NANCY

An Artificial Intelligent Aided Unified Network for Secure Beyond 5G Long Term Evolution [GA: 101096456]

Deliverable 4.3

Trustworthy Grant/Cell-free Cooperative Access Mechanisms

Programme: HORIZON-JU-SNS-2022-STREAM-A-01-06

Start Date: 01 January 2023

Duration: 36 Months

Co-funded by the European Union

6GSNS

NANCY project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101096456.

Document Control Page

Deliverable Name	Trustworthy Grant/Cell-free Cooperative Access Mechanisms
Deliverable Number	D4.3
Work Package	Work Package 4
Associated Task	T4.3 Trustworthy Grant/Cell-free Cooperative Access Mechanisms
Dissemination Level	Public
Due Date	31 January 2025 (M25)
Completion Date	23 January 2025
Submission Date	30 January 2025
Deliverable Lead Partner	UMU
Deliverable Author(s)	Ramon Sanchez-Iborra (UMU), Rodrigo Asensio-Garriga (UMU), Gonzalo Alarcón Hellín (UMU), Shih-Kai Chou (IJS), Blaz Bertalanic (IJS), Alvise Rigo (VOS), Anna Panagopoulou (VOS), Vamvourellis Stratos (8BELLS), Theodoropoulos Ilias (8BELLS), Jorge Sasiain (EHU)
Version	1.0

Document History

Version	Date	Change History	Author(s)	Organisation
0.1	27/02/2024	Initial version, Section 1	Ramon Sanchez	UMU
0.2	07/10/2024	Section 3.1	Gonzalo Alarcón Ramon Sanchez	UMU
0.3	20/10/2024	Section 2	Gonzalo Alarcón Carolina Fortuna Shih-Kai Chou Blaz Bertalanic Alvise Rigo Panagopoulou Anna	UMU, IJS, VoS
0.4	12/11/2024	Section 3.2	Gonzalo Alarcón Rodrigo Asensio Ramon Sanchez	UMU

0.5	27/11/2024	Section 3.5	Alvise Rigo Panagopoulou Anna	VoS
0.6	04/12/2024	Section 3.4	Vamvourellis Stratos Theodoropoulos Ilias	8BELLS
0.7	11/12/2024	Section 4.1.1	Rodrigo Asensio	UMU
0.8	17/12/2024	Section 4.2.1	Jorge Sasiain	EHU
0.9	7/1/2025	Section 3.6, Section 5	Rodrigo Asensio Ramón Sánchez Gonzalo Alarcón	UMU
1.0	14/01/2025	Address internal reviews and close the document	Rodrigo Asensio Ramón Sánchez Gonzalo Alarcón	UMU

Internal Review History

Name	Organisation	Date
Konstantinos Kyranou	SIDROCO	08 January 2025
Stylianos Trevlakis	INNO	13 January 2025

Quality Manager Revision

Name	Organisation	Date
Anna Triantafyllou, Dimitrios Pliatsios	UOWM	20 January 2025

Legal Notice

The information in this document is subject to change without notice.

The Members of the NANCY Consortium make no warranty of any kind about this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

The Members of the NANCY Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental, or consequential damages in connection with the furnishing, performance, or use of this material.

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SNS JU. Neither the European Union nor the SNS JU can be held responsible for them.

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Explanation
5G	Fifth Generation of Wireless Cellular Technology
APs	Access Points
ARM	Advanced RISC Machine
B5G	Beyond 5G
B-RAN	Blockchain Radio Access Network
CPU	Central Processing Unit
D2D	Device-to-Device
DDRL	Double Deep Reinforcement Learning
DID	Decentralized Digital Identity
DoS	Denial of Service
DRL	Deep Reinforcement Learning
EPC	Evolved Packet Core
gNB	Next Generation Node B
IoT	Internet of Things
LSTM	Long Short-Term Memory
LTE	Long Term Evolution
MADM	Multi-Attribute Decision Making
MRAT-NCP	Multi Radio Access Technology Nomadic Connectivity Provider
NR	New Radio
OBU	On-Board Unit
OPTEE	Open Portable Trusted Execution Environment
OS	Operating System
ProSe	Proximity Service
QoS	Quality of Service
RAN	Radio Access Network
RATs	Radio Access Technologies
RMSE	Root Mean Square Error
RNN	Recurrent Neural Network
RNs	Relay Nodes
RPC	Remote Procedure Call
RSUs	Roadside Units
SMC	Secure Monitor Call
SoTA	State of the Art
SPM	Smart Pricing Module
TCP	Transmission Control Protocol
TEEs	Trusted Execution Environments
TFS	Throughput Forecast Service
TZASC	TrustZone Address Space Controller
TZMA	TrustZone Memory Adapter
TZPC	TrustZone Protection Controller

UAV	Unmanned Aerial Vehicle
UDP	User Data Protocol
UE	User Equipment
V2X	Vehicle-to-Everything
VOSyS	Virtual Open Systems

1. Introduction

The pursuit of increased data rates, enhanced reliability, and improved user experiences has propelled the development of novel technologies in the quickly changing field of wireless communication. Of these, cell-free cooperative access mechanisms have become a prominent paradigm that holds the potential to fundamentally alter our current procedures for resource allocation and network management. Cell-free networks, in contrast to conventional cellular architectures, make use of a more flexible connectivity scheme which enables users to gain connectivity through a series of means. Thus, the shortcomings of conventional cellular architectures become more noticeable as we approach the 6G era. Conventional networks have problems with inflexible cell boundaries, interference, and unequal resource distribution that call for a paradigm change.

Cell-free networks are an alternative to the traditional cell-based methodology. Under this paradigm, a great number of access points (APs) are dispersed throughout the coverage area in a cell-free system, cooperating to serve every user. By eliminating the idea of cell boundaries, this cooperative approach makes resource utilization more adaptable and effective. Users are served dynamically by the best APs based on current conditions, rather than being locked into a particular cell or base station. This leads to improved user experiences and more consistent Quality of Service (QoS), especially in highly mobile and densely populated areas.

Adopting cooperative access mechanisms without cells brings many potential advantages:

i. Improved coverage and capacity: Cell-free networks, especially in difficult environments, can offer more consistent coverage and higher capacity by doing away with cell boundaries and utilizing distributed cooperation.

ii. Enhanced reliability and resilience: Cell-free networks are more resilient to failures and disruptions because of their distributed architecture. In the event that one AP fails, the others can easily take over and maintain service continuity.

iii. Reduced latency: By minimizing the need for handovers and optimizing resource allocation in real-time, the cooperative approach of cell-free networks can reduce latency, especially when coupled with task offloading and user-centric data caching mechanisms.

Besides, given the trustworthiness and reliability enabled by Blockchain-RAN (B-RAN) the exploitation of cell-free networks has been identified as of great interest by the research community.

1.1 Purpose of the Document

Considering the opportunities identified according to the previous exploration, NANCY has addressed the development of trustworthy grant/cell-free cooperative access mechanisms, specifically under the activities conducted in Task 4.3. Different technical approaches have been adopted to achieve the challenges posed by this novel paradigm. Several application scenarios and enabled services have been studied to validate the developments striving to achieve cell-free network realization, which could advance our goal of ubiquitous, seamless, and high-quality connectivity for all. This document presents all these advances and presents a vision of how they will be integrated into different NANCY's testbeds and demonstrators for their validation in the last stage of the project.

1.2 Relation to other Tasks and Deliverables

As mentioned above, this document reports the activities conducted under the umbrella of T4.3 "Trustworthy grant/cell-free cooperative access mechanisms", however, it has evident connections with the work carried out in other tasks and, therefore, reported in other deliverables. Regarding WP4, the data-caching mechanisms discussed in T4.1 "Computational offloading and user-centric caching functionalities" (reported in Deliverable 4.1) are adopted and further developed with the aim of achieving highly secure data-caching functionality. Besides, the SLA model designed for this task is also adopted here to check whether the QoS requirements of users are being fulfilled. Regarding T4.5 "Smart pricing policies", the smart-pricing module developed there is exploited here as it is a key component to enable trustworthy resource selection based on the final price for the users. Considering other WPs, the IA-based decision engines designed and developed in T3.2 "AI-based B-RAN orchestration functionalities & Self-evolving AI Model Repository Functionalities" (reported in Deliverable 3.2) are exploited in this task, concretely in the multi-cell selection process. Besides, the NANCY ID management process designed in T5.2 "Security and privacy blockchain-based mechanisms" (reported in Deliverable 5.2) is implemented in this task and integrated into the overall workflow of the cell-free access mechanism procedures. Finally, the implementation plan and integration points that should be followed to integrate the cell-free access mechanisms in NANCY's testbed and demonstrators were defined in T6.1 "Integration plan and facilities" and T6.2 "Continuous integration", respectively.

