**3GPP TSG-SA2 Meeting #170** **S2-2506196**

**25 – 29 Aug, 2025, Goteborg, SE (was S2-2505432)**

**Source: Nokia, KDDi**

**Title:** **Solution - Sensing service request and result exposure**

**Document for:** **Approval**

**Agenda Item: 20.2.1**

**Work Item / Release: FS\_Sensing\_ARC / Rel-20**

Abstract of the contribution: The contribution proposes a solution to KI#5, KI#6 and KI#2.

# Introduction

This contribution proposes the interface for the exposure of the sensing services.

# Discussion

There are various applications that could benefit by sensing services provided by an ISAC system. The Network Exposure Function (NEF) supports exposure of network capabilities to external application functions and shall be enhanced to also support exposing the ISAC capabilities. For managing the sensing service requests from different sensing consumers (also referred to as sensing clients in this document), a new core network function, Sensing Function (SF) needs to be introduced. The SF will interface with various network functions and sensing entities to perform sensing operation, calculate sensing result and send the result to the sensing clients. For an external/untrusted AF acting as sensing client, the sensing result shall be exposed via the NEF.

# Proposal

It is proposed update TR 23.700-14 v0.1.0 as below.

*FIRST CHANGE*

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |
| --- | --- |
|  | Key Issues |
| Solutions | KI#1 | KI#2 | KI#3 | KI#4 | KI#5 | KI#6 |
| #X |  | X |  |  | X | X |

*Second CHANGE (All new)*

## 6.X Solution #X: Sensing service request and result exposure

### 6.X.1 High-level solution Principles

Following are the high-level solutions principles that covers sensing configuration request, authorization the request and exposure of results

- Sensing capabilities are defined to detect objects and characteristics of the objects, and optionally environmental aspects.

- Sensing parameters for the sensing request between the SC and the SF and then to the SE are defined.

- Sensing request may be a one-time request, or a subscription for periodic or event-based result notification.

### 6.X.2 Description

The integration of sensing services into a communication system necessitates the introduction of a Sensing Function (SF), which determines and coordinates a sensing procedure, according to the sensing requirements, the network conditions, the capabilities of involved sensing entities (i.e. the sensing Tx and Rx) and the environment where the sensing takes place. The SF can be deployed as a dedicated Network Function (NF), since it is enabling a new functionality. For managing the sensing service requests from different sensing result consumers (also referred to as sensing clients in this document), a new core network function, Sensing Function (SF) is introduced.

The sensing service consumer can be a third party (e.g., an external Application Function (AF) such as a factory digital twin, or an NF. A trusted AF transmits to the SF a sensing service request and receives from the SF a sensing service output/result.

The network can offer one or more of the **following sensing capabilities:**

- Detect Objects according to Sensing Requirements (e.g., target area of sensing, accuracy etc.)

- Expose one or more of following characteristics w.r.t. the detected object:

- Location of the detected object

- Velocity of the detected object

- Attributes of the detected objects, e.g., type of object, size/shape of object, orientation of object etc.

- Environment sensing (e.g. rain detection)

NOTE 1: The detected Object can be a passive object (e.g. a human or an animal or a drone/vehicle without UE on board or any other passive objects etc.) or an object with UE onboard.

Editor’s Note: All the above capabilities are dependent on RAN study outcome.

Based on deployment scenarios and depending on the sensing request types, use cases and Sensing QoS requirements, there could be the following sensing result exposure types:

- Whether in a certain area an object (e.g., drone) is detected (e.g., intrusion detection)

- Sensing information identified in a specific area, which can be described for instance in the form of an object map.

- Sensing of environment conditions (e.g., rain).

The sensing request for any of the above may be a one-time request or a subscription-based request for periodic or event-based result notification. The events can be defined by the sensing client so as to trigger a specific sensing response.

#### 6.X.2.1 SF Functionality and System Architecture

In a cellular ISAC network, the SF can receive multiple and heterogeneous sensing requests from a Sensing Client (SC) (e.g., Application Function (AF) or other NFs) that indicate the type of the requested sensing service, the sensing area, the Sensing Quality of Service (SQoS) requirements, optionally information about the objects to be sensed etc. Each request may require its own configuration.

