Poster: Preserving Incumbent Users' Privacy in Exclusion-Zone-Based Spectrum Access Systems

Yanzhi Dou†, Kexiong (Curtis) Zeng, Yaling Yang†, Kui Ren‡
†Virginia Tech, Blacksburg, VA, USA
‡State University of New York at Buffalo, Buffalo, NY, USA
{yzdou, kexiong6, yyang8}@vt.edu, kuiren@buffalo.edu

ABSTRACT

Dynamic spectrum access (DSA) technique has emerged as a fundamental approach to mitigate the spectrum scarcity problem. As a key form of DSA, government is proposing to release more federal spectrum for sharing with commercial wireless users. However, the flourish of federal-commercial sharing hinges upon how the federal privacy is managed. In current DSA proposals, the sensitive exclusion zone (E-Zone) information of federal incumbent users (IUs) needs to be shared with a spectrum access system (SAS) to realize spectrum allocation. However, SAS is not necessarily trust-worthy for holding the sensitive IU E-Zone data, especially considering that FCC allows some industry third parties (e.g., Google) to operate SAS for better efficiency and scalability. Therefore, the current proposals dissatisfy the IUs' privacy requirement. To address the privacy issue, this paper presents an IU-privacy-preserving SAS (IP-SAS) design, which realizes the spectrum allocation process through secure computation over ciphertext based on homomorphic encryption.

CCS Concepts

•Networks → Mobile and wireless security; •Security and privacy → Privacy-preserving protocols;

1. SYSTEM DESIGN

1.1 Problem Statement

We consider an E-Zone-based SAS involving three parties: IUs, SUs, and SAS Server. SAS Server refers to a cloud-based spectrum management infrastructure that allocates spectrum resources while considering incumbent and secondary operation protection. In a typical scenario of E-Zone-based SAS, IUs first compute their E-Zones and send the E-Zone data to SAS in the initialization phase. When an SU wants to access spectrum, it needs to provide its operation parameters and geolocation to SAS. SAS checks whether the SU is within the E-Zone of any IU. For a given spectrum, if the answer is yes (no), SAS denies (permits) the SU's spectrum access to this spectrum. Note that the privacy issue of the protection-zone-based SAS, where interference from multiple IUs or SUs can be aggregated, has been addressed in our previous work [1, 2].

We assume SAS Server is semi-honest, which means it exactly follows the protocol as described above, but attempts to infer private operation data of IUs from the information communicated to it. Our goal is to design a privacy-preserving SAS that can correctly realize spectrum allocation without exposing any information that can potentially lead to IU privacy violation to the semi-honest SAS Server.

Our design is based on Paillier cryptosystem, which is an additive-homomorphic encryption scheme $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Add})$ that allows addition operation Add on ciphertexts and generates an encrypted result, when decrypted, corresponding to the sum of the plaintexts. For simplicity of notation, we use $\widehat{m}$ to denote the ciphertext of a plaintext message m by Paillier encryption in the remainder of this paper.

1.2 Design Overview

IP-SAS involves four parties: (1) a SAS Server $\mathcal{S}$ for spectrum allocation, (2) IUs, (3) SUs, and (4) a Key Distributor $\mathcal{K}$. $\mathcal{K}$ creates a Paillier public/private key pair $(\mathsf{pk}, \mathsf{sk})$ and is trusted for keeping sk a secret only known to itself. In the real world, the role of $\mathcal{K}$ can be played by some authorities such as FCC and NTIA, or even IUs *per se*. The protocol of IP-SAS is shown in Table 1. In the following, we describe the details of each step.