1.3 Structure of the Document

The rest of the document is organised as follows:

- **Section 2 - State of the Art** presents the state-of-the-art involving the employed technologies, along with an explanation of the project's developments that allow advancements in these fields.

- **Section 3 – NANCY's Trustworthy Grant/Cell-free Cooperative Access Mechanisms** introduces the cell-free access mechanisms developed in NANCY, together with additional related technologies and procedures.
- **Section 4 – Trustworthy Grant/Cell-free Cooperative Access in NANCY's Demonstrators and Testbeds** documents the way in which these elements are implemented in the different NANCY testbeds and demonstrators.
- **Section 5 – Conclusion and outlook** provides a synopsis of the most important facts and conclusions.

2. State of the Art

2.1 Connectivity Extension in 5G

With the evolution of communication networks towards beyond 5G (B5G), the extension of connectivity in 5G networks has emerged as a critical area of research and development [1]. This field is driven by the need to meet a growing demand for high capacity, which represents significant technical challenges for the current infrastructure. In this context, one of the most innovative technologies is cellular multi-hop communications, which allows the transmission of data through multiple mobile UEs before reaching its destination, namely, another UE or a gNB (next generation NodeB) in order to continue their path through the fixed infrastructure. This technique is particularly useful in environments where the cellular coverage provided by gNB is limited; thus, it facilitates the connection of remote devices thanks to the help of intermediate neighbors, which significantly improves network reliability, as well as its range and continuity [2].

The operation of multi-hop communications is achieved through the deployment of support APs (Access Points), known as relay nodes (RNs), materialising one of the types of cell-free access mechanisms considered in NANCY. These techniques extend the network range and avoid reliance on traditional cells, improving cellular systems' coverage, capacity, and spectral efficiency. In addition, these innovations optimize the use of radio frequency (RF) spectrum, a limited and congested resource, which becomes crucial in networks with high data traffic [3]. At the same time, proximity services (ProSe) have emerged as an innovative feature within this landscape, as they enable direct communication between nearby devices without the need for a network operator's infrastructure [4]. This capability is especially beneficial in situations where network connectivity may be weak or unavailable, allowing users to engage in real-time interactions among themselves in a device-to-device (D2D) fashion. Integrating ProSe with multi-hop communications improves overall network performance by leveraging local device interactions, reducing latency and increasing throughput [5].

Several studies have shown that the use of cell-free access combined with multi-hop communications and proximity services, not only improves coverage and capacity but also increases the quality of service (QoS), offering high throughput rates and reducing transmission latencies, which are critical for emerging applications such as the Internet of Things (IoT), augmented reality (AR) and real-time critical communications [6]. Consequently, the field of multi-hop communications has captured the attention of many researchers, motivating the creation of new network architectures and solutions aimed at optimizing the network performance in terms of throughput, reliability, energy efficiency, and self-management capabilities of these networks.

In addition, a virtual mesh networking framework can be implemented to support multi-hop D2D communications in 5G networks [7]. The proposed framework divides routing and packet forwarding into two separate mechanisms; one in the control plane and the other in the user plane. The gNB collects information from the topology, forming a virtual mesh network and determining the optimal routes for end-to-end (E2E) communication. This approach also introduces a routing algorithm designed to select routes combining cellular and D2D links, considering terminal mobility and possible link failure. On this basis, the authors of [8] presented an architecture that facilitates multi-hop communications in long-term evolution (LTE) and 5G networks, by introducing two key nodes: The RN and the Proxy eNB (P-eNB). The RN connects to the eNB/gNB and acts as an intermediary for the user equipment (UE), automatically forming a multi-hop network, while the P-eNB manages multiple RNs. The proposed design improves network coverage, capacity and flexibility, enabling the use of integrated access and backhaul technologies in both LTE and 5G. In addition, the RNs are plug-and-play devices, facilitating fast and flexible deployment in low-coverage areas or in emergency situations.

On the other hand, an alternative solution presented an architecture composed of two interconnected LTE/EPC (long-term evolution/evolved packet core) networks [9]. In this configuration, the transport operator network (Track EPC) manages the mobile relay nodes (eNBm), while the standard LTE network manages the UEs. This study showed that the use of eNBms significantly improves signal quality in situations where connectivity is limited. One of the main advantages is that by performing a single handover for the mobile relay (instead of one for each device), signaling overhead in the network is reduced and resource management is optimized.

Besides the architectures presented before, solutions combining long-range technologies (Uu interface) with D2D technologies (PC5) in multi-hop communications have also been proposed [10]. This solution uses roadside units (RSUs) located along train tracks that communicate with gNBs via the Uu interface, and with trains and other RSUs via the PC5 interface. In this context, joint optimization for resource management and routing topology is also introduced, tailored both to maximize throughput in data-intensive applications and to minimize delay in critical applications with strict latency requirements.

Beyond State-of-the-Art

The scenario introduced in NANCY for extending connectivity in 5G networks is based on:

i. extending coverage through multi-hop communications;
ii. the use of the PC5 link between UEs to establish D2D communications;

iii. the integration of a new type of node in the network, the so-called Multi Radio Access Technology Nomadic Connectivity Provider (MRAT-NCP), distributed over the field to extend the coverage provided by the cellular infrastructure; and

iv. the use of blockchain to improve security and reliability.

All these concepts are represented in Figure 1.

Conventional mobile networks face cost and scalability challenges, particularly in rural or complex urban areas where fixed infrastructure is difficult to deploy due to both technical and economic reasons. NANCY introduces an innovative solution based on multi-hop communications, leveraging the PC5 interface, which allows D2D communication without routing through a gNB. This approach enables UEs that are out of the gNB's range to communicate by relaying their data through other nearby UEs, creating a multi-hop communication chain. This method not only extends coverage beyond the reach of conventional infrastructure but also optimizes spectrum usage, mitigates network congestion and enhances network resilience in challenging environments. This service may be grant-free for the UE if the operator and the coverage-extending node reach an agreement. As can be seen in Figure 1, a key element of the NANCY architecture is the use of MRAT-NCPs distributed throughout the service area, which facilitates multi-hop communications aiming at providing connectivity to out-of-range devices. Thus, these nodes function as a bridge between remote UEs and the fixed infrastructure, not only extending coverage but also improving network capacity and network efficiency, which is particularly useful in situations where a direct connection to the gNB is not feasible. In addition, these nodes allow traffic to be efficiently redistributed, avoiding congestion and ensuring optimal resource utilization, especially when technologies such as task offloading and data caching are also considered. The MRAT-NCP will receive compensation for providing this service, which could be covered by the UE or by the operator, in this last case, it would be a grant-free service for the user.

With NANCY, interoperability between different operators is achieved, enabling seamless and uninterrupted connectivity for UEs. This collaboration allows UEs to move between different MRAT-NCPs without losing connectivity, offering a seamless handover experience when users switch from one node to another. To achieve this, the system integrates an intelligent pricing and control mechanism that dynamically allocates network capacity and adjusts costs based on demand and resource availability. This ensures that UEs can efficiently access network services independently of their original operator, promoting a collaborative and open-ecosystem between providers. As a result, UEs can seamlessly connect to other operators' networks, maintaining seamless connectivity across different service areas, and significantly improving both user experience and network resource management.

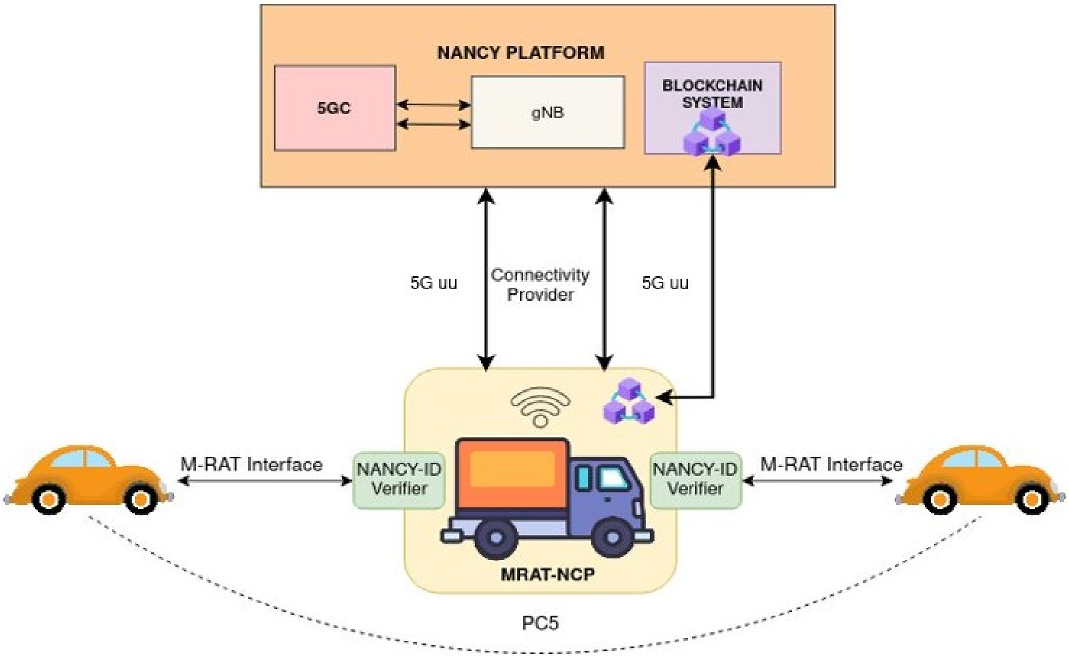

Figure 1. Multi-hop coverage extension in NANCY

At the same time, to address security and trust concerns, NANCY integrates blockchain technology along with authentication and authorization mechanisms, guaranteeing data integrity and ensuring that only authenticated UEs can participate in the network, minimizing the risk of malicious interference. As a result, NANCY provides a robust system for identity management and data protection throughout the multi-hop relay process.

