU privacy is shown as follows:

Definition 3. *PriDSA preserves individual ESC privacy if for all $\lambda \in \mathbb{N}$, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{ind-Priv}}(\lambda)$ is negligible in λ for all Probabilistic Polynomial-Time (PPT) Adversaries $\mathcal{A}$, where*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{ind-Priv}}(\lambda) = \left| \Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{ind-Priv}}(\lambda) = 1 \right] - \frac{1}{4} \right|$$

Theorem 3. *PriDSA-v2 preserves individual ESC privacy under DLIN assumption (See section IV-B for DLIN).*

Proof. (Sketch) To prove PriDSA-v2 is individually private for ESC reports, we assume that there exists an adversary $\mathcal{A}$ which can break individual ESC privacy with non-negligible probability. Then we construct a simulator $\mathcal{S}$ which aims at solving DLIN problem by taking advantage of the adversary $\mathcal{A}$. $\mathcal{S}$ receives an DLIN instance, yet meanwhile it sets up a simulated PriDSA-v2 privacy experiment to interact with $\mathcal{A}$, where the DLIN instance is leveraged to simulate encrypted data reports without knowing its actual safe zone status. Finally it can leverage the response from $\mathcal{A}$ to gain a non-negligible advantage in solving DLIN problem.

The full proof is presented in the extended version of this paper [13].

□

D. Soundness

Soundness feature requires that whenever SAS diverts from the protocol to intentionally give SU a wrong response that are not correctly computed based on safe zone information, SU can verify the response with the enforcer to dispute it. We show that PriDSA-v2 preserves the soundness property in section VI-C.

VIII. Evaluation

A. Implementation details

The AFGH cryptosystem is set up such that it provides approximately the same level of security as an RSA signature with a modulus size of 2048 bits. By using the pairing-based cryptography (PBC) library available at [14], we instantiate the AFGH cryptosystem and implement all SAS protocols and algorithms on a a laptop with 8x Intel(R) Core(TM) i7-4710HQ CPU @ 2.50GHz.

We deploy IUs in a 20 km by 20 km rectangular region and consider one channel centered at frequency 3600MHz. We set IUs as military radars with a 50m height and the interference threshold of IUs are -80 dBm; we assume SUs to be outdoor CBSD devices and set their antenna height as 6m and transmission power as 24 dBm. We use ECC-33 model [15] to formulate the path loss.

We compare PriDSA with one MPC-based privacy preserving system IP-SAS proposed in [7] and the data obfuscation technology proposed in [16]. IP-SAS is a MPC based protocol that assumes SAS is untrusted and achieves incumbent user privacy under exclusion zone model. The data obfuscation technology proposed in [16] can provide IU privacy in case of compromised SAS.

B. Privacy preserving level

When the SAS is malicious and colludes with SUs, inference attack based on safe zone information can reduce the location privacy level of IUs. Hence we can evaluate the location privacy preserving level of PriDSA or IP-SAS using the metric mentioned in [16], which is expressed as:

$$PPL = \frac{1}{S/u^2} = \frac{u^2}{S}, \tag{16}$$

where S is the size of the area where an adversary believe that a specific IU may appear, and u is the unit of IU location representation. The smaller PPL is, the better the privacy protection of IU will be.

Table I compares the IU location privacy between IP-SAS, PriDSA and obfuscation technique in [16], using the PPL metric in equation (16). We obtain the average PPL value by repeatedly, randomly and uniformly deploying 20 IUs 1000 times. We set the side length of grids as 100m for IP-SAS

and PriDSA, and assume there are 225 ESC sensor nodes with equally spaced distribution for PriDSA. The precision of u is set to be 10m. Note that for obfuscation techniques in [16] we only consider changing the parameter of "obfuscation strategy #1", where false IU entries are inserted and sent to SAS. This is because in our system model the "obfuscation strategy #2" proposed in [16] can only be processed at SAS, and thus it cannot preserve IU privacy in HBC model or malicious colluding model.

Under honest but curious (HBC) model, as a result of the provable security provided by IP-SAS and PriDSA, an adversary has to randomly guess the location of the IU across the whole SAS service area, so the PPL is very small.

Under the malicious colluding model, an adversary towards IP-SAS can directly pinpoint any given IU to a specific grid. The adversary towards PriDSA-v1 can identify all grids that have IUs, but cannot know the identify of the IU in each grid. Thus, while both PriDSA-v1 and IP-SAS's IU privacy suffers significantly when SAS can maliciously collude with SUs, PriDSA-v1 performs a little better than IP-SAS in terms of IU privacy protection. For PriDSA-v2, the adversary can only get an overall safe zone map and the location of an IU can possibly in any grid outside of safe zone.

