

NMRG  
Internet-Draft  
Intended status: Experimental  
Expires: 3 September 2026

CJ. Bernardos  
UC3M  
A. Mourad  
InterDigital  
M. A. Jadoon  
InterDigital Europe Ltd  
2 March 2026

Solutions for enabling agentic sensing with network optimization  
draft-bernardos-nmrg-agentic-network-optimization-00

## Abstract

Integrated Sensing and Communications (ISAC) represents a paradigm shift in wireless networks, where sensing and communication functions are jointly designed and optimized. By leveraging the same spectral and hardware resources, ISAC enables advanced capabilities such as environment perception, object tracking, and situational awareness, while maintaining efficient and reliable data transmission. There are sensing scenarios and use cases that involve a distributed sensing task, in which multiple sensors participate and contribute with (raw or pre-processed) sensing data, which is processed by a sensing service (e.g., fusing sensing measurements from the different sensors). This sensing service needs to be executed on some kind of sensing processing/computing function which receives raw (or preprocessed) data from multiple sources, potentially of different (heterogeneous) kinds (e.g., RF and non-RF sensing, or RF from different radio technologies). This processing might impose time synchronization constraints on the reception of the different parts of data, as well as potentially specific computing and/or AI/ML capabilities on the processing node.

The joint selection of sensing entities, processing locations, and network configuration under time-varying conditions results in a large, coupled, and non-stationary decision space. These characteristics motivate the use of agentic AI to enable distributed, closed-loop configuration and reconfiguration of sensing and networking resources.

This document presents initial considerations and potential solution directions for an architecture that enables the use of agentic AI for sensing (as an exemplary use case) supporting network optimization.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 3 September 2026.

#### Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

#### Table of Contents

1. Introduction . . . . .	2
2. Terminology . . . . .	4
3. Enabling agentic AI distributed sensing with network optimization . . . . .	5
4. IANA Considerations . . . . .	13
5. Security Considerations . . . . .	13
6. Acknowledgments . . . . .	13
7. Informative References . . . . .	13
Authors' Addresses . . . . .	14

#### 1. Introduction

Integrated Sensing and Communications (ISAC) is emerging as a key enabler for next-generation wireless networks, integrating sensing and communication functionalities within a unified system. By leveraging the same spectral, hardware, and computational resources, ISAC enhances network efficiency while enabling new capabilities such as high-resolution environment perception, object detection, and situational awareness. This paradigm shift is particularly relevant for applications requiring both reliable connectivity and precise sensing, such as autonomous vehicles, industrial automation, and smart city deployments. Given its strategic importance, ISAC has gained significant traction in standardization efforts. The ETSI

Industry Specification Group (ISG) on ISAC has been established to explore technical requirements and use cases, while 3GPP has initiated discussions on ISAC-related features within its ongoing research on future 6G systems. Furthermore, research initiatives within the IEEE and IETF are investigating how ISAC can be integrated into network architectures [I-D.ietf-green-use-cases], spectrum management, and protocol design, making it a critical area of development in the evolution of wireless networks.

There are sensing scenarios and use cases that involve a distributed sensing task, in which multiple sensors participate and contribute with (raw or pre-processed) sensing data, which is processed by a sensing service (e.g., fusing sensing measurements from the different sensors). This sensing service needs to be executed on some kind of sensing processing/computing function which receives raw (or preprocessed) data from multiple sources, potentially of different (heterogeneous) kinds (e.g., RF and non-RF sensing, or RF from different radio technologies). This processing might impose time synchronization constraints on the reception of the different parts of data, as well as potentially specific computing and/or AI/ML capabilities on the processing node.

The selection of the nodes that participate as sensors and sensing processing functions in a given distributed sensing task and the configuration of the network to facilitate the sensing task, and optimize both the sensing and the network operation, are not independent. However, achieving an overall optimal configuration is not a trivial task, especially when multiple optimization metrics and/or constraints are considered.

In distributed sensing, sensing KPIs (e.g., accuracy, refresh rate, confidence level, latency) are tightly coupled with radio, compute, and transport configurations. Moreover, mobility, traffic load, and environmental dynamics continuously alter the relationship between configuration and achieved sensing performance. Static or centrally pre-computed deterministic configurations can therefore become suboptimal or infeasible at run time. An agentic AI approach enables distributed decision-making, coordination among sensing and networking entities, and adaptive reconfiguration to sustain sensing KPIs under dynamic conditions

We assume a generic network architecture, where IETF CATS and GREEN architectural considerations and solutions can be of application, though the solution can be generalized to scenarios based on different architectures.