2.2 MultiRAT Selection

The selection of multi-radio access technology (RAT) is a crucial element in the development of modern communication networks, especially in the context of cell-free configurations in 5G and the Internet of Moving Things (IoMT) [11]. The complexity of these scenarios requires sophisticated methods to optimize RAT selection, each with unique strengths and challenges. Double Deep Reinforcement Learning (DRL) [12] is one of the more widely considered approaches, which aims to improve users' QoS while managing battery consumption and ensuring seamless connectivity in IoT environments. By using multi-parametric optimization, DRL effectively addresses different service requirements and is therefore particularly suitable for MultiRAT selection for dynamic network conditions.

Another promising strategy is multi-agent reinforcement learning [13], which utilizes collaborative decision-making between multiple agents. Recent studies show that these multi-agent systems are superior to traditional methods by achieving higher energy efficiency and lower latency, thus improving the overall performance of the network. In addition, the Multi-Attribute Decision Making (MADM) [12] framework systematically evaluates various network parameters, enabling the selection of the most suitable RAT based on user preferences and service requirements.

Game theory [14] approaches also play an important role as they apply concepts from game theory to establish stable connections between IoT devices and RATs. These models focus on energy efficiency and cost reduction, with evolutionary game theory proving particularly effective for load balancing in heterogeneous networks. Context-aware selection [15] method was an early attempt at MultiRAT selection. To enrich the decision-making process algorithms considered the user's context and preferences, enabling a personalized experience. These frameworks incorporated a real-time data about the user's environment and the device's capabilities and adapt the RAT selection to individual needs.

However, recent works also show that by combining different RATs one can improve resource utilization and connectivity reliability [16]. This framework aims to provide a seamless service across different network types, improving the overall user experience. In addition, dynamic traffic steering techniques are used to customize network selection based on real-time traffic conditions. By using advanced methods, including deep learning algorithms, these techniques can predict traffic patterns and dynamically optimize RAT selection, ensuring efficient resource allocation and improved QoS.

Overall, the landscape of multi-RAT selection is rapidly evolving, driven by advances in artificial intelligence, decision support systems and contextual systems. These innovations aim not only to optimize network performance but also to improve the user experience and resource efficiency across a wide range of applications, contributing to the future of communications technology.

Beyond State-of-the-Art

As explained before, the development of advanced technologies for multiple access technology selection (MultiRAT) has enabled the optimisation of metrics related to QoS and energy efficiency in 5G and B5G networks. However, traditional approaches, such as those based on deep learning or multi-agent decisions, face limitations in highly dynamic environments where network conditions change in real-time. In this context, performance forecasting capabilities integrated in multi-cell connectivity scenarios provides an innovative solution, enabling proactive and efficient resource management in next-generation networks.

In NANCY, the Throughput Forecast Service (TFS) module has been developed and implemented as a novel solution that complements MultiRAT selection techniques with accurate short-term throughput predictions. Using a Long Short-Term Memory (LSTM) model, the TFS predicts the throughput of neighbouring cells, providing a solid basis for dynamic selection of the 5G access node (gNB). The integration of relevant features such as signal strength (RSSI, RSRP, SINR), user position (speed and direction), and network status allows for a detailed and real-time evaluation of the available options. This approach not only optimises connectivity but also enables advanced mechanisms such as predictive handover, improving network resilience and reducing service interruptions. Furthermore, the TFS module is not limited to the selection of individual cells, it also supports a multi-cell connectivity scheme, where UEs can transmit simultaneously over multiple gNBs [please refer to Section 3.3]. This design allows not only to improve system reliability in high mobility scenarios but also to optimise resource allocation across multiple networks. For example, by comparing the throughput predictions generated by the TFS for each adjacent cell, a decision engine determines the optimal combination of cells that fulfils the predefined service level agreements (SLAs), guaranteeing QoS for critical tasks such as low latency or ultra-high reliability.

Through these features, the TFS module establishes a technical framework that not only improves MultiRAT selection in dynamic environments but also places multi-cell connectivity as a key enabler for resilient and adaptive networks for emerging high-demand applications in B5G and beyond.

2.3 Secure Data Handling at the Edge

Research on the design of modern vehicular networks reveals a tendency towards enhancing the confidentiality and trust of end-vehicles at the network edge [17]. Applications in V2X scenarios come with stringent Security, Privacy, Reliability and Integrity requirements which must not be compromised as their collaborative capabilities expand. At the same time, figuring out the means to ensure reliable and efficient V2X communication is challenging, due to the increased vulnerability and the extensive attack surface that V2X systems feature [17], [18]. In these regards, the importance of providing solutions that strengthen users' trust in connected vehicles is paramount. Alongside the design of cryptographic algorithms in software and the incorporation of secure protocols in V2X communications, efforts have been also directed towards the consolidation of hardware components that help boost security within the infrastructure. Trusted computing technologies, assisted by hardware, are at the centre of these innovations [17] because they enable a shift of trust from the back-end infrastructure to the edge, which therefore makes them an ideal fit for the decentralized V2X scenarios. These technologies are built upon a set of mechanisms that introduce trusted enclaves in the infrastructure, where critical code and data can be sealed and protected.

Trusted Execution Environments (TEEs) are a type of hardware-assisted trusted computing technology designed to protect the confidentiality and integrity of run-time code and data from compromised, privileged software [19]. In detail, a TEE provides an isolated environment where it is possible for critical services to execute securely, without the interference of a local, untrusted Operating System (OS) [20], [21]. Among the most usual TEE functionalities are the realization of a Trusted Storage Service, permitting data to be stored safely in the trusted enclave, an Authentication and Cryptographic Functions Service, with the ability to utilize trusted assets for authentication mechanisms and securely store the sensitive cryptographic keys, a Trusted UI Service and others.

In the core implementation of TEEs, there reside primary hardware security features, which are embedded in TEE-enabled devices. In the context of embedded edge devices in V2X, we will give our focus to the ARM TrustZone [20], being an influential hardware technology that acts as an enabler for TEE systems. In a nutshell, the ARM TrustZone is a hardware extension integrated into ARM Cortex devices that allows the creation and execution of TEEs in software. The ARM TrustZone establishes two separate domains denoting the CPU execution state at any given point of time in the system, which are known as the Secure and the Non-Secure worlds. While the secure world can access the information and data residing in both worlds, the non-secure world can only access the data, code, and peripherals of its own domain. On the basis of the ARM TrustZone technology there exist specialized hardware registers designed to be accessed exclusively by highly privileged, software running in the secure world. The most highly privileged software in ARM TrustZone systems is known as the Secure Monitor software, which has absolute control over the system's configurable hardware and resources and monitors the CPU execution states.

The solution is completed with other peripherals, properly adjusted so that they can support it, such as:

- The GIC with v3 extensions, able to associate incurring interrupts to the respective world.
- The TrustZone Address Space Controller (TZASC), able to partition system's DRAM memory between the two worlds.
- The TrustZone Memory Adapter (TZMA), able to partition off-chip ROM or SRAM memory between the two worlds.
- The TrustZone Protection Controller (TZPC), able to partition the devices present in the system between the two worlds.

It is worth noting that the TZASC, the TZMA and the TZPC are optional components of the ARM TrustZone specification and their incorporation into a TrustZone-enabled SoC is implementation-defined [20]. With ARM TrustZone, the TEE is possible to execute in the isolated and protected environment that the Secure world provides. Following the Global Platform established standards for TEEs, as depicted in Figure 2, in the secure world there is deployed a Trusted Kernel and a specific Trusted Application or Service. Because the secure world is totally isolated, access to its services is provided by setting up a minimum communication path between the two worlds.

