ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Report

(11/2025)

YSTR.ISAC-fra

Considerations on integrated sensing and communication in IMT-2020 networks and beyond

Technical Report ITU-T YSTR.ISAC-fra

Considerations on integrated sensing and communication in IMT-2020 networks and beyond

Summary

This Technical Report provides considerations on the requirements and framework of integrated sensing and communication in IMT-2020 networks and beyond. It addresses the following aspects:

– overview of integrated sensing and communication;

– potential requirements of integrated sensing and communication;

– framework considerations on integrated sensing and communication.

Keywords

IMT-2020 networks and beyond, integrated sensing and communication, sensing function.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Technical Report ITU-T YSTR.ISAC-fra

Considerations on integrated sensing and communication in IMT-2020 networks and beyond

1 Scope

This Technical Report provides considerations on integrated sensing and communication in IMT-2020 networks and beyond. The scope of this Technical Report includes:

– overview of integrated sensing and communication;

– potential requirements of integrated sensing and communication;

– framework considerations on integrated sensing and communication.

2 References

[ITU-T Y.3104] Recommendation ITU-T Y.3104 (2018), *Architecture of the IMT-2020 network.*

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following term defined elsewhere:

3.1.1 device [b-ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.2 Terms defined in this Technical Report

This Technical Report defines the following term:

3.2.1 sensing function: A network function providing the capabilities of integrated sensing and communication.

NOTE – These capabilities include, but are not limited to, sensing authentication, sensing procedure control, sensing capability acquisition, sensing node selection, sensing measurement data processing and sensing results exposure.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AF Application Function

AI Artificial Intelligence

AN Access Network

ASF Authentication Server Function

CEF Capability Exposure Function

CN Core Network

ISAC Integrated Sensing and Communication

KPI Key Performance Indicator

LOS Line-Of-Sight

NACF	Network Access Control Function
NFR	Network Function Repository
NLOS	Non-Line-Of-Sight
NSSF	Network Slice Selection Function
PCF	Policy Control Function
QoS	Quality of Service
RF	Radio Frequency
SF	Sensing Function
SMF	Session Management Function
UAV	Unmanned Aerial Vehicle
UE	User Equipment
UPF	User Plane Function
USM	Unified Subscription Management

5 Conventions

In this Technical Report, potential requirements, which are derived from a given use case, are classified as follows:

The keywords "it is of critical value" indicate a possible requirement which would be necessary to be fulfilled (e.g., by an implementation) and enabled to provide the benefits of the use case.

The keywords "it is expected" indicate a possible requirement which would be important but not absolutely necessary to be fulfilled (e.g., by an implementation). Thus, this possible requirement would not need to be enabled to provide complete benefits of the use case.

The keywords "it is of added value" indicate a possible requirement which would be optional to be fulfilled (e.g., by an implementation), without implying any sense of importance regarding its fulfilment. Thus, this possible requirement would not need to be enabled to provide complete benefits of the use case.

6 Overview of integrated sensing and communication

Integrated sensing and communication (ISAC) technology enables IMT-2020 networks and beyond with the capability to sense the physical world. At the same time, the information about the physical word can also enhance the capability of the network. Via ISAC, both communication-assisted sensing and sensing-assisted communication are enabled.

6.1 Communication-assisted sensing

In communication-assisted sensing, IMT-2020 networks and beyond utilize the existing infrastructure and devices to sense the characteristics of surrounding objects and environments. The collected sensing information can then be transmitted to the core network (CN) for further processing and service delivery.

The overall sensing process is shown in Figure 6-1. It illustrates the relationships between the key components and the chaining of concepts involved in communication-assisted sensing. First, the service requesters initiate a sensing service request through an application user. The network then selects appropriate sensing nodes to perform required sensing tasks based on the sensing capabilities to support the sensing service. Generated sensing data will be provided by selected sensing nodes through a sensing service to the sensing requesters directly or to applications. These steps together constitute the end-to-end sensing process in communication-assisted sensing systems.

NOTE 1 – Sensing services are the services by which networks provide sensing data and sensing information to service requesters.