We assume that there is a network function in charge of the coordination and configuration of the distributed sensing task, aware of which nodes in the network can participate as sensor nodes, and potentially of the capabilities of potential sensing processing nodes. This network function can be, for example, the Gateway Sensing Function (GSF)/ the Sensing Control Function (SCF) as introduced by 3GPP.

We also assume that there is a network function in charge of managing the network configuration of the network, such as an SMF/AMF in a 3GPP 5G architecture.

We assume that there are AI agents, which might run on network nodes (such as terminals, radio access nodes or infrastructure nodes), of two types: AI agents for Sensing (AIaS) and AI agents for Network (AIaN). These agents can run tasks aimed at finding an optimal configuration for sensing and connectivity, respectively and can interact among them to pursue these goals.

A given network function or application function might request a specific sensing task (with associated requirements, e.g., in terms of accuracy) to the SCF directly or indirectly via the NEF and/or GSF, which can then request several AI agents for Sensing to select a sensing configuration and interact with the AI network agents to ensure the network is configured as needed. Note that the sensing task request might have some associated requirements, specific to the task (such as accuracy, or privacy) but also global ones, such as energy consumption, etc.

## 2. Terminology

The following terms are used in this document:

AIaS: AI agent for Sensing.

ISAC: Integrated Sensing and Communications.

SCF: Sensing Control Function, responsible of configuring and triggering distributed sensing performed by a group of sensors.

SF: Sensing Function, participates in a distributed sensing function as a sensor.

SPF: Sensing Processing Function, participates in a distributed sensing function processing raw (or pre-processed) sensing data.

### 3. Enabling agentic AI distributed sensing with network optimization

We describe next an example of operation and signaling for a distributed sensing task to be configured and dynamically optimized based on agentic AI for sensing and networking. An AI agent for Sensing and an AI agent for Networking run on several network nodes (terminals, access nodes and processing nodes) and might interact to agree on a sensing and networking configuration that overall meets the sensing requirements while optimizing other metrics (such as privacy and energy consumption).