In the non-secure world side, there should exist a Client API, which serves as a pathway for accessing the features of the Trusted Application within the TEE. Without getting further into details, on the basis of this cross-world communication it can be found the Secure Monitor Call feature, which provides a way to switch the CPU into executing the Secure Monitor software to instrument the overall communication, as well as a basic Non-Secure shared memory area, to actually exchange data between the worlds.

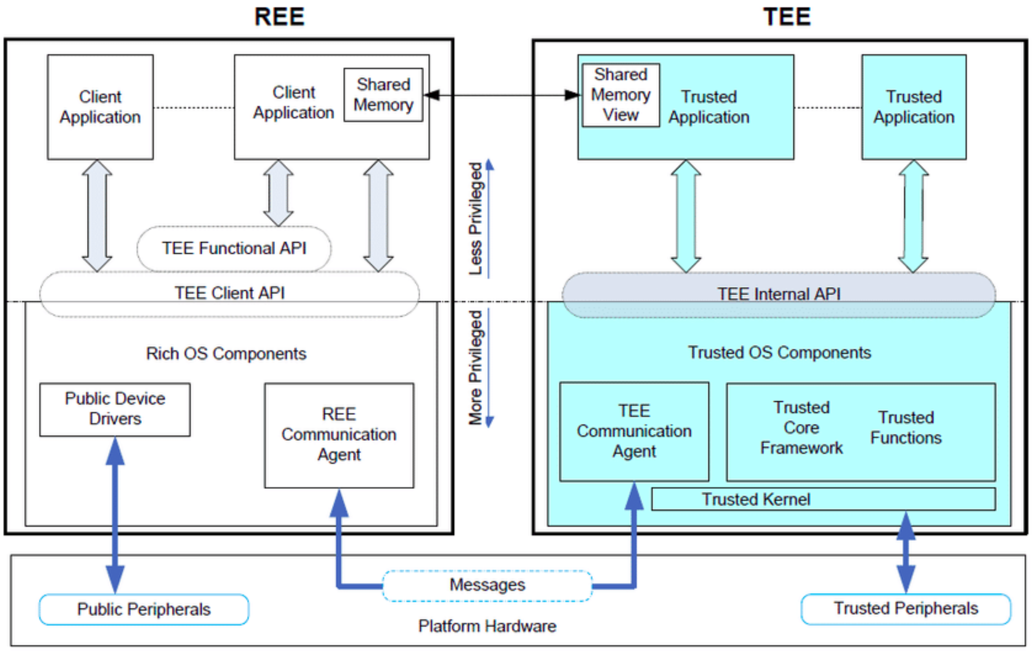

Figure 2. Global Platform specification for TEEs

Returning to the context of V2X, there are few research works that incorporate TEE-enabled services in V2X nodes. Specifically, the work of Jangid and Lin [19] proposes a TEE protected symmetric key-based communication protocol to achieve V2V authentication, utilizing a Daily Symmetric cryptographic service of TEE as well as the TEE sealed storage feature for securing the keys. Also, the work of Mahadevegowda *et al.* [22] provides a secure framework based on ARM TrustZone to defend against replay and Denial of Service (DoS) attacks on devices running a C-V2X application. In particular, the C-V2X application is deployed inside the TEE of a UE that is tampered to the vehicle and undergoes Basic Safety Messages (BSMs) exchange with other vehicles in the network. Focusing more on the trusted storage capabilities of TEEs, the work of Guita *et al.* [23] presents the design of a novel trusted storage service that allows sharing and backing-up data between TEEs found in different devices. Finally, another research activity that closely resonates with NANCY is the work of Giannetsos and Krontiris [17], which proposes the integration of tamper-proof devices, such as TrustZone-based devices in OBUs, to securely produce and store pseudonym credentials. This work introduces the concept of rendering each end-vehicle responsible for the generation of its own pseudonyms, which results in an infrastructure where there is no need for a centralized entity to take up this role.

Beyond State-of-the-Art

In the context of the de-centralized vehicular infrastructure, NANCY aims to achieve enhanced trust towards devices at the network edge. For this reason, NANCY employs tamper-proof devices through which is possible to guarantee data integrity, confidentiality and atomicity in terms of data operations and thus ensure secure data handling in a de-centralized fashion. Following existing approaches, NANCY integrates TEE-based devices in V2X nodes with support for Secure Storage services for sealing critical data and cryptography assets. For this purpose, NANCY focuses on ARM devices with Trustzone hardware support. At the Secure Monitor layer, VOSySmonitor [24] is deployed as the certified, privileged solution that accommodates the safety-critical standards of the industry that are relevant to this layer. Also, for the realization of the TEE Secure Storage service, NANCY employs Open Portable Trusted Execution Environment (OPTEE) [25] - a mature, open-source implementation of TEE that conforms to the GlobalPlatform [26] TEE specifications [27].

In the context of NANCY, we expect the increased security to provide substantial benefits within the decentralized, cell-free access framework. By integrating advanced solutions like VOSySmonitor and OPTEE to create tamper-proof devices, NANCY will achieve enhanced trust towards the network edge - an essential feature of V2X communications. As further detailed in Section 3.5, NANCY will leverage the Trustzone-enabled architecture to implement an innovative user-centric data-caching mechanism, which safeguards sensitive pseudonyms on edge devices, isolating them from normal world interfaces. Eventually, through this approach, the role of these devices as secure, distributed caches will be strengthened, and their reliability will be enhanced in the decentralized infrastructure.

3. NANCY’s Trustworthy Grant/Cell-free Cooperative Access Mechanisms

3.1 Cell-free Access Scenarios in NANCY

Challenging verticals and their novel applications give rise to new requirements that must be handled collaboratively by robust software engineering and operational procedures to effectively manage available resources offered by various stakeholders. This includes the efficient exploitation of radio resources. Regarding this, NANCY has mapped the potential vertical scenarios envisioned for 6G environments [28] into three separate usage scenarios regarding how users gain connectivity towards the network infrastructure: i) Fixed topology fronthaul network; ii) advanced coverage expansion; and iii) advanced mobile node connectivity (Figure 3). Although these scenarios were presented in detail in Deliverable 2.1 “Requirements Analysis”, in the following we also provide a brief description of them, in order to provide the necessary context before continuing with the explanation of the technical designs and developments.

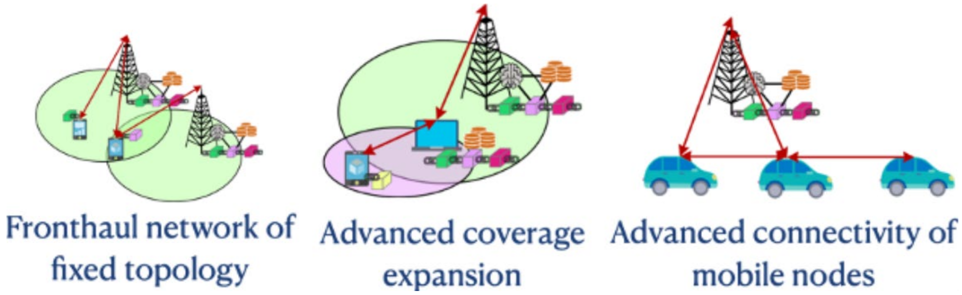
Fronthaul network of fixed topology
Advanced coverage expansion
Advanced connectivity of mobile nodes

Figure 3. NANCY usage scenarios

As a result, NANCY facilitates multi-tenancy and reliable, private, and secure provider collaboration by adopting different strategies. This is accomplished by fusing blockchain, MEC, data-caching, and AI functionalities considering a highly-virtualized set of multi-domain resources. In this line, the development of different trustworthy cell-free access procedures provides answers for the reliable and secure implementation of the three identified usage scenarios mentioned above, considering the radio access segment. The following describes such scenarios and provides a general vision of the role of cell-free access mechanisms in their realization.

3.1.1 Fronthaul Network of Fixed Topology

The first scenario presented in Figure 3 is based on simultaneous multi-cell connectivity, hence, taking advantage of the coverage provided by multiple base stations deployed in a given environment. These points of access towards the B5G infrastructure may belong to the same operator or to different ones. From the UE perspective, a decision engine should select the optimal base station to be connected, based on real-time metrics such as throughput/latency estimation, outage probability, etc., ensuring that users maintain the best possible connection in terms of speed and reliability. This dynamic approach to connectivity is particularly useful in dense urban areas or highly mobile environments, where frequent base station switching is necessary to avoid connection drops or performance degradation. From a cell-free access perspective, this scenario improves reliability and seamless coverage to UEs, with multiple distributed access points providing connectivity in a ubiquitous way. An intelligent agent coordinates UE handovers between base stations, optimising resource allocation and ensuring that UEs remain connected without interruption as they roam the service area. This approach also facilitates network capacity enhancement and congestion reduction, allowing more simultaneous connections throughout the network.