1.3 E-Zone Information Generation & Representation

Following the recommendations in [3], we assume that

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

MobiCom'16 October 03-07, 2016, New York City, NY, USA

© 2016 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-4226-1/16/10.
DOI: http://dx.doi.org/10.1145/2973750.2985283

Table 1: The protocol of IP-SAS

I. Initialization Phase:	
$\mathcal{K}$:	(1) $\mathcal{K}$ runs KeyGen and generates a Paillier key pair $(\mathsf{pk}, \mathsf{sk})$. pk is distributed to $\mathcal{S}$ and IUs, and sk is kept secret.
IUs:	(2) IU k calculates its E-Zone map $\mathbf{T}_k$. (3) IU k encrypts $\mathbf{T}_k$ with pk and gets $\widehat{\mathbf{T}}_k$. (4) IU k sends $\widehat{\mathbf{T}}_k$ to $\mathcal{S}$.
$\mathcal{S}$:	(5) Upon receiving all the IUs' E-Zone maps $\widehat{\mathbf{T}}_k$, $\mathcal{S}$ aggregates them generates $\widehat{\mathbf{M}}$.
II. Spectrum Computation Phase:	
SU b:	(6) SU b submits spectrum request containing its operation parameters $(h_s, p_{ts}, g_{rs}, i_s)$ and location l to $\mathcal{S}$.
$\mathcal{S}$:	(7) $\mathcal{S}$ retrieves the corresponding entry in the global E-Zone map $\widehat{\mathbf{M}}$ and obtains $\widehat{\mathbf{X}}_b$. (8) $\mathcal{S}$ adds random blinding factor $\widehat{\boldsymbol{\beta}}$ to $\widehat{\mathbf{X}}_b$ to generate $\widehat{\mathbf{Y}}_b$. (9) $\mathcal{S}$ returns $\widehat{\mathbf{Y}}_b$ and $\boldsymbol{\beta}$ to SU b.
III. Recovery Phase:	
SU b:	(10) SU b sends $\widehat{\mathbf{Y}}_b$ to $\mathcal{K}$ for decryption.
$\mathcal{K}$:	(11) $\mathcal{K}$ decrypts $\widehat{\mathbf{Y}}_b$ with sk and returns $\mathbf{Y}_b$ to SU b.
SU b:	(12) SU b recovers $\mathbf{X}_b$ by removing the blinding factor $\boldsymbol{\beta}$ from $\mathbf{Y}_b$.

the E-Zones computed by an IU can have multiple tiers. Each tier corresponds to SUs with a specific operation parameter setting. An SU operation parameter setting is a tuple $(f_s, h_s, p_{ts}, g_{rs}, i_s)$. Similarly, an IU operation parameter setting is a tuple $(f_i, h_i, p_{ti}, g_{ri}, i_i)$. f_s and f_i denote operation frequency, h_s and h_i denote antenna height, p_{ts} and p_{ti} denote transmitter effective radiated power, g_{rs} and g_{ri} denote receiver antenna gain, i_s and i_i denote receiver interference tolerance threshold.

Plug SU and IU's operation parameter settings into some accurate radio propagation model (e.g. Longley-Rice model), IU can accurately compute its E-Zone for a specific SU operation setting, which is denoted by $EZ(f_s, h_s, p_{ts}, g_{rs}, i_s)$. Each IU k in IP-SAS captures its multi-tier E-Zone information using a multidimensional E-Zone map matrix $\mathbf{T}_k := \{T_k(l, f, h_s, p_{ts}, g_{rs}, i_s)\}$, where

$$T_k(l, f, h_s, p_{ts}, g_{rs}, i_s) := \begin{cases} \epsilon, & \text{grid } l \in EZ(f, h_s, p_{ts}, g_{rs}, i_s) \\ 0, & \text{grid } l \notin EZ(f, h_s, p_{ts}, g_{rs}, i_s) \end{cases} \quad (1)$$

ϵ is a positive random number used to denote that SU is in the E-Zone and should not be allowed to operate, and 0 means SU is out of the E-Zone and can be allowed to operate.

To protect IU privacy against semi-honest $\mathcal{S}$, each entry of $\mathbf{T}_k$ is encrypted by pk before sending to $\mathcal{S}$. Therefore, IU k transmits $\widehat{\mathbf{T}}_k := \{\widehat{T}_k(l, f, h_s, p_{ts}, g_{rs}, i_s)\}$ when updating $\mathcal{S}$ with its E-Zone map.