/\_\ AI agent for Sensing

|\_ | AI agent for Networking

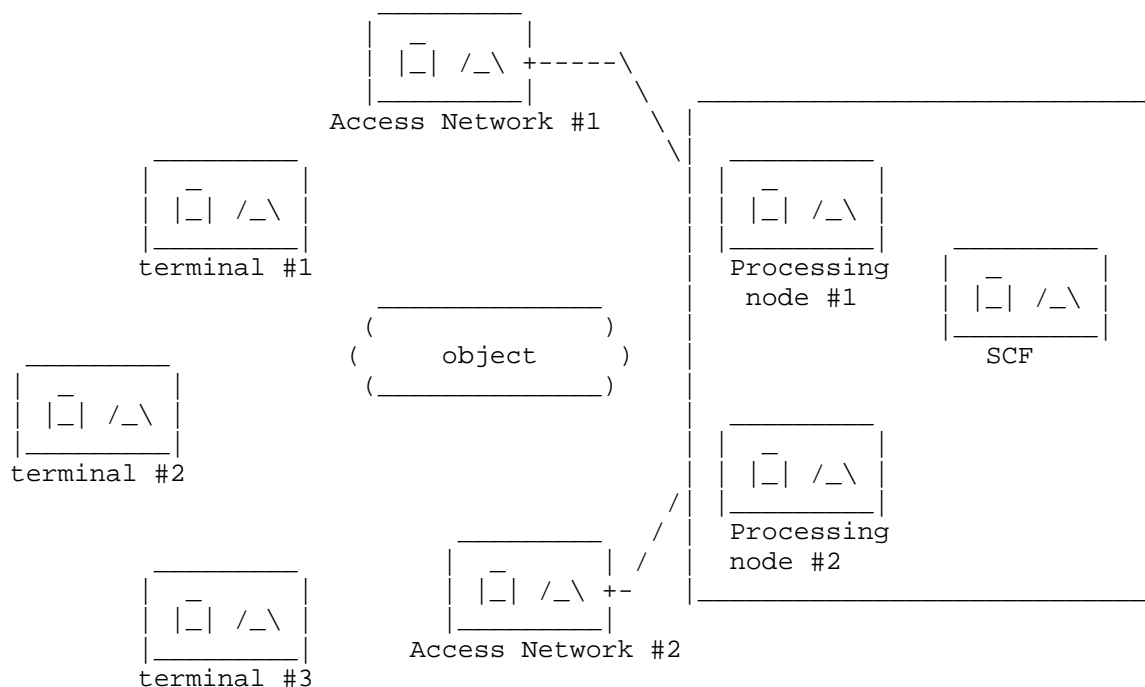


Figure 1: Exemplary scenario and architecture

Figure 1 shows a high-level picture of the architecture.

In the following, we describe an exemplary procedure showing how different agents can interact to configure a distributed sensing task. The focus is on the interactions, the information exchanged and what actions might be triggered.

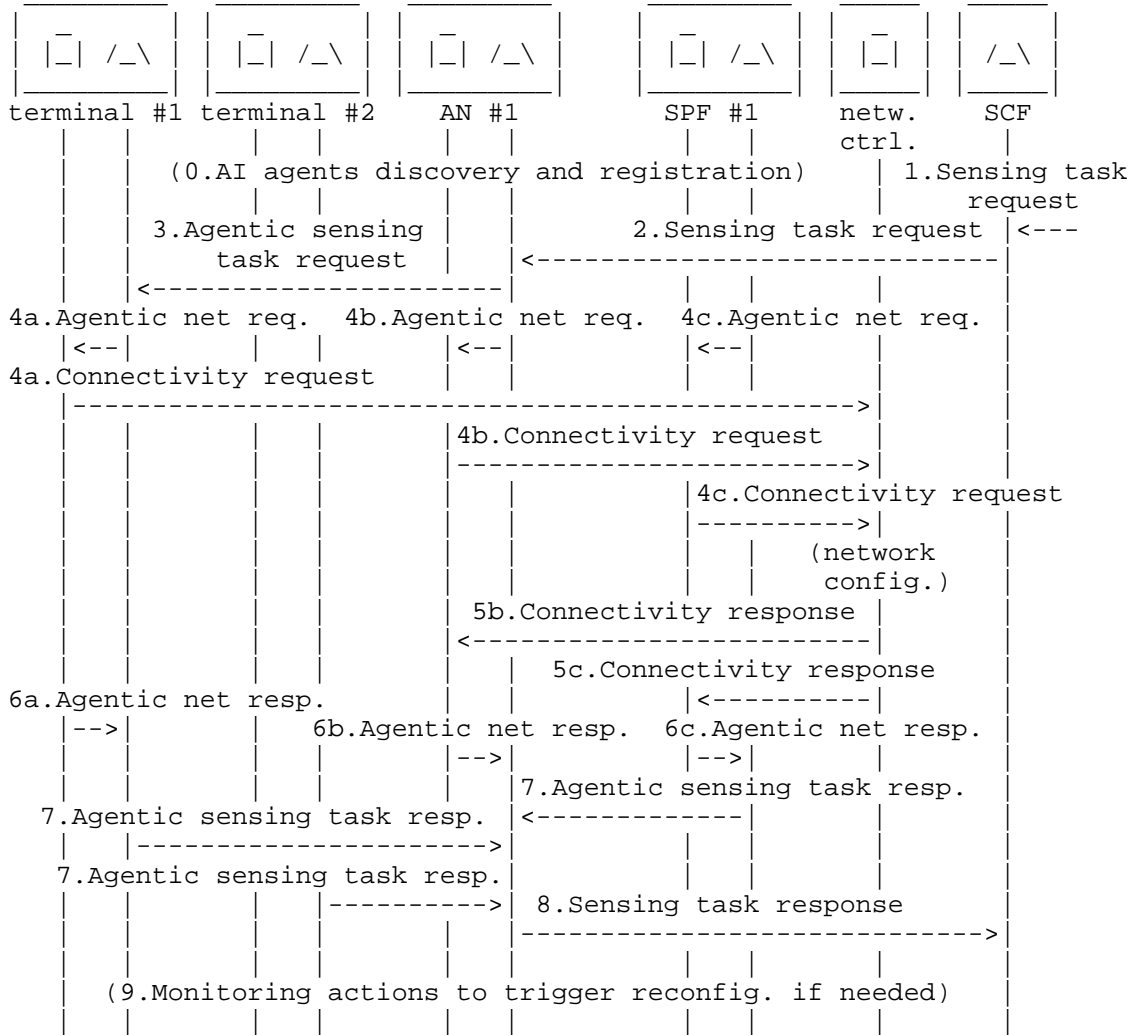


Figure 2: Exemplary signaling of agentic AI interactions for optimized distributed sensing