3.1.2 Advanced Coverage Expansion

On the other hand, the second scenario in Figure 3 focuses on extending the coverage provided by a given base station in a multi-hop fashion. In this way, UEs can act as relay nodes (RNs) to extend network coverage in challenging environments. This type of communication allows data to pass from one device to another all the way to the network infrastructure, overcoming the traditional limitations of one-hop direct communications. As explained in detail in the next sections, NANCY bets on the use of the 5G's PC5 link to establish these direct connections between UEs. Furthermore, the incorporation of blockchain technology adds an additional layer of security and trust, ensuring secure identity management and data integrity during the multi-hop communication process. Blockchain-based registries ensure that communications between nodes are authenticated and authorised, preventing interference from malicious actors in the network. Besides, the exploitation of secured data-caching mechanisms is also greatly helpful in expediting this type of operations. Therefore, this combination of PC5, blockchain, and trustworthy data caching not only optimises the security and reliability of the system, but also enables a dynamic expansion of coverage in areas where fixed infrastructure is limited or non-existent.

3.1.3 Advanced Connectivity of Mobile Nodes

Finally, the third scenario in Figure 3 adds an extra layer of complexity as highly mobile UEs (e.g., vehicles) are considered. It can be understood as a combination of the two previous scenarios, particularly applied to the highly challenging vehicular ecosystem. In this scenario, a special vehicle, known as Multi-Radio Access Technology Nomadic Connectivity Providers (MRAT-NCP), acts as a relay node (RN) for the rest of the vehicles, enabling multi-hop data transmission and seamless connectivity for them (usage scenario 2 previously described). Besides, this element in the system is also able to connect simultaneously to different base stations, therefore bringing the first usage scenario to this equation. From the cell-free access perspective, this scenario addresses key challenges such as network scalability and dynamic resource allocation. MRAT-NCPs are strategically deployed across the service area to ensure optimal positioning of Radio

Access Network (RAN) provider nodes, dynamically extending network coverage in regions where the fixed infrastructure is limited. These nomadic nodes create multi-hop networks, allowing data to be relayed from one MRAT-NCP to another, enhancing both coverage and reliability. To manage the dynamic interactions between UEs and MRAT-NCPs, an advanced control and pricing system is required. Furthermore, blockchain technology is integrated to ensure secure cooperation between different operators, providing immutable records for authentication and authorization processes, guaranteeing data integrity and privacy across multiple operators, allowing UEs to seamlessly transition between MRAT-NCPs from different providers without compromising security. The use of blockchain also enables smart pricing policies, which optimize resource allocation by dynamically adjusting fees based on network demand and availability, ensuring cost-efficient usage of network capacity. Finally, as mentioned above, the use of secured user-centric data caching mechanisms permits to speed up these transactions in order to improve the user experience.

3.2 Multi-hop Coverage Extension

As previously explained, the scenario proposed in NANCY for the expansion of connectivity in 5G networks offers multiple advantages by simultaneously addressing both spectrum optimization and coverage improvement in complex and challenging areas. The solution relies on three key pillars: The use of PC5 links between user devices (UEs) to establish D2D communications, the extension of coverage through multi-hop communications, and the integration of a new node called Multi-Radio Nomadic Connectivity Provider (MRAT-NCP). Furthermore, this architecture is complemented by blockchain technology and secure data-caching, which improves the security, reliability, and performance of the network (see Figure 1).

In contexts such as rural environments or dense urban areas, where traditional 5G infrastructure deployment is often expensive and technically challenging, the ability to extend coverage via D2D links and multi-hop communications offers a cost-effective and flexible solution [2]. By using the PC5 interface, UEs can communicate directly without the need for a base station, creating a multi-hop network in which data travels through nearby devices until it reaches a base station or MRAT-NCP node. Thus, this approach not only extends coverage but also facilitates connectivity for users in remote or hard-to-reach areas, thereby contributing to a more inclusive network.

Moreover, this proposed scenario also addresses critical coverage gaps in current 5G infrastructures by implementing cell-free access mechanisms that strategically deploy MRAT-NCPs throughout service areas, optimizing network coverage and connection reliability. As a result, UEs can connect and move seamlessly across the area, supported by operator collaboration, while maintaining strong connectivity even in challenging environments. The multi-hop connections formed by these strategically placed MRAT-NCPs allow data to be relayed among nodes until reaching the 5G fixed infrastructure, hence creating a more resilient network that provides extended and reliable coverage in locations underserved by fixed infrastructure. Depending on the agreement reached by each MRAT-NCP and the operators, this could be a grant-free service for the users or not.

Beyond these connectivity advantages, MRAT-NCP will play a key role in the integration of the identity management system of the NANCY security ecosystem, as described in section 3.4. This ensures strong authentication and seamless identity verification across all network nodes, maintaining trust and security of interactions between user devices and the infrastructure. This feature is especially valuable in dynamic, multi-hop communication scenarios, where it is critical to establish and maintain secure connections. In addition, MRAT-NCP will employ the secure caching mechanism described in Section 3.5, which provides an encrypted and immutable solution for storing and retrieving data. This mechanism improves performance by reducing latency and ensuring data integrity, which is crucial for multi-hop communication, where data traverses several nodes before reaching its destination. Together, these features make MRAT-NCP a key element for the connectivity and security of the NANCY architecture.

One of the most relevant aspects of this scenario is the optimization of frequency spectrum usage, a key advantage in the expansion of 5G coverage [29]. Through direct D2D communication, the dependency on base stations is reduced, resulting in lower spectrum usage on commonly congested frequencies. This approach enables the PC5 interface to facilitate efficient transmissions between UEs, thus liberating the spectrum on base stations and allowing for greater flexibility in the allocation of network resources. In particular, spectrum optimization proves beneficial in high-density environments, such as urban areas or mass events, where frequency band space is limited, and bandwidth demand is high. By dynamically distributing traffic among multiple MRAT-NCP devices and nodes, the network adaptively allocates resources according to user density and real-time traffic needs, maximizing the use of the available spectrum.

Besides, NANCY also investigates the implementation of semantic communication (Task 4.4), an emerging approach in 5G networks that optimizes transmission by considering the context and specific content of messages [30]. In this scheme, devices connected to the 5G network via the *Uu* link can employ semantic coding, which allows messages to be analyzed and compressed, transmitting only the most relevant information to the user. By significantly reducing the volume of data, this approach improves spectrum efficiency and reduces latency, especially in the transmission of multimedia content such as video. A concrete example of an application in semantic communication could include the use of a short-range frequency band for high-quality video transmission between devices over the PC5 link, so that only a fraction of the processed information is sent over the 5G network. This combination leverages multi-hop communication capabilities and the *Uu* link, allowing MRAT-NCP nodes to efficiently process, aggregate and distribute data, sending only essential and relevant information to end users. Consequently, this strategy further optimizes the available bandwidth, improving network efficiency. The integration of semantic communication with multi-hop architecture and data distribution allows real-time processing and transmission to be suited to the specific requirements of each application. For example, in augmented reality or video streaming applications, semantic communication could filter and select the most relevant visual or auditory information, reducing the load on the network and providing a smoother and more adaptive user experience. This ability to adjust streamed content according to context and relevance improves network performance in high-demand scenarios, optimizing not only the user experience but also the use of network resources. More details about Semantic Communications and its implementation in NANCY will be given in D4.4 'Trustworthy Grant/Cell-free Cooperative Access in NANCY's Demonstrators and Testbeds'.

As a whole, the NANCY scenario offers a comprehensive approach to overcome the current limitations of 5G, improving both coverage and network flexibility in areas underserved by conventional infrastructure. Through the use of advanced connectivity mechanisms, adaptive resource management and optimized spectrum usage, this model improves efficiency and signal quality, making better use of available bandwidth Altogether, this design not only addresses critical connectivity gaps, but also establishes a solid foundation to support ProSe-based applications expected in next-generation networks.

Technical implementation/results

The On-Board Units (OBUs) utilized in this study correspond to Cohda MK6 polyvalent units, integrating multiple Radio Access Technologies (RATs) such as 802.11p, PC5 (LTE), and 5G. Due to their limited computational capacity, these units have been connected via Ethernet to slightly more capable devices, such as Raspberry Pi 5 and LattePanda. These external devices handle most of the computational workload required for the study.

The primary focus of these experiments has been operating on the PC5 interface. Since PC5 lacks native IP connectivity, a series of proxy mechanisms have been implemented to transform PC5 traffic into UDP traffic and vice-versa. This transformation enables seamless raw IP data handling through an endpoint, such as a Raspberry Pi. Additionally, scripts on the external device encapsulate TCP and UDP traffic into UDP packets, which are then reformatted into PC5-compatible transmissions.

