IEEE ICDCS 2016

IP-SAS: Preserving Incumbent Users' Privacy in Server-Driven Dynamic Spectrum Access Systems

Yanzhi Dou∗, He Li∗, Kexiong (Curtis) Zeng∗, Jinshan Liu∗, Yaling Yang∗, Bo Gao† and Kui Ren‡

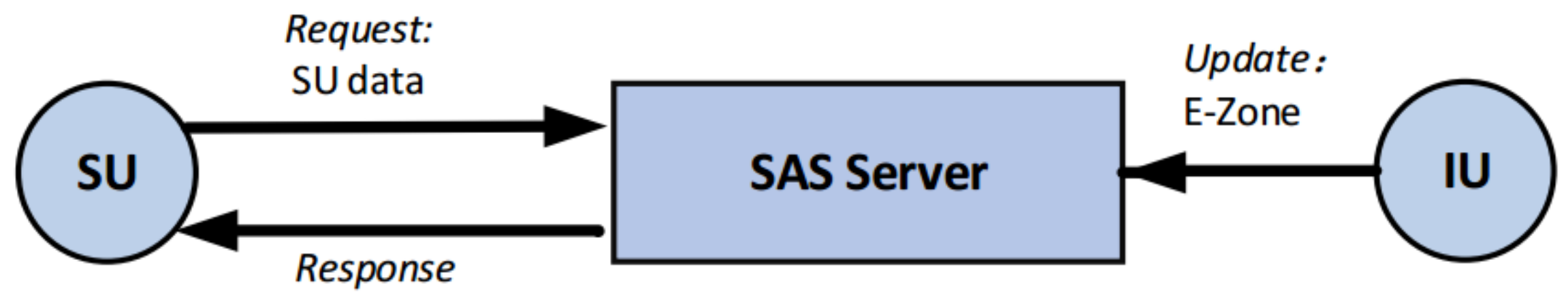
∗ Virginia Tech (USA) †Chinese Academy of Sciences (China) ‡SUNY at Buffalo (USA)

Background & Motivation

- To mitigate the potential spectrum scarcity problem and spur economic growth, PCAST and FCC have proposed spectrum access system (SAS) to realize the full potential of government-hold spectrum by sharing with wireless broadband operators/users.
- In current SAS proposals, the sensitive operation information of federal incumbent users (IUs) needs to be shared with the centralized SAS to realize spectrum allocation.
- However, SAS is not necessarily trust-worthy for holding such sensitive IU data. Particularly, PCAST and FCC allow industry third parties (e.g., Google) to operate SAS to enhance its efficiency and scalability.
- Therefore, the current proposals dissatisfy the IUs' privacy requirement, while IUs' privacy issues need to be carefully managed for promoting the flourish of federal-commercial sharing.

Problem Statement

- **System Model:** In a typical scenario of E-Zone-based SAS systems, IUs first compute their E-Zones and send the E-Zone data to SAS in the initialization phase. When an SU wants to access the 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.