TABLE I: Comparison of IU privacy level (PPL)

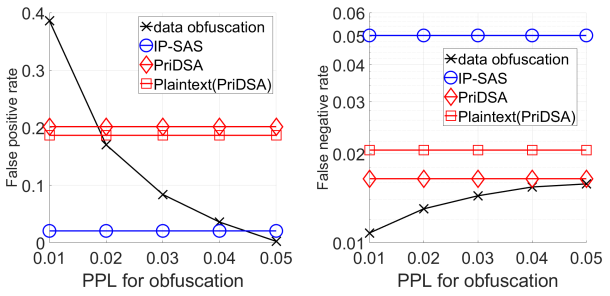
	HBC model	Malicious colluding model
IP-SAS	$2.5 * 10^{-7}$	0.01
PriDSA-v1	$2.5 * 10^{-7}$	0.0005
PriDSA-v2	$2.5 * 10^{-7}$	$2.049 * 10^{-6}$
Obfuscation (10 false IUs)	0.033	0.033
Obfuscation (30 false IUs)	0.02	0.02
Obfuscation (80 false IUs)	0.01	0.01

When obfuscation techniques in [16] is applied, SAS received extra IU location data entries, and the adversary (under HBC model or malicious colluding model) can find out the true location of target IU by randomly guessing. Hence we can achieve smaller PPL as long as more false IU entries are inserted. However, since in [16], SAS also protects false IUs from harmful interference, inserting more false IU entries may affect the accuracy of the system greatly. We'll evaluate this effect in the next subsection.

C. Accuracy

We use two metrics to evaluate the accuracy of spectrum allocation: false positive error rate, and false negative error rate. False positive error refers to declining an SU's request although it is safe for this SU to access the spectrum, and false negative error refers to accepting an SU's request although it may cause harmful interference to IU. To evaluate accuracy, we simulate 10000 SU requests from random locations for all three approaches under different settings, and we assume the error ECC-33 model obeys normal distributions with $\mu_e = -0.7$dB and $\sigma_e = 11.8$dB, according to the studies in [17].

Figure 6 shows the accuracy for different approaches. The parameters for grid side length, number of IUs and ESC nodes are the same as previous subsection. In figure 6a, we can observe that data obfuscation approaches in [16] sacrifices a lot of false positives even to achieve 0.01 PPL, while PriDSA achieves a much smaller PPL using the same parameter setting. This is because to preserve IU privacy towards compromised SAS using data obfuscation technique in [16], lots of false IU entries are inserted. In figure 6b, we can observe the obfuscation technique in [16] achieves lower false negative rate, since some false negative error might be avoided as a result of interference to the extra false IUs. In figure 6, we also evaluate the performance of plaintext version of PriDSA, where ESC doesn't encrypt its messages. The plaintext version performs better in false positives and worse in false negatives, since in plaintext version the area is not discretized.



(a) False positive rate (b) False negative rate

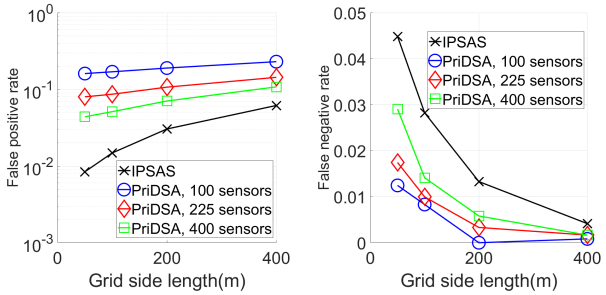
Fig. 6: Accuracy for techniques in [16], IP-SAS and PriDSA(both versions)

We also evaluate accuracy for IP-SAS and PriDSA as a result of discretization error. Figure 7 shows the effect of grid size and number of ESC sensors on the spectrum allocation accuracy for PriDSA(in both versions) and IP-SAS. From figure 7a, we can see that PriDSA can achieve lower false positive rate by deploying more ESC sensors. For both PriDSA and IP-SAS, the false positive rate decreases when grid side length decreases, as a result of more accurate safe-zone representation. Meanwhile, performance on false negative errors shows an opposite trend. In figure 7b we see false negative rate decreases when side length increases. This is because safe zones are defined by ESC systems only when a single grid is completely inside a safe zone, and larger grid side length makes the spectrum allocation more robust towards propagation model inaccuracy. We also observe that PriDSA(in both versions) achieves lower false negative rate compared to IP-SAS, since some false negative error might be avoided as a result of being out of the safe zone.

Note that for all approaches evaluated in this subsection, false negative errors happen as a result of the inaccuracy of the adopted radio propagation model, so the false negative error performance can be potentially improved by adopting more accurate model. Moreover, the design of PriDSA doesn't bring any additional false negative errors, which is guaranteed by the correctness property discussed in section VII-A.