Latency Analysis for PC5 Interface

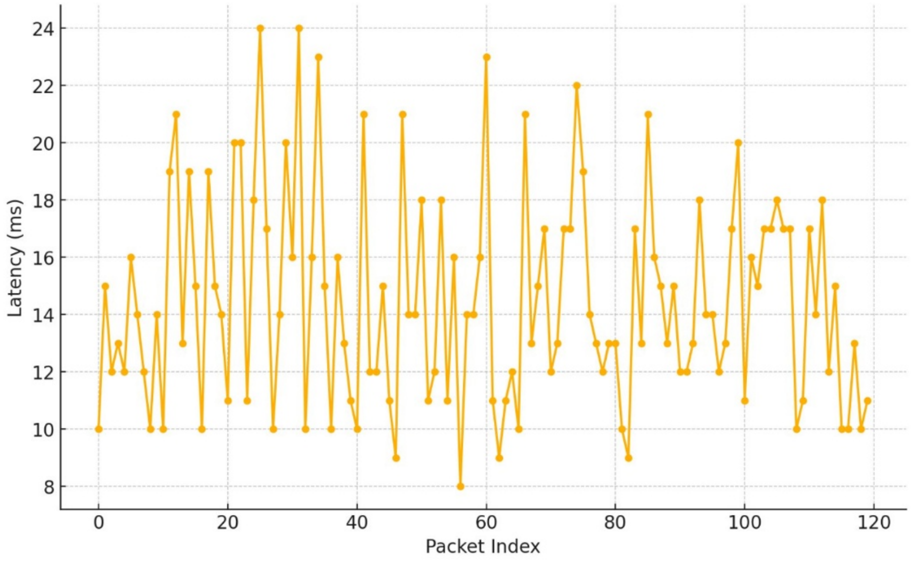

Figure 4. Latency Analysis for PC5 Interface

By using the ping tool, the latency performance of the PC5 interface was analyzed (Figure 4) Concretely, we have measured the time lapse since a ping request is generated by one OBU and sent through its PC5 interface until the reply from another OBU (also transferred from a PC5 interface) is received.

Key results are as follows:

- **Minimum Latency:** 8 ms
- **Maximum Latency:** 24 ms
- **Mean Latency:** 14.49 ms
- **Standard Deviation:** 3.69 ms
- **Jitter:** 4.08 ms

The analysis highlights relatively high stability in latency with a controlled jitter, which is essential for time-sensitive Vehicle-to-Everything (V2X) communications.

Bandwidth and Packet Loss

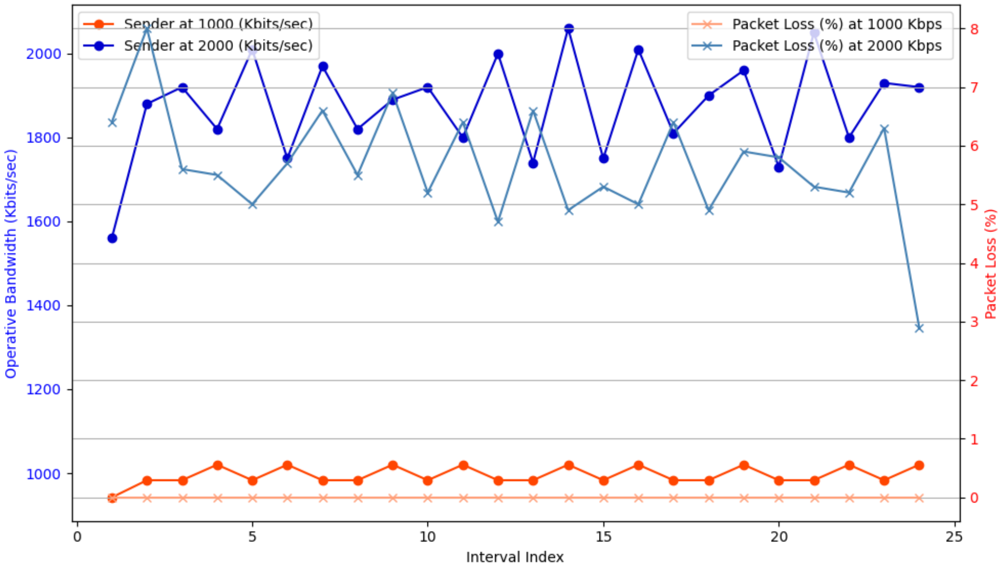

Figure 5. Comparison of bandwidth and packet loss at different data rates

In the next experiment, we evaluated the performance of the PC5 interface when supporting different data-rates constant traffic, namely, 1Mbps and 2 Mbps (see Figure 5). The results from both experiments are shown in Table 1:

Table 1. Results from PC5 transmissions at different bitrates

	1 Mbps	2 Mbps
Data Transferred	2.91 Mbytes	8.10 MB
Jitter	7.043 ms	3.36 ms
Average Bitrate	1.02 Mbps	1.89 Mbps
Packet Loss	0/595 (0%)	503/8799 (5,7%)

It can be seen that the PC5 link presents modest bandwidth. At 1 Mbps it shows good reliability in terms of packet loss (see Figure 5). However, at 2 Mbps, the link begins to be overloaded, and packet loss starts to occur.

These results are justified as follows: The amount of data bursts depends on the MCS configured for the OBU. The MCS is dynamically adjusted based on the packet length, with a maximum value of 11. Theoretically, this corresponds to 9.84 Mb/s. The channel bandwidth for the European regulation of PC5 is 10 MHz. In PC5, there are two modes for link operation. The first mode, SPS, has an unavoidable latency of 20 ms due to its operating mechanism. In contrast, the event mode reduces this latency to 5 ms. In event mode, the device transmits the packet in a 1 ms slot but needs to repeat the transmission five more times for the receiver to fully assemble the packet and forward it to the upper layers. Therefore, the maximum effective bitrate is calculated as 9.84

Mb/s ÷ 5 ms = 1.968 Mb/s, which is confirmed in the obtained results. As a result, any data rate above this limit results in packet loss, leading to channel unreliability.

Latency Comparative Analysis: PC5 vs. Uu interfaces

Given the bandwidth restrictions found for the PC5 interface aforementioned, we focus our comparative analysis between the *PC5* and *Uu* interfaces on the latency obtained by each of them in a similar ping experiment as the one employed above. As depicted in Figure 6, we make use of both interfaces to ping one OBU from another one.

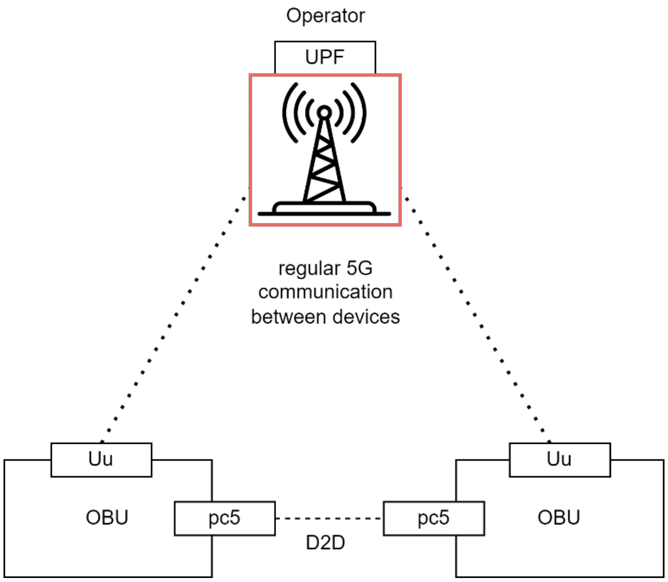

Figure 6. Test setup

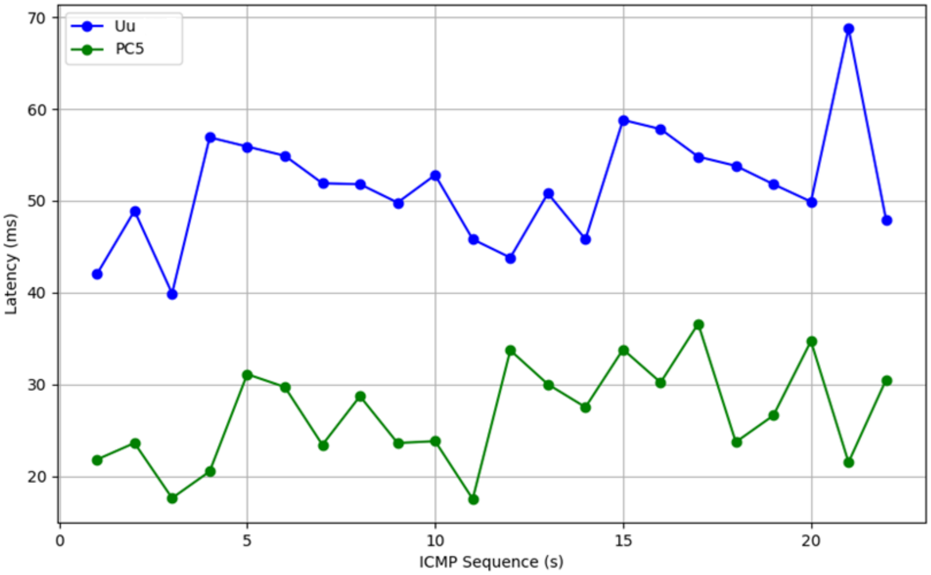

Figure 7. Latency comparison using Uu and PC5 interfaces

Figure 7 illustrates the comparison of the ping latency obtained using the PC5 and *Uu* interfaces. The latency for using the *Uu* interface is notably higher, averaging around 50 ms, compared to the lower and more stable latency observed when using PC5. This is an expected outcome as the connection of the OBUs through the PC5 interface is direct, without intermediaries, as happens in the case of using the *Uu* link.

