Privacy Preserving Integrated Sensing and Communication Architecture for 6G Networks

Prajnamaya Dass, Yevhen Zolotavkin, Stefan Köpsell
Barkhausen Institut, Dresden, Germany
{prajnamaya.dass|yevhen.zolotavkin|stefan.koepsell}@barkhauseninstitut.org

***Abstract*—Integrated sensing and communication (ISAC) technology allows sensing services alongside communications, supporting diverse 6G applications by detecting and analyzing the target areas. However, the collection and processing of sensing data containing personally identifiable information (PII) raises concerns about consent and transparency according to standard data protection regulations. To address this, in this paper, we integrate new functions into the 6G-ISAC architecture, focusing on transparency exposure, consent acquisition, and privacy enforcement. These functions ensure privacy and data regulatory requirements for each sensing request handled by the network. Furthermore, we explore various interface-based approaches to facilitate consent and transparency for users connected to their own mobile network operator (MNO), users belong to other MNOs, and users not connected to any MNO.**

***Index Terms*—Integrated sensing and communication, ISAC, JCAS, privacy, consent, transparency, 6G.**

I. Introduction

Integrated sensing and communication (ISAC) is one of the key technologies to be introduced in 6G systems, enabling the use of the same radio frequency signals for both communication and sensing. With ISAC, a 6G system can sense a target area using base stations (gNBs), process the collected data in the core network, and generate results for ISAC applications, as illustrated in Fig. 1. Potential applications include determining traffic density in specific areas, detecting obstacles at intersections, and monitoring object movements. Since sensing is involved, the 6G system will inevitably collect and process personally identifiable information (PII) of individuals within the target area. While user equipment (UE) can also participate in sensing and support application requests, this work focuses solely on privacy concerns related to gNB-based sensing.

Emerging 6G-ISAC architectures introduce new sensing management functions (SeMF), such as the sensing control function (SCF) for configuring sensing sessions and the sensing data processing function (SPF) for processing sensing data to produce the required results [1]. In previous work [2], we introduced a new function sensing policy, consent and transparency management (SPCTM) to consider the regulatory requirement for sensing data. However, that work did not explore how to effectively provide transparent information to PII owners or how to obtain their consent when necessary. Therefore, in this work, we present:

- New architectural functions, control and user plane flows within the 6G-ISAC framework that enable transparency exposure, consent acquisition, and privacy imposition into the core network design.
- 3GPP-aligned mechanisms to ensure consent and transparency for users within the sensing area – whether associated with their own mobile network operator (MNO), associated with other MNOs, or not associated with any MNO. We also present ISAC-specific input/output flows for 6G-ISAC interfaces, tailored to sensing session requirements.

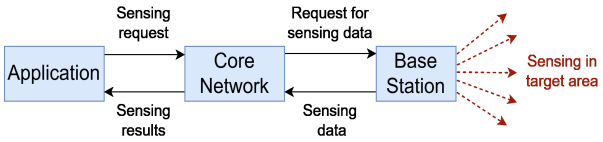

Fig. 1. Overview of 6G sensing services.

II. Privacy Preserving 6G-ISAC Architecture

Figure 2 shows the privacy-preserving ISAC architecture with newly introduced network functions and associated data and control flows. Along with SCF and SPF, the SPCTM can also be considered as part of the SeMF. The sensing request (`Sens_Req`) from the application function (AF) triggers sensing services in the core network via the network exposure function (NEF). After verifying initial security checks, NEF forwards the `Sens_Req` to the SCF, which acts as the enforcement point for sensing policies.

The SCF queries the SPCTM to determine applicable consent, transparency, and privacy policy requirements (`Sens_Pol_Req`) as per regulatory standards. SPCTM requests the unified data management (UDM) to fetch policies (`Policy_Fetch`) from the unified data repository (UDR). The UDM serves as the sensing policy administration and information point, responsible for storing, updating, and deleting policies. Based on