Figure 2 shows the message sequence chart of an agentic AI-enabled multi-sensor distributed sensing which is explained next:

0. We assume AI agents for Sensing have been trained with some data, possibly based on their own local knowledge and potentially enriched with additional data. We also assume they have some knowledge about other neighboring agents and that there could be some type of centralized/distributed repository where they are registered.
1. The network receives a sensing request. A sensing managing entity, such as the SCF, receives this request and decides to delegate that request, or part of that request to some AI agents for Sensing running in the network. For example, the initial request received by the network may be for a XR/multi-media service (which explicitly or implicitly require sensing services), while the sensing request that is delegated to AI Agents may be created to meet the sensing requirements of the initial request. SCF would decide which specific sensing request should be processed via AI agents and which part of the sensing could be done using sensing "traditional" (i.e., not using agentic AI) methods.
2. Based on the information and metadata associated to the sensing request (e.g., location of the intended sensing), the SCF determines to use AI Agents for executing the sensing task, and sends a request to the AI agent for Sensing at the chosen sensing entity (Access Node #1 [AN#1], in our example). In this step the SCF may determine to use AI Agents based on any combination of:
  - a. an indication received in the initial request that AI Agents can/must be used.
  - b. Received policy information, indicates that AI Agents can/must be used.
  - c. Fast reactions to changes in contextual information and availability of resources is required.
  - d. The overall service requirements allow for delays and errors incurred due to potential conflicts among agents and performance oscillations. These may be specified as threshold values.

This request might include the following information:

- a. Sensing task description: metadata indicating what is the sensing task, sensing accuracy (spatial and temporal), whether the sensing task involves stationary or mobile targets, Time information associated with the sensing task (e.g., a time period), etc.
- b. Sensing data governance requirements about privacy, security and trustworthiness such as for example what sensing data can be processed where in the system and what pre-processing and processing might be allowed to happen with the data, its fusion framework with other data and its exposure to application function or network function. Examples (non-limiting) of encoding of this are:
  - i. Processing of raw sensing data: only local at the originating node / local or remote processing allowed / partial processing allowed remotely.
  - ii. Trustworthiness of data: any generated data is trusted / only data from a list of explicit sources is trusted / data has to be signed by a trusted source to be trusted.
  - iii. Confidentiality of exchanged data: all data (processed or not) must be encrypted (specifying the mechanism to be used to encrypt it), data (raw/partially processed/processed) must be encrypted, all data can be sent in clear.
  - iv. List of trusted generating entities/administrative domains.

Allowed types of sensing fusion, e.g., a combination of the following possible options: only with raw data of some kind, mixing data partially processed with raw data, mixing different types of sensing technologies, mixing different levels of trustworthiness, etc. If the nodes involved in the sensing task belong to different administrative domains, additional mechanisms might need to be used to guarantee/prove that the processing and/or confidentiality of the sensing data is enforced. An example would be the use of a private or public blockchain.

- c. Allowed level of agentic AI interactions. This parameter, which might be expressed in different ways, indicates how different agents are allowed to interact towards completion of the intended task. For example, the requester may indicate that the agent receiving the request has to perform



the required actions without interacting with other sensing agents, or without interacting with networking agents, or which limitations to apply in regards of other agentic interactions (e.g., agent ownership limitations). It also includes whether the involved agents are responsible for monitoring the sensing task to trigger alerts and propose reconfiguration actions if needed. This parameter may also indicate the maximum size of the agent-to-agent communication hops, or tiers or number of worker Agents used for executing part of a task or in whole. This may be seen as the maximum size or depth of the agent-to-agent network (graph). When this parameter is sent from one agent to another agent (as in step 3.d), it may adjust the value to be the (maximum size) relative to that specific agent node/hop (for example, `allowed_level_of_agentic_AI_interactions = allowed_level_of_agentic_AI_interactions - 1`).