However, as discussed before this advantage is counterbalanced by PC5's reduced reliability and limited data throughput, due to its technological immaturity in comparison with the extensively used *Uu* interface. Actually, the PC5 link is primarily designed for V2X communications, making it less suitable for more complex data traffic; nevertheless, in NANCY we have been able to transmit raw IP traffic over this interface in order to reach its performance limits and understand the potential of the 3GPP’s Proximity Services (ProSe) working over it.

Challenges and Limitations

As just mentioned, several limitations were identified during this study. The PC5 implementation is inherently constrained due to its design, mostly focused on V2X-specific communications. This design limitation introduces additional complexity in managing other kinds of data traffic and results in suboptimal performance in terms of bandwidth, latency and link reliability. These factors underscore the need for further refinement and adaptation of PC5 technology in the next versions of cellular technologies, e.g., 6G, for supporting diverse applications beyond V2X.

3.3 Multi-cell Connectivity

Throughput, in the context of the work in the NANCY project, denotes the effective amount of information that can be transferred over the NANCY radio network to the end users. As opposed to the notion of bandwidth that typically reflects the amount of information that can be transferred over the network under ideal conditions, throughput is a network performance indicator that quantifies how much data can be practically transferred over the network under given operational and environment conditions. Measured at the application level, it is tightly coupled with the radio transmission techniques implemented in the network, the configuration/parameterization of other mechanisms at higher layers of the protocol stack, and the specific context of network operation.

Since throughput measurements capture the running network performance, throughput forecasting provides a means to infer changes in the network operational conditions and anticipate performance degradation, so as to trigger corrective actions. For instance, it can predict a user handover event and help the radio network manage it resulting in overall better network coverage and resilience. In the context of the cell-free paradigm studied in this deliverable, throughput forecasting can prove to be an important functional block for guiding the selection of the best available AP and realizing seamless connectivity. When approached as a service, the TFS builds on state-of-the-art models, while respecting the specific characteristics of the NANCY B5G functionality. Hence, it works with real-time data series and makes modest use of computational resources.

At the core of the TFS service, lies an LSTM model, a type of Recurrent Neural Network (RNN), which implements the following layers:

- Two LSTM layers.
- 1 Dropout Layer for each LSTM layer for bolstering robustness and removing overfitting.
- 2 Dense Layers, which are meant to capture complex data patterns and look into high-level, feature-combining dependencies providing sequential output.

This LSTM model was trained with the Lumos 5G dataset [31], a large record of throughput values, as measured by a custom application running on the user side, together with the logs of several features, which can be separated into three groups:

- The **Basic (B) group,** including *Throughput*, *nrStatus, latitude, longitude* and *abstractSignalStr.*
- The **Positional (P) group,** including user mobility-related features such as the *moving speed* and *compass direction.*
- The **Signal Strength (S) group,** including physical layer features such as the *lte_rssi, lte_rsrp, lte_rsrq, nr_ssRsrp, nr_ssRsrq* and nr_*ssSinr* features.

The LSTM model training process was carried out with four different feature set combinations, namely the basic group of features alone (B), the basic group together with the positional group (B+P), the basic group together with the signal strength group (B+S) and finally, all three feature groups (B+P+S). The preprocessing of the training set included linear interpolation to make up for missing signal strength values, Moving Average-based filtering to address the noise in the respective recordings, and MinMax normalization of feature values to map them in the interval between zero and one.

For all 118 time-series in the dataset, the 80%-10%-10% split between training, validation and test data, respectively, was applied. For the model training processes an i5-12600K processor was used with a GPU NVIDIA 3060 of 8GB graphics card and 16GB RAM. The training time was measured approximately 14 seconds per epoch including the whole Lumos 5G dataset. The inference time was also measured in the order of seconds, much less than one minute.

The model prediction accuracy was assessed through the RMSE (Root Mean Square Error), defined as the square root of the average of the squared differences between the original throughput values and the predicted ones. With training dataset values spanning 20 seconds, the outputs of the algorithm are throughput value predictions for up to 20 seconds ahead of time. For all runs, we compared the predictions of our LSTM model to those of the Seq2Seq model [32] and a Seq2Seq model with Luong attention mechanism [33].

Our experiments showed that the lowest RMSE between the predicted and real throughput values was observed for the combination of the basic (B) and signal strength (S) feature groups. The inclusion of the positional feature group was found to rather worsen performance. The respective RMSE results obtained from model execution are summarized in Table 2.

Table 2. RMSE values of three tested throughput predictions models (in Mbps)

	LSTM	seq2seq	seq2seq Luong
B + S + P	267	258	290
B+P	276	264	271
B+S	239	248	249
B	247	260	259

As expected for any LSTM model, the most accurate predictions in terms of RMSE were those referring to the first few time steps (4-7 seconds ahead in time). Figure 8 compares the RMSE achieved under the three tested models, pointing to the better performance of the LSTM model after the seven initial steps of time ahead.

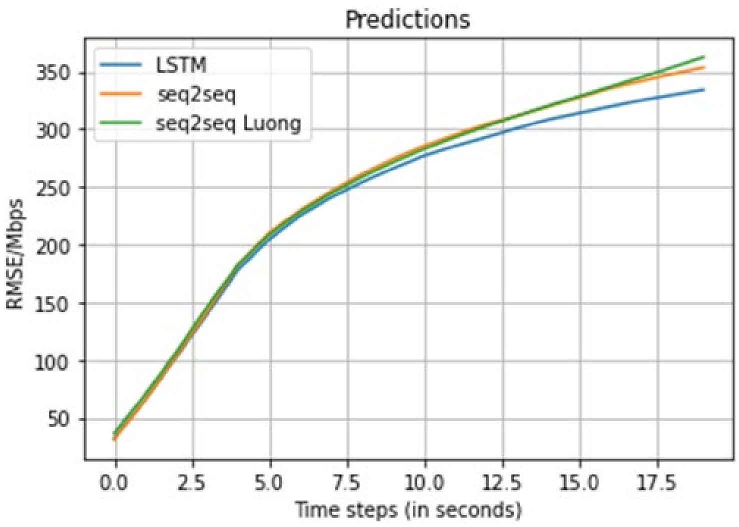

Figure 8. Throughput Forecasting RMSE for all 3 models considered

Within the NANCY concept, the throughput forecasting module is envisioned to provide its throughput predictions for the different networks available to serve a UE. More specifically, since the UE is usually within the range of more than one BS/AP, it utilizes the available API to execute the TFS algorithm separately for each adjacent base station that can serve it. These throughput predictions are then fed to a decision engine that compares them and selects the cell that best satisfies the QoS requirements of the UE, possibly in combination with other QoS information available to it through different means. These requirements are clearly defined in the SLA signed between the UE and each service provider to ensure that critical goals, such as extremely low latency in delay-sensitive tasks or ultra-high reliability in tasks involving high risk, are always guaranteed (detailed in D4.1 'Computational Offloading and User-centric Caching'). The Throughput Forecasting Service can also support the scenario of the UE transmitting simultaneously through different networks, in order to boost the system's reliability, and enhance resource allocation and energy efficiency, as considered in the NANCY multi-tenant intelligent O-RAN architecture.

From an experimental perspective, the LSTM model of the TFS has been implemented, with the results graphed as shown above and integrated into a Docker Container, communicating via an API. This approach permits its easy integration in different kinds of devices as explained in Section 4.1.1.

3.4 Blockchain-based Trustworthy Access, Pricing, and Accounting

Trustworthy access to the NANCY ecosystem requires the infrastructure to enable mechanisms that support seamless, privacy-preserving authentication, authorization, and accounting (AAA). Accessing services involves both trustworthy authentication and authorization. In this context, blockchain has been integrated into the NANCY ecosystem to provide these essential properties. Distributed Identifiers (DiDs) are stored on the blockchain, adding a trusted layer to these processes. Additionally, a permissioned blockchain ensures that only authorized blockchain users can access and write to specific nodes. UEs and service providers are equipped with wallets that enable interaction with the blockchain mechanisms. With the DiD included in the blockchain, any node can verify the genuineness of an originating request. All the details about these processes will be provided in D5.2 'NANCY Security and Privacy Distributed Blockchain-based Mechanisms'.