The sensing services can support various sensing-related applications. Typical sensing service examples include ranging, speed and angle measurement, positioning, tracking, imaging, detection and recognition, which can be provided to applications (sensing-related applications), such as intelligent transportation, smart home, health monitoring and environment detection. Depending on the business scenarios, diverse sensing services can be selected.

NOTE 2 – The sensing nodes in IMT-2020 networks and beyond are hardware and/or software that provide the sensing capability to applications.

The sensing nodes may be located in a core network and be supported by core network elements. The sensing nodes may be also located in the access network and be supported by sensing devices, such as base station devices and terminal devices. Specific network functions and devices related to sensing are enhanced to support the sensing capability.

NOTE 3 – The sensing capability is the ability of the network to detect, measure and provide sensing data. The sensing capability of a single sensing node may be limited. Multiple sensing nodes can be fused to achieve collaborative sensing.

The sensing capability can be described by sensing capability information.

NOTE 4 – Sensing capability information refers to specific parameters, performance and other information related to different sensing services, such as sensing delay, service area, sensing accuracy and resources.

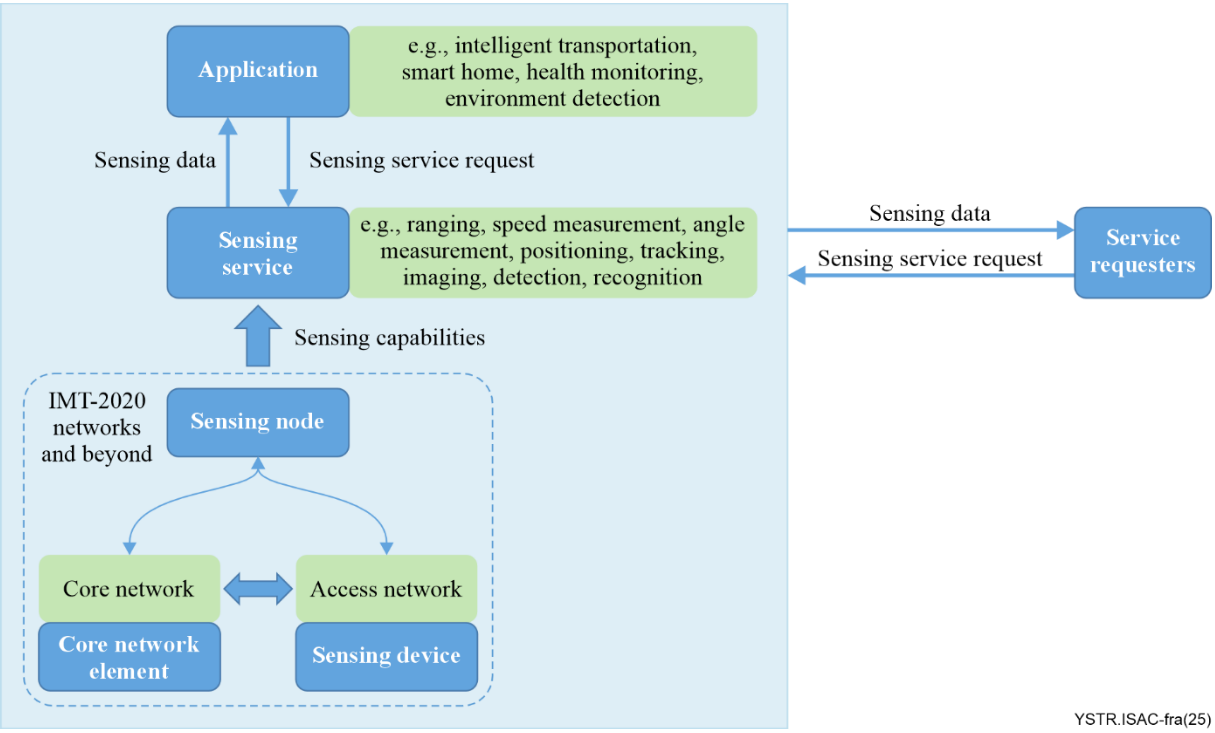

Figure 6-1 – An overview of the sensing process in communication-assisted sensing

In the context of communication-assisted sensing, intelligent data analysis plays a crucial role in optimizing sensing performance. It supports intelligent node selection, flexible control of the sensing processes and dynamic allocation of sensing resources.