1.4 E-Zone Map Aggregation in $\mathcal{S}$

Assume that there are altogether K IUs registered in $\mathcal{S}$ and all of them have sent in their E-Zone map. The first step of $\mathcal{S}$ is to aggregate all the IUs' E-Zone maps to create a global E-Zone map $\widehat{\mathbf{M}} := \{\widehat{M}(l, f, h_s, p_{ts}, g_{rs}, i_s)\}$ by $\widehat{\mathbf{M}} := \oplus_{k \in \{1,2,\ldots,K\}} \widehat{\mathbf{T}}_k$, where $\oplus$ is the homomorphic version of summation symbol $\sum$. From formula (1), it is easy to see that for an SU at location l with operation parameter setting $(h_s, p_{ts}, g_{rs}, i_s)$, if $M(l, f, h_s, p_{ts}, g_{rs}, i_s) = 0$, the grid l is out of E-Zones of all IUs and spectrum f is available for the SU; If $M(l, f, h_s, p_{ts}, g_{rs}, i_s) > 0$, f is unavailable for the SU.

1.5 Spectrum Computation Phase & Recovery Phase

When an SU b needs to access spectrum, it submits a spectrum request containing its operation parameters $(h_s, p_{ts}, g_{rs}, i_s)$ and location l in plaintext to $\mathcal{S}$. $\mathcal{S}$ retrieves the corresponding entries in the global E-Zone map $\widehat{\mathbf{M}}$ and generates $\widehat{\mathbf{X}}_b := \{\widehat{X}_b(f)\}$, where $\widehat{X}_b(f) := \widehat{M}(l, f, h_s, p_{ts}, g_{rs}, i_s)$. Essentially, $\widehat{\mathbf{X}}_b$ holds the spectrum availability information for SU b.

$\mathcal{S}$ then homomorphically adds some random blinding factors $\widehat{\boldsymbol{\beta}} := \{\widehat{\beta}(f)\}$ to obfuscate the results by: $\widehat{Y}_b(f) := \mathsf{Add}(\widehat{X}_b(f), \widehat{\beta}(f))$, where the plaintext of the blinding factor $\beta(f)$ is a one-time random number. $\widehat{\mathbf{Y}}_b$ and the plaintext $\boldsymbol{\beta}$ are both sent back to SU b. SU b needs to decrypt $\widehat{\mathbf{Y}}_b$ for the spectrum availability information, so it sends $\widehat{\mathbf{Y}}_b$ to $\mathcal{K}$ for decryption. $\mathcal{K}$ decrypts every entry of $\widehat{\mathbf{Y}}_b$ using sk and gets $\mathbf{Y}_b$. $\mathcal{K}$ cannot infer the spectrum availability information from $\mathbf{Y}_b$ since it does not have the values of the blinding factors $\boldsymbol{\beta}$ to recover $\mathbf{X}_b$. Finally, SU b recovers the correct spectrum computation results $\mathbf{X}_b$ by $X_b(f) = Y_b(f) - \beta(f)$.

2. PRELIMINARY RESULTS

We evaluate IP-SAS on a 154.82 km^2 area in Washington DC. We employ the Longley-Rice model provided by SPLAT! to generate the E-Zone maps in this area. High resolution terrain data SRTM3 is fed to SPLAT!. We build IP-SAS on a Paillier cryptosystem of 112-bit security level. Evaluation results show that the total time to process an SU spectrum request in SAS Server is around 1.25 seconds, and the total communication overhead for SU is 17.75 KB. In future work, we will extend IP-SAS to consider malicious parties.

3. REFERENCES

[1] Y. Dou, K. C. Zeng, H. Li, Y. Yang, B. Gao, C. Guan, K. Ren, and S. Li. P2-SAS: Preserving Users' Privacy in Centralized Dynamic Spectrum Access Systems. In *Proceedings of the 17th ACM MobiHoc*, pages 321–330, 2016.

[2] Y. Dou, K. C. Zeng, and Y. Yang. Poster: Privacy-Preserving Server-Driven Dynamic Spectrum Access System. In *Proceedings of the 21st ACM MobiCom*, pages 218–220, 2015.

[3] A. Ullah, S. Bhattarai, J.-M. Park, J. Reed, D. Gurney, and B. Bahrak. Multi-Tier Exclusion Zones for Dynamic Spectrum Sharing. In *Proceedings of IEEE ICC*, 2015.