ISBN 978-3-903176-72-0 © 2025 IFIP

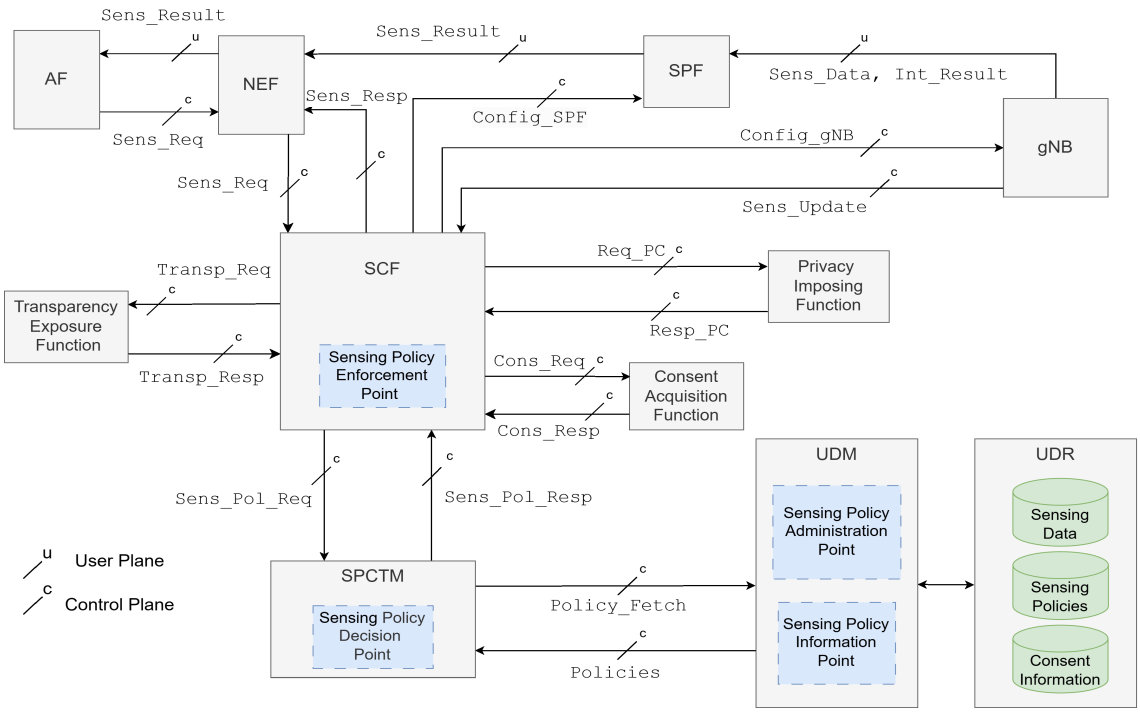

Fig. 2. Privacy-preserving ISAC architecture for 6G networks.

the returned `Policies`, the SPCTM evaluates what applies to the sensing request and responds to the SCF with the outcome (`Sens_Pol_Resp`), including permissions for sensing in the requested area, and consent, transparency, and privacy requirements. The SCF verifies feasibility and either responds to the AF (`Sens_Resp`) if the request is denied, or proceeds with parameters like result delivery timing and KPI assurances.

For transparency, the SCF uses the transparency exposure function (TEF) to deliver required information to all sensing targets (`Transp_Req`), as specified by SPCTM. The TEF determines the optimal method and responds with `Transp_Resp`. Similarly, the consent acquisition function assists SCF in identifying how to obtain consent from MNO users (`Cons_Resp`).

Each sensing request may carry specific privacy requirements. Thus, privacy controls must be imposed both during sensing and data processing. These controls are decided by the privacy imposing function in response (`Resp_PC`) to SCF's request (`Req_PC`). Before sensing, parameters like frequency, beamforming, and resolution are set for privacy-preserving data collection. During processing, controls such as data shielding or anonymization are applied and conveyed to the SPF via `Config_SPF` with other instructions.

Once all responses are collected, the SCF configures the sensing session and sends the configuration parameters (`Config_gNB`) to the gNBs. If needed, gNBs report back to the SCF with sensing updates (`Sens_Update`) such as operation failures or completion status. The gNB provides sensing data or intermediate results to the SPF, which processes them per SCF's instructions and delivers the final sensing result (`Sens_Result`) to the AF via NEF. Throughout, the SCF ensures that sensing events, updated policies, and necessary data are recorded in the UDM.

A. Potential Ways for Transparency and Consent

Delivering transparent sensing information to each sensing target and obtaining consent from the users is challenging but still feasible. Figure 3 outlines essential transparency and consent properties for ISAC services according to the standard legal requirement. Transparency and consent messages are exchanged via the sensing protocol (SeP) between the gNB and SeMF, and the ISAC API between SeMF and AF [3]. We explore implementation approaches based on current 3GPP architecture and proposed extensions.

Users from own MNO: The gNB can broadcast the transparent information to all its users through the system information block (SIB) messages. During handover, gNB performing sensing can send the transparency information, which will allows the user to select the network based on its choice.