- d. Additional network requirements, such as energy consumption metrics.
  - e. List of AI agents available (optional, as this might be known by the receiving AI agent based on its local context and/or other AI agent discovery mechanisms).
3. The receiving AI agent for Sensing (in this example `AIaS@AN#1`) processes the request and based on the parameters received and its knowledge of the local context and prior training, decides whether it can honor the received request and whether it can interact with other agents. In this example, the agent decides to interact with three additional AI agents for sensing (`@terminal#1` and `@terminal#2`, `@processing node/SPF #1`) to basically configure a multistatic active sensing (involving terminals #1 and #2 and `AN#1`) with the sensing processing done at processing node/SPF #1. `AIaS@AN#1` sends an Agentic sensing task request, which includes the following parameters:
- a. Sensing task description: metadata indicating what is the intended sensing task, sensing accuracy (spatial and temporal), whether the sensing task involves stationary or mobile targets, etc.
  - b. Intended sensing task configuration, including parameters such as:
    - i. Static/Multi-static.
    - ii. Active/passive sensing.

- iii. Sensing technology (e.g., WiFi, 5G).
  - iv. Other participant node's IDs.
- c. Sensing data governance requirements about privacy, security and trustworthiness such as for example what sensing data can be processed where in the system and what pre-processing and processing might be allowed to happen with the data, its fusion framework with other data and its exposure to application function or network function. Examples (non-limiting) of encoding of this are:
- i. Processing of raw sensing data: only local at the originating node / local or remote processing allowed / partial processing allowed remotely.
  - ii. Trustworthiness of data: any generated data is trusted / only data from a list of explicit sources is trusted / data has to be signed by a trusted source to be trusted.
  - iii. Confidentiality of exchanged data: all data (processed or not) must be encrypted (specifying the mechanism to be used to encrypt it), data (raw/partially processed/processed) must be encrypted, all data can be sent in clear.
  - iv. List of trusted generating entities/administrative domains.
- Allowed types of sensing fusion, e.g., a combination of the following possible options (non limiting): only with raw data of some kind, mixing data partially processed with raw data, mixing different types of sensing technologies, mixing different levels of trustworthiness, etc. If the nodes involved in the sensing task belong to different administrative domains, additional mechanisms might need to be used to guarantee/prove that the processing and/or confidentiality of the sensing data is enforced. An example would be the use of a private or public blockchain.
- d. Allowed level of agentic AI interactions. This parameter, which might be expressed in different ways, indicates how different agents are allowed to interact towards completion of the intended task. For example, the requester may indicate that the agent receiving the request has to perform the required actions without interacting with other sensing agents, or without interacting with networking agents, or

which limitations to apply in regards of other agentic interactions (e.g., agent ownership limitations). It also includes whether the involved agents are responsible for monitoring the sensing task to trigger alerts and propose reconfiguration actions if needed. An example of a possible encoding of the allowed level of agentinf AI interaction is the following:

0. no delegation,
  1. local AIaS may interact with local AIaN,
  2. local AIaS may delegate/talk to other sensing nodes, but those cannot delegate it further,
  3. local AIaS may delegate/talk to other sensing nodes, which can delegate it to N-2 levels.
- e. Additional network requirements, such as energy consumption metrics.

How an agent decides that additional sensing tasks need to be performed in order to honor/complete the received sensing task is out of the scope of this document. It is up to the specific agents' implementation and the knowledge they have of the local context.

4. The receiving agents process the request, and similarly to what was done in the previous step, decide whether they need to do additional agent interactions (this can only happen if the received "allowed level of agentic AI interactions" is  $> 1$ , on each level the "allowed level of agentic AI interactions" is decreased by 1). (Non-limiting) examples of these sub-tasks are:
  - \* Perform an isolated sensing task targeting a specific goal (i.e., track an object in a given geographic area, with an intended accuracy, sensing technology and energy constraints).
  - \* Configure the network and/or specific network elements to support a given connectivity level to transport the data generated by another agents.
  - \* Find out which types of sensing, and with which level of trustworthiness/security/privacy are allowed to be used by certain nodes and/or in a given geographic area.
  - \* Etc.