NOTE 5 – For example, according to key performance indicators (KPIs) such as sensing resolution, accuracy and business requirements, the core network functions can be dynamically selected and resource allocation can be performed as needed.

NOTE 6 – As far as intelligent data analysis, in dynamic network environments, reinforcement learning can enable dynamic decision-making to select appropriate sensing nodes.

Moreover, intelligent data analysis and sensing results prediction are required for the reported data from sensing nodes.

NOTE 7 – For instance, deep learning methods can extract high-level features embedded in sensing information to achieve target recognition and classification. When sensing data is insufficient, the network can utilize generative AI models to generate and enhance data based on historical data, thereby improving network sensing capabilities.

6.2 Sensing-assisted communication

In sensing-assisted communication, through further analysis of the sensing measurement data, a network optimization scheme can be designed to enhance communication capabilities.

In the context of sensing-assisted communication, in terms of intelligent network optimization, the ISAC technology enables real-time network monitoring, user demand analysis and device status perception. Through data analysis, the network can automatically optimize resource allocation to provide more efficient and stable network connections and service quality, thus meeting the growing communication demands.

In the context of sensing-assisted communication, the ISAC technology also allows the network to dynamically adjust communication parameters based on different environments and usage scenarios, thus enabling energy conservation in the network.

7 Potential requirements of integrated sensing and communication

7.1 Common requirements of integrated sensing and communication

It is of critical value that IMT-2020 networks and beyond support both communication capabilities and sensing capabilities.

It is expected to support:

– authentication for sensing services;
– triggering, modification and termination of sensing processes according to sensing service requests;
– acquisition of sensing capability information of network functions;
– selection of suitable sensing nodes;
– handling of sensing measurement data;
– exposure of sensing capabilities and sensing results.

The following subclauses provide detailed requirements with respect to the points above.

7.1.1 Authentication

It is of critical value that IMT-2020 networks and beyond support the authentication of sensing service requests and sensing devices.

NOTE 1 – Sensing services may involve sensitive information regarding sensing targets and sensing areas, thus authentication is necessary to mitigate security risks associated with sensing.

Authentication refers to verifying whether a sensing service requester has the right to access the network.

NOTE 2 – When the sensing service requester requests the sensing service from the network, the network determines whether to allow the use of its sensing capabilities by the sensing service requester based on the authentication information of the service requester.

NOTE 3 – Authentication checks are based on specific applications, users, sensing quality of service (QoS), geographical regions, time requirements, etc.

Authentication also refers to verifying whether a sensing device has the right to register its sensing capabilities to the network.

NOTE 4 – When the sensing device registers its sensing capabilities to the network, the network determines whether to allow it to register them based on the network operator's policies or the authentication information of the device.

NOTE 5 – Authentication can include checks on aspects such as the type of sensing device, the type of sensing capability, the sensing area, time, etc.

7.1.2 Sensing service requests processing

Sensing service requests refer to the sensing service requirements of the service requester on the network.

It is of critical value that IMT-2020 networks and beyond support the handling of sensing service requests from the service requester.

NOTE 1 – The service requester can be user equipment (UE), an internal network function or external application servers.

NOTE 2 – Upon receiving a sensing request, the network triggers a sensing process based on the service type (such as low-altitude UAV ranging and vehicle tracking) and the service requirements (such as sensing accuracy, sensing resolution, latency, etc.).

NOTE 3 – The network modifies the sensing process when there are changes in the sensing service request information and terminates the sensing process based on actual conditions.

7.1.3 Acquisition of sensing capability information

It is of critical value that IMT-2020 networks and beyond support the acquisition of sensing capability information of sensing nodes.

NOTE 1 – Sensing nodes may report their sensing capability information in real time or on demand.

NOTE 2 – Sensing nodes include network functions for sensing, sensing devices and other enhanced network functions supporting sensing capabilities.

NOTE 3 – Sensing devices refer to devices that send a sensing signal or receive a sensing signal and take a measurement. They include base stations devices and terminal devices such as UEs.

NOTE 4 – Sensing devices report their information related to sensing services to the network, allowing other network functions to select sensing devices suitable for a sensing service based on the type and requirements information of the sensing service, etc.