D. Efficiency

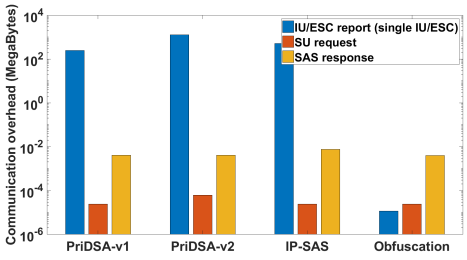
Figure 8 shows the communication overhead and computation overhead comparison between PriDSA, IP-SAS and the



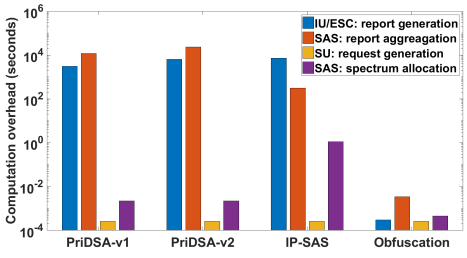
(a) False positive rate (b) False negative rate

Fig. 7: Accuracy for techniques in [16], IP-SAS, and PriDSA(both versions) over different grid side length

approach in [16]. We evaluate the performance of the three approaches over a 400 km^2 area with 10 channels, and the grid side length is set to be 100m. We see that PriDSA achieves similar computation and communication overhead compared to IP-SAS, yet PriDSA-v2 preserves individual ESC privacy in the scenario of SAS-SU collusion. We can also observe that data obfuscation approach in [16] is more efficient in terms of IU data updating, yet as we analyzed above, its security strength is much weaker and it suffers from great accuracy loss for stronger privacy protection.



(a) Communication overhead



(b) Computation overhead

Fig. 8: Communication overhead and computation overhead for different approaches

IX. Conclusion

In this paper, we propose a novel ESC-based DSA scheme called PriDSA, which preserves IU privacy when SAS is not entirely trusted. We also study the situation when SAS may intentionally deviate from the protocol and collude with some SUs, and propose PriDSA-v2 to tackle this problem. In PriDSA-v2, ESC input data is further blinded such the security goal can be achieved without making system accuracy as trade-off. Future work may focus on adapting PriDSA to more sophisticated ESC and SAS service models.

X. Acknowledgement

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

References

[1] F. C. Commission *et al.*, "Report and order and second further notice of proposed rulemaking," *Amendment of the Commissions Rules with Regard to Commercial Operations in the*, pp. 3550–3650, 2015.

[2] S. S. C. W. Security, "Cbrs operational security," *Wireless Innovation Forum*, no. WINNF-15-S-0017, 2016.

[3] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 236–247.

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

[5] Z. Zhang, H. Zhang, S. He, and P. Cheng, "Achieving bilateral utility maximization and location privacy preservation in database-driven cognitive radio networks," in *Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on*. IEEE, 2015, pp. 181–189.

[6] 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," in *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, 2016, pp. 321–330.

[7] Y. Dou, H. Li, K. C. Zeng, J. Liu, Y. Yang, B. Gao, and K. Ren, "Preserving incumbent users' privacy in exclusion-zone-based spectrum access systems," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 2486–2493.

[8] C. Guan, A. Mohaisen, Z. Sun, L. Su, K. Ren, and Y. Yang, "When smart tv meets crn: Privacy-preserving fine-grained spectrum access," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 1105–1115.

[9] O. Goldreich, "Requirements for commercial operation in the u.s. 3550-3700 mhz citizens broadband radio service band," *Wireless Innovation Forum*, no. WINNF-15-S-0112, 2016.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Trans. Inf. Syst. Secur.*, vol. 9, no. 1, pp. 1–30, Feb. 2006.

[11] H. Shafagh, A. Hithnawi, L. Burkhalter, P. Fischli, and S. Duquennoy, "Secure sharing of partially homomorphic encrypted iot data," in *Proceedings of the 15th ACM Conference on Embedded Network Sensor System*, 2017.

[12] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Conference on the Theory and Application of Cryptographic Techniques*. Springer, 1986, pp. 186–194.

[13] [Online]. Available: https://www.dropbox.com/s/f1e1sbcrq4h4gbn/dyspan_full.pdf?dl=0

[14] B. Lynn, "PBC: Pairing-based cryptography," https://crypto.stanford.edu/pbc/.

[15] E. C. Committee *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., ECC Report 33, Tech. Rep., 2003.

[16] M. Clark and K. Psounis, "Can the privacy of primary networks in shared spectrum be protected?" in *Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on*. IEEE, 2016, pp. 1–9.

[17] V. Abhayawardhana, I. Wassell, D. Crosby, M. Sellars, and M. Brown, "Comparison of empirical propagation path loss models for fixed wireless access systems," in *Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st*, vol. 1. IEEE, pp. 73–77.