Firstly, the SF performs the authorization of the sensing service request and privacy checks for sensing data privacy as well as the privacy of users that are potentially impacted by sensing or are present in the target area for sensing. Then the SF determines the set of sensing operations to be performed, discovers and selects the Sensing Entities (SE) (e.g., BS) to be involved in a sensing session, according to the requirements in the sensing request and the available sensing capabilities in the sensing area of interest. For instance, different parts of the sensing area can be assigned to the different Sensing Entities. SF is then responsible for configuring the Sensing Entities by transmitting sensing operation configuration to the involved Sensing Entities, starting the sensing operations, collecting the measurement information, calculate the final sensing result and send the sensing result to the corresponding Sensing Client.

It should be noted that the SF can consist of two logical entities which may be collocated or placed at different physical entities: a) the Sensing Control Function (SCF) and b) the Sensing Processing Function (SPF).

- The SCF is responsible for the reception of sensing requests as well as the control and configuration of sensing operations.

- The SPF is responsible for collection and processing of sensing data received from one or more Sensing Entities to generate the required sensing outputs.

Editor’s Note: Whether the interface between the SCF and SPF is standardized is FFS.

#### 6.X.2.2 Parameters for configuration to the SF and then to SE

Depending on the sensing use case scenario and the application, one or more of the following information elements can be provided in the sensing service request:

a) Sensing service type: e.g., detection of an object type, tracking of an object, detection of environment conditions etc.

b) Sensing target area; indicates the location where the sensing service needs to be performed and may contain:

- Universal Geographical Area Description (GAD) as specified in TS 23.032.

- Target area which can be deduced from the location of onboard UE; if the request is to perform sensing in the proximity of a UE (i.e. the target sensing area is determined by UE's current location) then the UE ID is included in the request.

c) Sensing time parameters; indicates the time period over which the sensing is to be performed e.g., start time and end time and/or total duration.

d) Sensing context information

- target object type (e.g., drone, car, human etc): indicates the type of objects and its corresponding properties (e.g., object size, Radar Cross Section) that shall be detected in the specific sensing service request

- target object mobility profile (e.g., static, low mobility etc): indicates whether fixed objects or objects with a specific mobility profile shall be detected in the specific sensing service request

- environment of sensing (e.g. indoor, outdoor etc.)

e) Requested Sensing QoS parameters (SQoS); The QoS parameters include positioning accuracy, velocity accuracy and confidence level for the detected object(s), sensing range resolution for object detection, maximum latency to obtain the sensing result, missed detection probability, false alarm probability etc (see also TS 22.137 [x]).

f) Sensing results configuration:

- expected sensing output (e.g. detected object, location, velocity etc)

- periodicity of result reporting; shall be provided for sensing request with periodic result notification

- subscribed events for sensing result reporting; indicates when the SF shall trigger the provision of sensing results to the sensing client. Examples of these events can be:

 - Sensing results are sent in the case that a specific type of object (e.g., drone) is detected in the target sensing area.

- Sensing results are sent in the case that mobility is detected in the target sensing area.

- Sensing results are sent in the case that the velocity of an object in the target sensing area is above a defined speed threshold.

- sensing result exposure type (for e.g., object map); indicates the type of sensing results and corresponding parameters that the sensing client requests.

Editor’s Note: The parameters listed above (e.g., a), d), e), f)) are dependent on RAN study outcome.

#### 6.X.2.3 Result generation parameters or associated information

The sensing result that is transmitted to the Sensing Client depends on the sensing use case scenario and the requested sensing service type.

In the case of an object detection the following information elements can be provided:

Objects Map: Report more high-level information about the performed measurements, indicating characteristics of one or more objects including

- object ID

- object type (e.g., UAV, car, drone, pedestrian, building, etc…)

- object location information

- object detection time information

- object mobility information e.g., velocity

- confidence level for object detection and/or above parameters

The sensing results can also provide Sensing QoS information, in case that one or more Sensing QoS parameters are lower from the initial request.

Editor’s Note: Details of sensing data report from the SE based on sensing service type are dependent on RAN study outcome.

### 6.X.3 Procedures

#### 6.X.3.1 Sensing service procedure for on demand, periodic and event-based result exposure

 

Figure 6.x.2.2-1: Sensing service request authorization and result exposure

Figure 6.x.2.2-1 above shows the information flow for sensing service request and result exposure. The sensing service consumer can be a trusted/untrusted AF or an NF (e.g. NWDAF, LMF etc). In case of untrusted AF the request is forwarded via the NEF.

How the communication is implemented between the SF and the SE is carried out is not defined in the scope of this solution.