NOTE 5 – Network functions for sensing report information about their capabilities related to sensing services, allows other network functions to select sensing functions suitable for a sensing service based on the type of sensing service, requirements, regional restriction information, etc.

7.1.4 Sensing nodes selection

It is of critical value that IMT-2020 networks and beyond support sensing nodes selection in order to meet the need of sensing services.

NOTE 1 – Different sensing nodes (such as network functions for sensing) located in different places may be deployed in the network due to the need of zone management or management of different types of sensing services.

NOTE 2 – When initiating a sensing service request, the network selects a specific network function suitable for the sensing service based on the type of sensing service, requirements, regional restriction information, etc.

NOTE 3 – The selection of sensing nodes considers factors such as the location, load and capabilities of sensing nodes.

NOTE 4 – The network chooses appropriate options for sensing, i.e., different sensing modes based on sensing requests: (1) single base station responsible for both transmission and reception; (2) one base station responsible for transmission and another base station responsible for reception; (3) one base station responsible for transmission and one UE responsible for reception; (4) single UE responsible for both transmission and reception; (5) one UE responsible for transmission and one base station responsible for reception; and (6) one UE responsible for transmission and another UE responsible for reception.

NOTE 5 – Based on the selected sensing mode and the capability information of the sensing devices, network functions for sensing select suitable sensing devices in order to serve the sensing services, thereby performing the transmission of sensing signals, measurement of sensing signals and reporting of sensing measurement data.

7.1.5 Sensing measurement data processing

It is of critical value that IMT-2020 networks and beyond support the processing of sensing measurement data according to sensing requests and reports the sensing results.

NOTE – In different sensing scenarios and service requirements situations, the original sensing signals received by sensing devices (such as complex values of channel responses with amplitude and phase) will be processed by one or more processing nodes to obtain sensing measurement data (such as latency, doppler, angle) or sensing results (such as distance, speed, position, trajectory, heart rate, imaging results).

7.1.6 Sensing capabilities exposure

It is of critical value that IMT-2020 networks and beyond support the exposure of the sensing capabilities of sensing nodes to sensing services and to expose sensing results to sensing service requesters.

7.2 Requirements of collaborative sensing

7.2.1 Multi-mode collaborative sensing

It is of critical value that IMT-2020 networks and beyond support multi-mode collaborative sensing.

NOTE 1 – There are several available sensing modes, as described in clause 7.1.4.

NOTE 2 – The network supports the fusion of these modes to achieve multi-mode collaborative sensing. Thus, the multi-mode collaborative sensing effectively makes up for the shortcomings of different modes.

NOTE 3 – As an example, in the condition of one base station responsible for transmission and another base station responsible for reception, when there is an obstacle (such as a building in the city) between two base stations, the sensing link will be non-line-of-sight (NLOS). A sensing device UE can be used to make collaborative sensing, providing two line-of-sight (LOS) paths between two base stations and UE, leading to a better sensing condition.

7.2.2 Multi-source collaborative sensing

It is of critical value that IMT-2020 networks and beyond support multi-source collaborative sensing.

NOTE 1 – There are many sensing technologies, including video, image, sensor, radar, radio frequency (RF), etc. The sensing capability of a single sensing technology is usually limited.

NOTE 2 – Combining different sensing technologies to realize multi-source sensing effectively plays to the advantages of the different sensing technologies in different situations.

NOTE 3 – As an example, the sensing technologies based on image and video can obtain more detailed information about the sensing target, but they have disadvantages in poor lighting and NLOS environments. However, radar sensing and RF sensing have considerable advantages. In addition, the wide variety of sensors has absolute advantages in high-precision scenarios. Therefore, integrating these technologies to achieve multi-source collaborative sensing will greatly improve sensing performance.

7.2.3 Multi-node collaborative sensing

It is of critical value that IMT-2020 networks and beyond support multi-node collaborative sensing.

NOTE 1 – The sensing capability of a single sensing node is usually limited.

For example, there are certain limitations in the scope and accuracy of the sensing. Therefore, it is necessary for the network to have the capability of multi-node collaborative sensing.