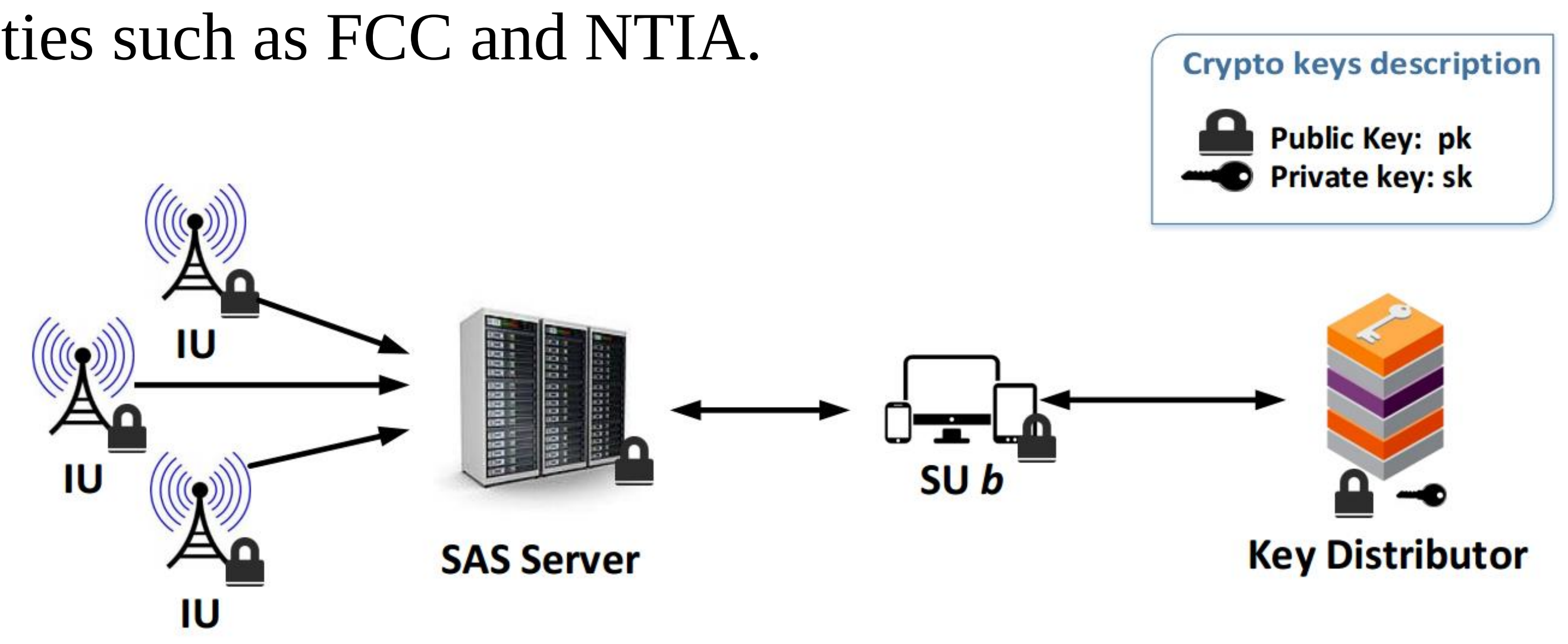
  - Remark: In this paper, we focus on the exclusion zone method for interference management. The privacy issue of the protection-zone method has been addressed in our previous work [1].

- **Adversary Model:** 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.

- **Design Goal:** 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.

System Design

IP-SAS involves four parties: (1) a SAS Server *S* for spectrum allocation, (2) IUs, (3) SUs, and (4) a Key Distributor *K*. *K* creates a Paillier public/private key pair (pk, sk) and is trusted for keeping sk a secret only known to itself. In the real world, the role of *K* can be played by some authorities such as FCC and NTIA.



Why Paillier Cryptosystem?

Homomorphic Addition ($\mathsf{Add}_{\mathsf{pk}}$):
$\mathsf{Dec}_{\mathsf{sk}}\left(\mathsf{Add}_{\mathsf{pk}}(\widehat{m_1}, \widehat{m_2})\right) = \mathsf{Dec}_{\mathsf{sk}}\left(\widehat{m_1} \cdot \widehat{m_2}\right) = m_1 + m_2.$

For notation simplicity, given any plaintext m, we denote $\widehat{m}$ as its ciphertext created using pk.

Protocol Details

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 (numbered as $1, 2, ..., k, ..., K$):
(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 uploads $\widehat{\mathbf{T}}_k$ to $\mathcal{S}$.
$\mathcal{S}$:
(5) Upon all IUs having uploaded their E-Zone map, $\mathcal{S}$ aggregates the E-Zone map of all IUs and 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 relays $\widehat{\mathbf{Y}}_b$ 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 $\mathbf{Y}_b$.

Formulas in Protocol Steps:

Step (2) $$T_k(l, f, h_s, p_{ts}, g_{rs}, i_s) := \begin{cases} \epsilon, & \text{grid } l \in EZ(f, h_s, p_{ts}, g_{rs}, i_s) \\ 0, & \text{grid } l \notin EZ(f, h_s, p_{ts}, g_{rs}, i_s) \end{cases}$$