1. The sensing client (e.g. AF) sends a sensing service request to the SF. For untrusted AF the request is routed via the NEF. For the untrusted AF case, the NEF may perform AF authorization before forwarding the request to the SF. The sensing service request can be for a one-time (i.e. on demand) sensing result or it can be a subscription based request for periodic or event-based sensing result notification. The content of the sensing service request is described in section 6.X.2.2

 The appropriate SF is discovered through the NRF based on one or more of the following criteria:

- The expected Sensing QoS

- The target sensing area

- The SF capabilities required (e.g., sensing request type, method, processing capability etc.)

- By regulatory requirements e.g. the SF instance for emergency/public safety can be pre-configured.

2-3. The SF performs Sensing service request authorization and may also perform necessary privacy checks, as described in section 6.X.3.3.

**For the On Demand Sensing scenario:**

4. The SF then determines the appropriate sensing method, discovers and selects the corresponding sensing entities (i.e. sensing Tx, Rx) and configures them to start sensing session and report the measurement data. The SF calculates the result based on the measurement data collected from the sensing entities.

5. The SF provides the sensing result to the sensing client. The content of the sensing result is described in section 6.X.2.3

**For the periodic or event-based Sensing scenario:**

4. The SF then determines the appropriate sensing method, discovers and selects the corresponding sensing entities (i.e. sensing Tx, Rx) and configures them for sensing operation.

5. The SF sends sensing service response with a positive acknowledgement to the subscription from sensing client (in step 1) for the periodic or event-based sensing result notification. The sensing service response may also contain an immediate sensing result, if available.

6. At the configured periodicity or at the detection of the configured event(s), sensing operation is performed, the sensing data measurements are collected and reported to SF. The SF may perform privacy checks at this point again. The SF calculates the sensing result based on the measurement data collected from the sensing entities and notifies the sensing result to the sensing client. This step is performed at the subscribed periodicity or each time the subscribed event is detected. The content of the sensing result is described in section 6.X.2.3

NOTE 1: The details of how the SF determines the sensing method, how the SF selects and configures the sensing entities and how the SF collects the measurement data from the sensing entities are not in scope of this solution and assumed to be described in other solutions of this TR.

Editor’s Note: Configuring the sensing entities and sensing measurement data collection is dependent on RAN study outcome

#### 6.X.3.3 Sensing request authorization and privacy check

Once a sensing service request is received by the SF, the SF shall perform authorization and privacy checks depending on the type of the sensing service request, the target sensing area, the target objects sensing.

The privacy and policy checks may be performed based on the provisioned privacy profiles and policies, that indicates whether to allow or disallow a sensing service or what information can be exposed in sensing result. The following types of profiles may be used:

- Location-aware sensing profile that indicates whether to allow or not to allow a sensing request in a specific area.

- UE sensing privacy indication that indicates whether to allow or not to allow a sensing request for a specific UE.

- Object-aware sensing profile that indicates whether to allow or not to allow a sensing request for a specific object.

Information that shall be obfuscated when sending the sensing results; this shall be based on the privacy profile (as per above), for example for a specific object SF may obfuscate the location based on the requirement.

The above profiles can be used by the SF a) to configure a sensing procedure or b) to decide whether and what to expose with the sensing results for a specific sensing service request.

Editor’s Note: The privacy profiles shall be co-ordinated with SA3 WG as required.

6.X.4 Impacts on services, entities and interfaces

SF (New):

For scalability, for faster generation of sensing outputs and the more localised sensing data processing a separation of sensing control (SCF) and sensing data processing (SPF) logic can be assumed:

SCF:

- receives sensing requests from a sensing consumer and provides the sensing outputs to the sensing consumer.

- conducts authorization and privacy-related checks for each sensing service request

- discovers and selects the sensing entities to be involved in the sensing session.

- configures and control the sensing sessions that serve a specific sensing service request , according to the requirements received in the sensing service request, and the available sensing capabilities in the target sensing area.

- transmit sensing session configuration to the involved sensing entities.

SPF:

- collects and processes the sensing data from sensing entities to generate the required sensing outputs.

NEF:

- receives a sensing service request from an (untrusted) AF sensing request and after AF authorization forwards to the selected SF, including in the request message the attributes received from the AF request and if needed converting certain received parameters into 5GC internal parameters (e.g. target sensing area).

- receive sensing result from SF and forward the result to the untrusted AF

- selects the SF that can serve a specific sensing service request, according to the requested sensing area and/or the sensing service request requirements.

NRF:

* stores the profile of each SF, indicating the supported sensing capabilities and features (e.g., supported sensing area, supported sensing services)

AF:

- trusted AF transmits to the SF a sensing service request and receives from a SF a sensing service output, In the case of untrusted AF NEF is involved.

*End of Changes*