NOTE 2 – Different sensing nodes carry out sensing measurements of the same sensing target or sensing area. The sensing measurements from different directions and distances provide more complete information. The sensing data of different sensing nodes is fused and processed by the network to improve sensing performance.

7.3 Requirements of communication-assisted sensing

It is of critical value that IMT-2020 networks and beyond support communication-assisted sensing. IMT-2020 networks and beyond support different functions, such as management and scheduling, collaborative processing, intelligent computing, data storage and performance evaluation, for executing sensing tasks.

The specific requirements of the IMT-2020 networks and beyond for communication-assisted sensing are given in the following clauses 7.3.1 to 7.3.5.

7.3.1 Resource management and scheduling

It is of critical value that IMT-2020 networks and beyond support resource management and scheduling.

NOTE 1 – The network dynamically allocates network resources, including core network resources and access network resources, based on the requirements of communication and sensing tasks, enabling real-time scheduling to balance communication and sensing performance.

NOTE 2 – The network dynamically allocates computational and storage resources for sensing tasks and continuously optimizes allocation strategies to support large-scale sensing tasks.

NOTE 3 – The network dynamically balances traffic and node loads based on sensing demands, avoiding bottlenecks and congestion.

7.3.2 Cloud-edge collaborative processing

It is of critical value that IMT-2020 networks and beyond support cloud-edge collaborative processing.

NOTE 1 – Certain sensing scenarios demand low latency and rapid response. By deeply integrating cloud and edge computing capabilities, some sensing tasks (e.g., signal processing, sensing-related data (sensing data) analysis) can be offloaded to the edge, reducing the computational burden on the network.

NOTE 2 – Robust edge computing capabilities can process large volumes of sensing data in real time, significantly reducing sensing response times.

7.3.3 Intelligent computing

It is of critical value that IMT-2020 networks and beyond support intelligent computing.

NOTE 1 – The network deploys AI capabilities to provide intelligent computing for sensing tasks.

NOTE 2 – The network supports multi-modal, multi-source and multi-node data fusion, enabling centralized processing and integration of sensing data to enhance accuracy and reliability.

7.3.4 Historical data storage

It is of critical value that IMT-2020 networks and beyond support historical data storage.

NOTE 1 – The network stores and archives the historical data related to sensing tasks for performance optimization and issue diagnosis.

NOTE 2 – Historical data involves sensing data in various stages, such as original sensing signals, sensing measurement data and sensing results.

7.3.5 Performance evaluation

It is of critical value that IMT-2020 networks and beyond support performance evaluation.

NOTE 1 – The network supports performance evaluation of sensing results (e.g., sensing accuracy, resolution, coverage range) to ensure that sensing performance meets service requirements.

NOTE 2 – Based on feedback from performance evaluations, the network dynamically adjusts sensing strategies to optimize results.

7.4 Requirements of sensing-assisted communication

It is of critical value that IMT-2020 networks and beyond support sensing-assisted communication.

7.4.1 Communication resource scheduling and optimization

It is of critical value that IMT-2020 networks and beyond support communication resource scheduling and optimization based on sensing data.

NOTE – The network can optimize resource scheduling strategies by leveraging sensing-derived user information (e.g., location, quantity, mobility) and environmental information (e.g., buildings, roads, vehicles). By sensing user locations and densities, the network can accurately adjust signal coverage areas and resource allocation strategies. As an example, for users in densely populated areas or complex environments, communication resource allocation can be enhanced to ensure network service quality and user experience, while in sparsely populated areas, resource allocation can be reduced to improve overall network energy efficiency.

7.4.2 Network energy saving

It is of critical value that IMT-2020 networks and beyond support network energy saving based on sensing data.

NOTE 1 – The network improves network energy efficiency by utilizing sensing capabilities to optimize communication resource usage and reduce unnecessary energy consumption.

NOTE 2 – Sensing data provides real-time information about network traffic and user locations, enabling the dynamic adjustment of network resources.

NOTE 3 – By sensing user proximity and access network conditions, the network can optimize transmission power, reducing energy consumption without compromising service quality.

NOTE 4 – Sensing capabilities help identify low traffic areas and allows base stations to switch to low power modes or turn off unused resources.