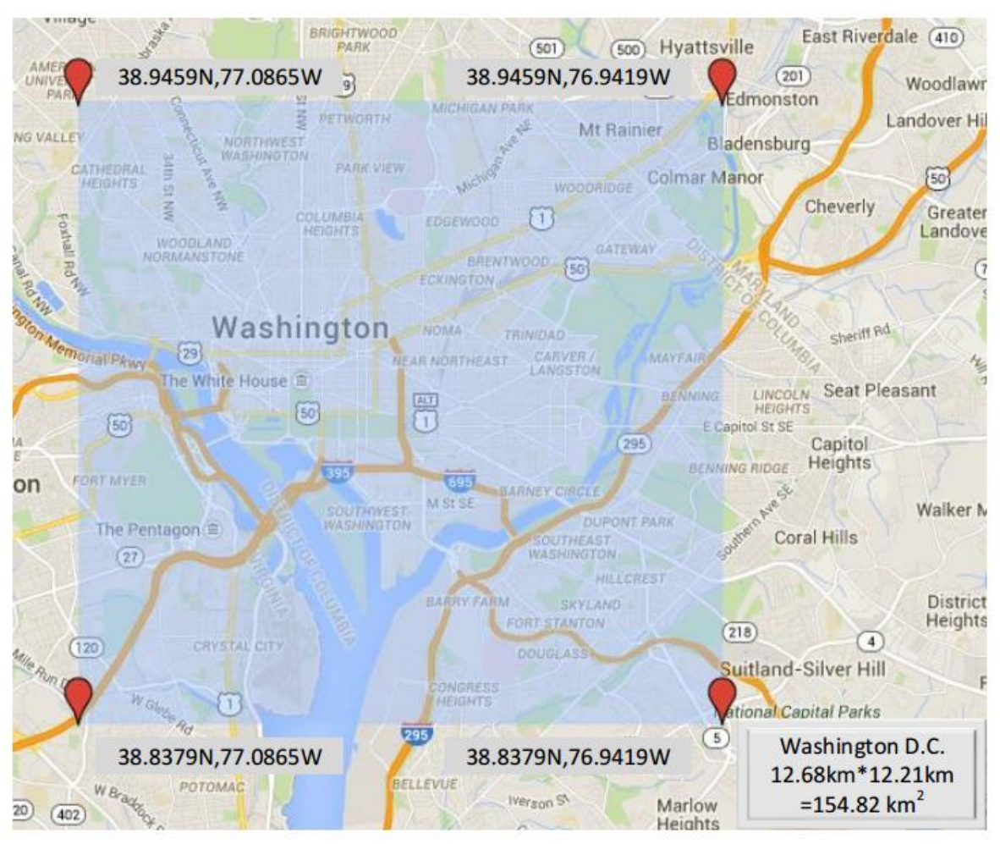
Step (5) $$\widehat{\mathbf{M}} := \oplus_{k \in \{1,2,\ldots,K\}} \widehat{\mathbf{T}}_k$$

Step (7) $$\widehat{X}_b(f) := \widehat{M}(l, f, h_s, p_{ts}, g_{rs}, i_s)$$

Step (8) $$\widehat{Y}_b(f) := \mathsf{Add}(\widehat{X}_b(f), \widehat{\beta}(f))$$

Step (12) $$X_b(f) = Y_b(f) - \beta(f)$$

Preliminary Results



- Washington D.C.
- Longley-Rice model provided by SPLAT! [2]
- High resolution terrain data SRTM3 [3]

- 112-bit security level.
- 1.25 second, 17.75 KB for each SU spectrum request.

The evaluation results show that IP-SAS's performance is good enough even for *mobile* SUs in highly changeable environment.

Conclusion & Future Work

In this paper, we build IP-SAS to perform efficient SAS process while preserving IUs' privacy. This system takes advantage of additive-homomorphic encryption to allow secure SAS operations. Experiments based on real-world data demonstrate the scalibility and practicality of IP-SAS in real-world deployment. In the future, we will design mechanisms to prevent non-colluding malicious parties from compromising the IP-SAS system.

References

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

[2] http://www.qsl.net/kd2bd/splat.html.

[3] http://dds.cr.usgs.gov/srtm/version2 1/SRTM3/.

Acknowledgement & Contact

This work is supported by US National Science Foundation under grant CNS-1547366, CNS-1228903, CNS-1054697.

For more information, please contact Yanzhi Dou (yzdou@vt.edu) or Yaling Yang (yyang8@vt.edu).