As shown in Fig. 3, SeMF can send the consent and transparent messages to the connected UEs though the service-based interface NSeMF. N1–NSeMF (NAS) is a logical interface representing non-access stratum (NAS) signaling messages originating from the SeMF

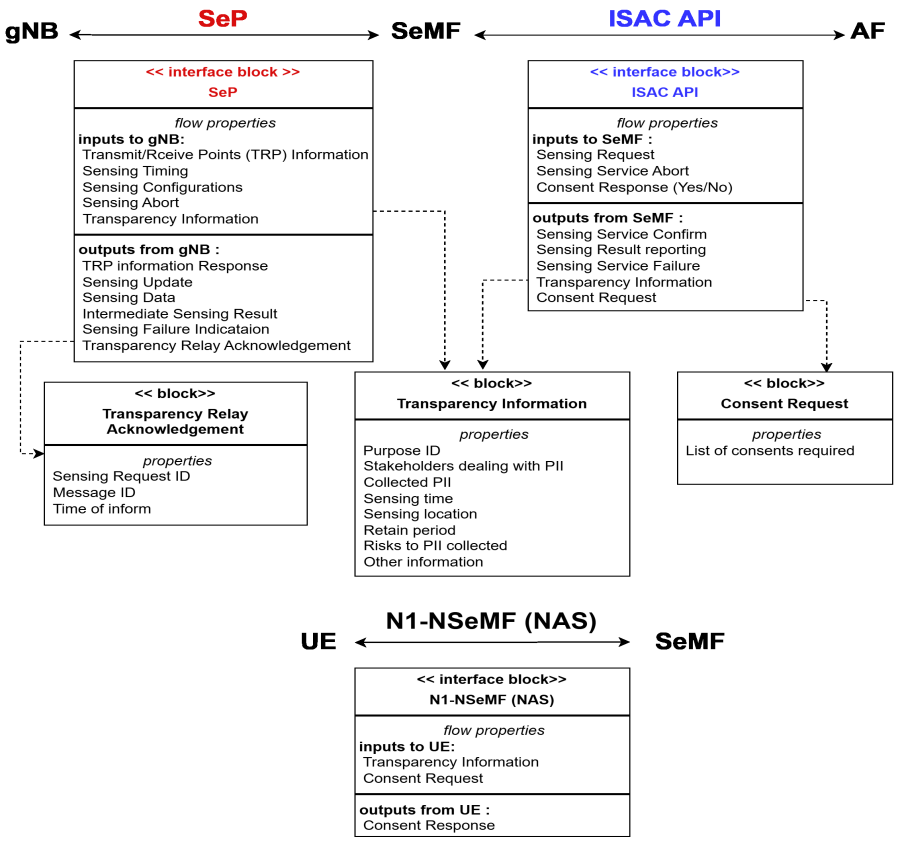

Fig. 3. ISAC-specific interfaces and flow properties to ensure consent and transparency in 6G networks.

and delivered to the UE via the access and mobility management function (AMF). This interface utilizes the standard 3GPP N1 interface between AMF and UE for delivery. However, custom NAS message types or containers should be defined for this purpose.

User associated to other MNO: When a gNB from one MNO performs sensing, it may also sense users from other MNOs within its coverage. In multi-operator core network scenarios [4], the gNB can still share sensing information with other operators, who in turn can relay transparency information to their respective users.

Users not connected to any MNO: The MNOs can provide transparency and consent mechanisms via a NEF-accessible application, enabling even unconnected users to grant consent when required. Sensing activities may also be published on a trusted public platform or website, showing information like which MNO performs sensing and where.

For all the cases, any changes to the transparency information (e.g., repurposing sensing data) must be disclosed to users again, requiring storage of the sensing data, involved users, and related details.

III. Conclusion

In this work, we discussed new network functions to address consent, transparency, and privacy requirements for ISAC in 6G systems. We also identified key properties aligned with regulatory requirements and explored potential implementation approaches based on current 3GPP standards. In future, we plan to design detailed interfaces for the proposed functions, along with their associated data and control flows.

Acknowledgment

This work has been supported by the Federal Ministry of Education and Research of Germany through the 6G-ICAS4Mobility project (grant no. 16KISK231) and KOMSENS-6G (grant no. 16KISK122). Additionally, the authors are also financed based on the budget passed by the Saxonian State Parliament in Germany.

References

[1] P. Gersing, M. Doll, J. Huschke, and O. Holschke, "Architecture proposal for 6G systems integrating sensing and communication." Available at: https://www.komsens-6g.com/, 2024. [Accessed on 17-03-2025].

[2] P. Dass, S. Ujjwal, J. Novotny, Y. Zolotavkin, Z. Laaroussi, and S. Köpsell, "Addressing privacy concerns in joint communication and sensing for 6G networks: challenges and prospects," in *Annual Privacy Forum*, pp. 87–111, Springer, 2024.

[3] "ISO/IEC Information technology — Online privacy notices and consent," *ISO/IEC 29184:2020(E)*, pp. 1–26, 2020.

[4] 3GPP, "Technical specification group services and system aspects; telecommunication management; network sharing; concepts and requirements (release 19)," Tech. Rep. 3GPP TS 32.130 V19.0.0, 3GPP, 2025.