Let's assume for the sake of this example, that the following actions are required:

- i.     AIaS@terminal#1 needs to interact with its local AI agent for Networking (AIaN@terminal#1) to ensure that the radio interface of terminal#1 is configured as required by the sensing task.
- ii.    AIaS@AN#1 needs to interact with its local AI agent for Networking@AN#1 to request a guaranteed communication path to the processing node#1. As a result of this, AIaN@AN#1 sends the required request to the networking control entity (in this example SMF/AMF), which then performs the required configuration.
- iii.   AIaS@processing-node#1 needs to interact with its local AI agent for Networking@processing-node#1 to request a guaranteed communication path to AN#1 and terminals #1 and #2. As a result of this, AIaN@processing-node#1 sends the required request to the networking control entity (in this example SMF/AMF), which then performs the required configuration.

Note that it might also be possible that the request for guaranteed communication paths (e.g., between the processing node #1 and terminals #1 and #2, could also be triggered by AI agents running on the terminals.

5.     As a result of the requests (4b and 4c) for guaranteed communication paths to the AMF/SMF, the AMF/SMF performs the required configurations and responds back to the AI agents for networking (5b and 5c).
6.     The AI agents for networking respond back to the AI agents for sensing, after completing their tasks.
7.     Each involved AI agent that was tasked a given action responds back to the initiating AI agent. In this example, AIaS@terminal#1, AIaS@terminal#2 and AIaS@processing-node#1 responds to AIaS@AN#1, including the result of the operation.

8. Once all the required configurations are completed, the initial agent (AIA@AN#1) responds back to the SCF with a sensing task response, providing the result of the sensing task request (success/failure) and about the resulting sensing (and networking) configuration. At this point, the distributed sensing task is ongoing. This may also include information of the established Agent Network, e.g., a graph of agents and their capabilities.
9. SENSING and CONNECTIVITY MONITORING. Depending on whether the agents were instructed to perform continuous monitoring or not, different options are possible:
  - a. Monitoring performed by the agents. In this case, agents monitor the activity and local context for variations that, according to its previous training and knowledge, might require corrections. If that is the case, the conducted actions are notified back to the SCF, through the chain of involved agents. Examples of monitoring include: (i) Measuring (passively or actively) connectivity between sensing sources and processing node, (ii) Measuring estimated sensing precision, (iii) Measuring energy consumption associated with the sensing task. The monitoring can include additional parameters, such as: (i) specific thresholds for each/some monitored parameters and associated actions if those threshold are passed, (ii) Frequency of monitoring.
  - b. Monitoring performed by the network. In this case, "legacy" monitoring mechanisms are used, which might trigger reconfiguration actions (in a similar fashion to the initial sensing task request).

#### 4. IANA Considerations

N/A.

#### 5. Security Considerations

TBD.

#### 6. Acknowledgments

The work of Carlos J. Bernardos in this document has been partially supported by the Horizon Europe MultiX (Grant Agreement No. 101192521) and DISCO6G-CM.

#### 7. Informative References

[I-D.ietf-green-use-cases]

Stephan, E., Palmero, M. P., Claise, B., Wu, Q.,  
Contreras, L. M., Bernardos, C. J., and X. Chen, "Use  
Cases for Energy Efficiency Management", Work in Progress,  
Internet-Draft, draft-ietf-green-use-cases-01, 22 January  
2026, <<https://datatracker.ietf.org/doc/html/draft-ietf-green-use-cases-01>>.

#### Authors' Addresses

Carlos J. Bernardos  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
28911 Leganes, Madrid  
Spain  
Phone: +34 91624 6236  
Email: [cjbc@it.uc3m.es](mailto:cjbc@it.uc3m.es)  
URI: <http://www.it.uc3m.es/cjbc/>

Alain Mourad  
InterDigital Europe Ltd  
London  
United Kingdom  
Email: [Alain.Mourad@InterDigital.com](mailto:Alain.Mourad@InterDigital.com)  
URI: <http://www.InterDigital.com/>

Muhammad Awais Jadoon  
InterDigital Europe Ltd  
London  
United Kingdom  
Email: [muhammad.awaisjadoon@interdigital.com](mailto:muhammad.awaisjadoon@interdigital.com)