8 Framework considerations of integrated sensing and communication

Figure 8-1 illustrates the framework of integrated sensing and communication which is based on the IMT-2020 framework specified in [ITU-T Y.3104]. The framework is enhanced with the sensing function (SF) for enabling integrated sensing and communication in IMT-2020 networks and beyond.

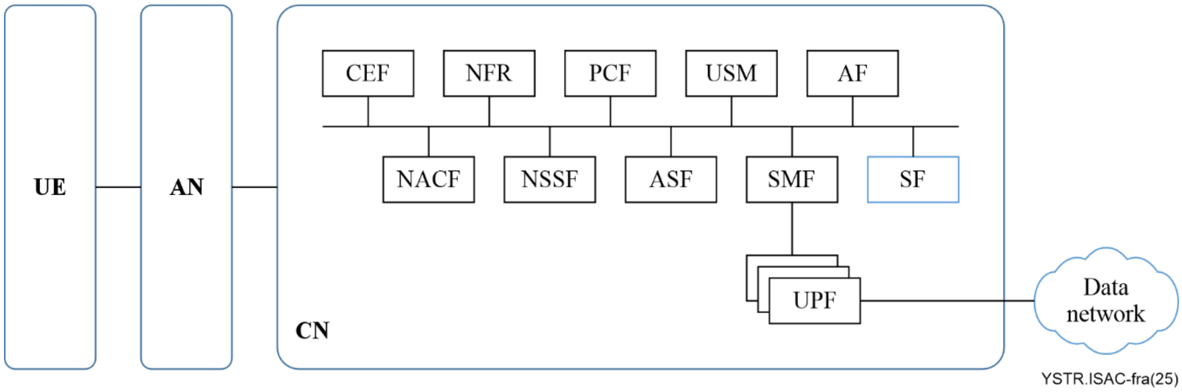

Figure 8-1 – Framework of integrated sensing and communication

The IMT-2020 network receives sensing information from UE or an AN, and provides the sensing information possessing capabilities. When the CN receives a sensing service request, the CN schedules the sensing resources and conducts the sensing process, which is executed by an SF in cooperation with other core network functions.

Specifically, according to the requirements specified in clause 7, SF interacts with other entities to provide the capabilities which are described in clauses 8.1 to 8.6.

8.1 Authentication capability

The SF performs authentication the first time it receives a sensing request or a sensing device registers its sensing capabilities to the network.

When the sensing service requester (such as UE or an internal network function) requests a sensing service from the network, the authentication information can be stored in unified subscription management (USM) or an SF, and the network access control function (NACF) and the authentication server function (ASF) conduct authentication checks on the UE or internal network elements based on the authentication information obtained from USM or the SF.

When the sensing service requester (such as an external application) requests a sensing service from the network, the authentication information can be stored in USM or an SF. The capability exposure function (CEF) conducts authentication checks on an application function (AF) based on the authentication information obtained from USM or an SF.

The authentication information for the sensing devices can be stored in USM or an SF. The NACF or ASF conducts authentication checks based on the obtained authentication information.

8.2 Sensing service requests processing capability

The SF supports initiation, update and termination of the sensing process based on the sensing service requirements.

When the network receives the sensing request from UE or from the AF through CEF, it generates sensing control commands for the sensing devices based on the service requirements carried in the sensing request to obtain the corresponding sensing measurement data; when the sensing service requirements change, an SF supports the update or termination of the sensing process.

8.3 Sensing capability acquisition capability

The SF acquires sensing capability information of sensing nodes.

Not all sensing nodes in the IMT-2020 network and beyond support the sensing function. For instance, only a portion of UEs or ANs or network elements support the sensing function and interact with the SF; moreover, each network element will have its own service area. Therefore, in order to successfully execute the sensing service request, the sensing nodes that support the sensing function need to notify their sensing capabilities to other network elements or register the information of the capabilities it supports to the network function repository (NFR), so that the other network elements can query and select the network elements with the corresponding sensing capabilities.

The NACFs acquire the sensing capabilities and register them to the NFR, for the SF to select an appropriate NACF.

The SF registers its sensing capabilities to the NFR, for the CEF to select an appropriate SF.

8.4 Sensing nodes selection capability

The SF selects the appropriate sensing node for the different sensing services taking into account the location, capabilities, load and authentication information of sensing nodes.

As mentioned in clause 7.1.4, there are six basic sensing modes. Additionally, in the actual sensing process, these six sensing modes can be combined in different ways according to various sensing scenarios, sensing environments and sensing service requirements.

As the centralized control node, an SF selects the sensing nodes and determines the appropriate sensing modes, the transmission and reception roles of the sensing devices, sensing frequency, sensing time and sensing performance, based on the sensing service requirements, AF expected sensing mode, sensing result information (SF historical sensing statistics information), AN capability information, resource information and UE capability information.

8.5 Sensing measurement data processing capability

The SF generates the final sensing result upon receiving the sensing measurement data.

The processing of data takes into account supporting scenarios of multiple sensing devices. For example, in the multiple sensing devices scenario, the sensing areas of different sensing devices may overlap. Therefore, data processing involving information extraction and merging is carried out.

After obtaining sensing measurement data based on sensing requirements, the sensing devices report the data to the SF for processing. The SF then generates the final sensing results. The sensing measurement data processing involves single-site sensing, multi-site non-cooperative sensing and multi-site cooperative sensing.

Multi-site non-cooperative sensing: sensing results are generated based on the sensing measurement data from multiple sites. However, the sensing measurement data from each site does not overlap or have any correlation. The sensing measurement data is not processed collaboratively.

Multi-site cooperative sensing: sensing results are generated also based on the sensing measurement data from multiple sites. And the multi-site sensing measurement data is collected for the same area or for the same sensing service. The multi-site sensing measurement data can be fused and processed collaboratively to improve sensing performance.

8.6 Sensing results exposure capability

The SF exposes the sensing measurement data and the sensing results to the sensing service requesters.

Sensing results exposure refers to the situation where, after receiving a sensing request from the sensing service requester (such as an external AF or UE or internal network element), the SF generates sensing control commands for the sensing device to perform sensing operations and obtain sensing measurement data. It then processes the sensing measurement data to generate sensing results and finally opens these results to the external AF through the CEF, or it directly sends them to the UE and internal network elements. With the authentication of the network and user consent, the SF can also open the sensing results to non-sensing service requesters' network functions or systems, such as the management system, for intelligent analysis.

9 Workflow of integrated sensing and communication

This clause provides typical workflows of the sensing process of integrated sensing and communication.

The sensing process can be triggered by the AF or UE to send a sensing request. The AF sends the sensing request to the SF through the CEF and NACF. The UE sends the sensing request to the SF through the NACF.

The SF is enabled to generate sensing control commands to the sensing devices to perform sensing measurements based on the sensing request, as well as to calculate and provide the sensing results to the AF and UE.

9.1 The sensing process triggered by AF

Figure 9-1 illustrates the sensing process triggered by the AF.

The process begins when the AF initiates a sensing service request (step 1) toward the CEF. Upon receiving the request, the network performs sensing authentication (step 2) to verify the validity of the service requester and the requested sensing task. After successful authentication, a sensing request (step 3) is sent. The NACF performs sensing node selection (step 4), determining appropriate sensing nodes based on their capability information and current network conditions. Once the sensing nodes are selected, a sensing request (step 5) is issued to the AN or to the UE, depending on where the sensing process will be executed. The sensing process is then carried out either by the AN (step 6a) or by the UE (step 6b). During this process, the sensing data is collected and processed. The resulting sensing data processing (step 7) produces the sensing information required for the service. The network then sends back a sensing response (step 8) to the SF and the processed results are subsequently exposed to the AF (step 9) via the CEF, completing the sensing service procedure.

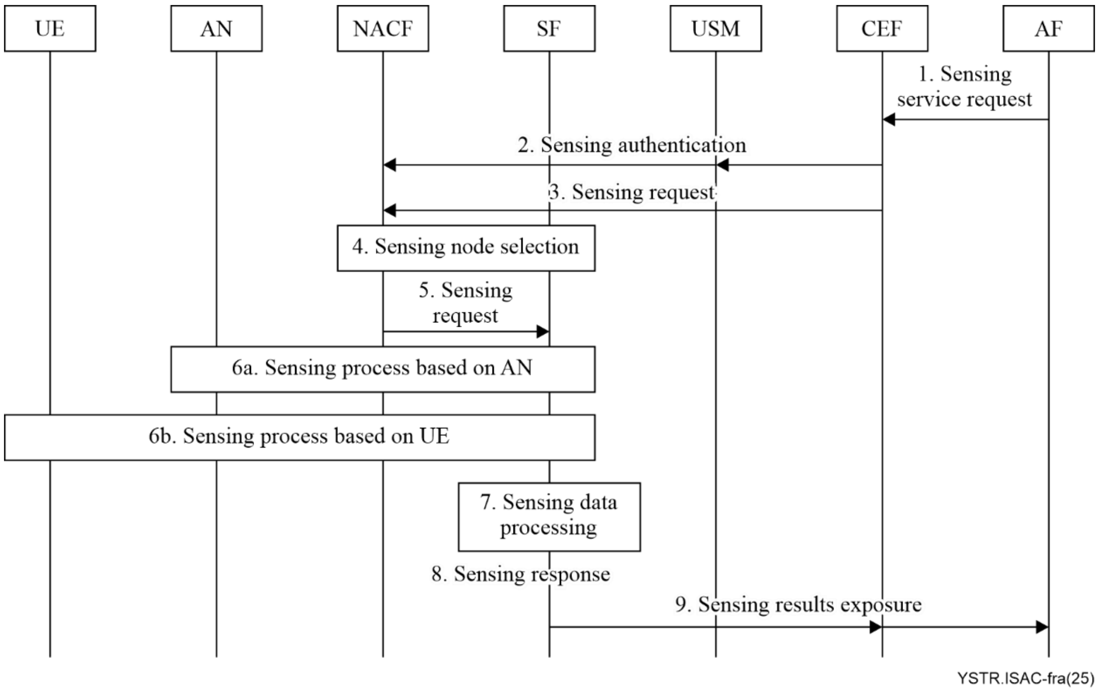

Figure 9-1 – The sensing process triggered by an application function (AF)

9.2 The sensing process triggered by UE

Figure 9-2 illustrates the sensing process triggered by UE.

The sensing process can be triggered by UE to send a sensing request (step 1). After the sensing authentication (step 2), the NACF performs sensing node selection (step 3), then forwards the sensing request to the SF node (step 4). This enables the SF to generate sensing control commands to the sensing devices to perform sensing measurements based on the sensing request. The sensing process is then carried out either by the AN (step 5a) or by the UE (step 5b). During this process, the sensing data is collected and processed. The resulting sensing data processing (step 6) produces the sensing information required for the service. The network then sends back a sensing response (step 7) to the SF, and the processed results are subsequently exposed to the UE (step 8).

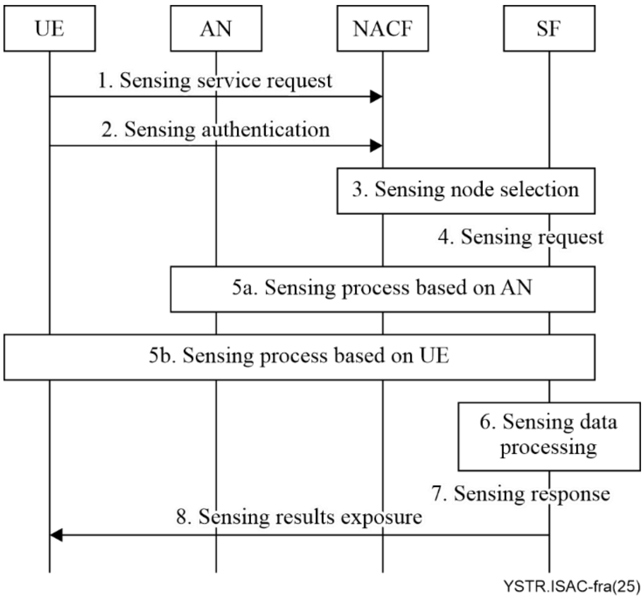

Figure 9-2 – The sensing process triggered by user equipment (UE)

Bibliography

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*