Furthermore, the privacy-preserving Attribute-Based Credential (p-ABC) scheme is adopted in NANCY to grant authorization to third-party services in a privacy-preserving manner. In this scheme, the UE presents only the minimal, obfuscated information that the verifier requires to authorize access. The UE possesses several attributes signed by an Issuer and can derive these attributes into pseudonyms. These pseudonyms are then used by a service provider (e.g., a MultiRAT-NCP) for authentication and authorization without revealing the UE's actual identity. For more details about this process, please refer to D5.2 'NANCY Security and Privacy Distributed Blockchain-based Mechanisms'.

For accounting purposes, requests are forwarded to the original Issuer, who can retrieve the original identity of the UE. This step ensures both security and effective accounting, enabling accountability while maintaining user privacy. For every cross-operator service, such as cell-free mechanisms, smart pricing comes into play. Smart pricing is a key component to enable trustworthy resource selection based on the final price for the UEs.

The Smart Pricing Module (SPM) represents an AI approach to dynamic pricing, using AI technology to foster a competitive and balanced market. Hosted securely on Eight Bells premises, the SPM's role is the optimization of pricing decisions, creating value for both providers and consumers.

At its core, the module operates as a multi-agent reinforcement learning environment, where individual agents represent different providers in the Marketplace. These agents are trained using a self-play mechanism, allowing them to adapt and refine their strategies autonomously through iterative interactions. This training methodology ensures that the system can dynamically respond to complex market conditions.

The process begins with the collection of maximum and minimum price boundaries set by providers in the Marketplace. These boundaries establish the permissible range within which each provider can submit bids. With this information, the SPM initiates a multi-round blind reverse auction, a process inspired by game theory principles. Providers submit secret bids over multiple rounds, with each round revealing only their rank relative to competitors. This iterative process allows providers to incrementally adjust their bids based on their rank. In the final round, the provider with the most competitive bid is declared the auction winner.

This game-theoretic approach promotes a competitive and balanced market. The SPM reduces the possibility of monopolistic pricing by motivating providers to work within pre-defined limitations. This guides market prices towards a state that balances profit for providers with consumer affordability.

Once the final price is determined, the SPM communicates this information to the Marketplace infrastructure via a dedicated API. In this role, the SPM functions as an oracle, providing verified pricing data to the blockchain. Importantly, the SPM does not directly interact with blockchain operations, ensuring a modular and secure integration.

3.5 Secure Data Handling

As introduced in Section 2.3, NANCY integrates an advanced Secure Storage solution based on VOSySmonitor and OPTEE to provide tamper-proof devices at the network edge that will secure sensitive data for this layer. With further details, in the V2X ecosystem, there is the need to quickly associate users with their corresponding capabilities within the network. A user must be quickly checked to verify whether it is already registered through its assigned pseudonym and whether is granted access to NANCY particular services. On the one hand, these data should be easily accessible at relay nodes, where they are cached close to the end-vehicles. On the other hand, these data are sensitive and for this purpose, they must be sealed by storing them in secure mediums, in a de-centralized fashion. For this use case, the V2X ecosystem will benefit from OPTEE-enabled nodes that feature a Secure Storage service, which will provide a straightforward way to load and store data in a secure way.

3.5.1 VOSySmonitor

NANCY goes beyond the existing state-of-the-art by introducing VOSySmonitor at the Secure Monitor layer of ARM Trustzone-based architectures, to support OPTEE services on top. Specifically, VOSySmonitor is an ASIL-C certified software [24] that adheres to the stringent automotive standard ISO 26262 [34]. In a nutshell, VOSySmonitor is the firmware that enables the concurrent execution of safety-critical applications in the secure world and non-critical applications in the normal world. Compared to alternative solutions, with VOSySmonitor it is possible for a safety-critical and a non-critical OS to share the same processors and co-execute on them in a time-sliced fashion. The overall architecture of the VOSySmonitor software on an ARM multi-core platform is depicted in Figure 9. As it is logical, the internal scheduling policies of VOSySmonitor always prioritize the safety-critical OS when it comes to sharing the same processing units with the normal world, which can be only scheduled on them as soon as the secure world is idle. Moreover, VOSySmonitor achieves great setup times and context switching latencies compared to other solutions and thus will benefit NANCY for the implementation of the de-centralized Secure Storage service.

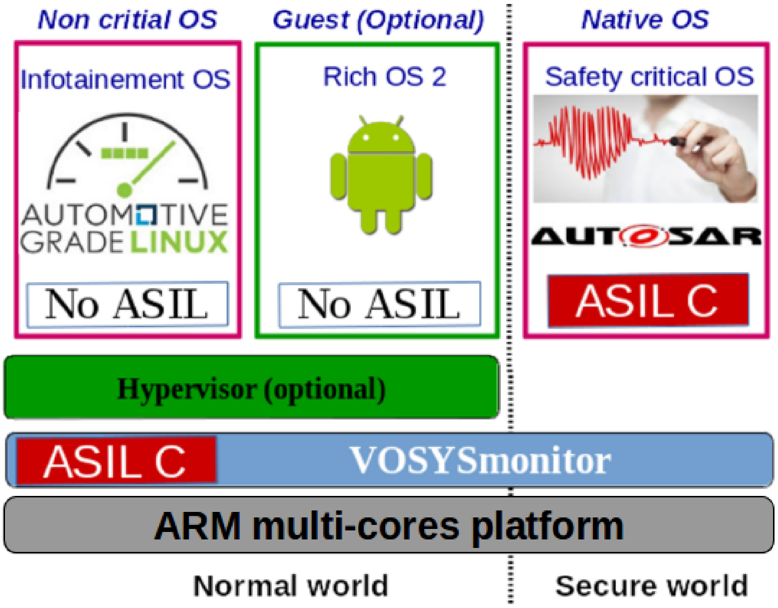

Figure 9. VOSySmonitor architecture

3.5.2 VOSySmonitor and OPTEE Integration

The target is to integrate VOSySmonitor with OPTEE and achieve the overall architecture as depicted in Figure 10. In this scenario, the normal world accommodates a general-purpose feature-rich OS like Linux, while the secure world hosts the OPTEE core in the kernel and the OPTEE Trusted Application in the user-space, which is the Secure Storage in this case. The Trusted Application is only activated upon request from the normal world and the two OSes (Linux and OPTEE) are co-executed on some pre-defined core. A Client Application deployed on the user-space of the Linux OS can therefore issue requests towards the Secure Storage service, according to the Global Platform specification standards previously depicted in Figure 2.

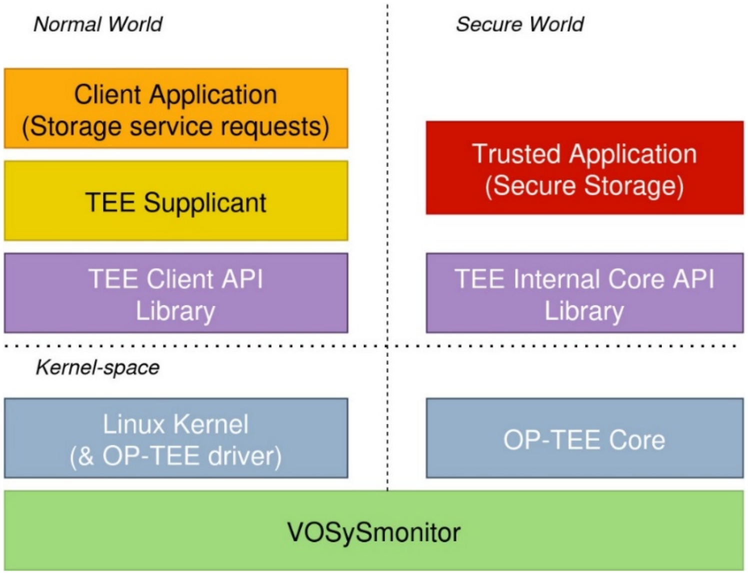
Normal World
Secure World
Client Application (Storage service requests)
TEE Supplicant
TEE Client API Library
Trusted Application (Secure Storage)
TEE Internal Core API Library
Kernel-space
Linux Kernel (& OP-TEE driver)
OP-TEE Core
VOSySmonitor

Figure 10. VOSySmonitor and OPTEE deployment for Secure Storage provision

Regarding the integration needs for VOSySmonitor, according to the Global Platform specifications VOSySmonitor has to support some specific OPTEE Secure Monitor Call functions, that adhere to the SMC Calling convention [35]. By implementing the proper OPTEE SMC functions, VOSySmonitor will be able to address SMC requests coming from the OPTEE driver deployed in the normal world, as well as requests coming from the OPTEE core OS deployed on the secure world, as demonstrated in Figure 11.

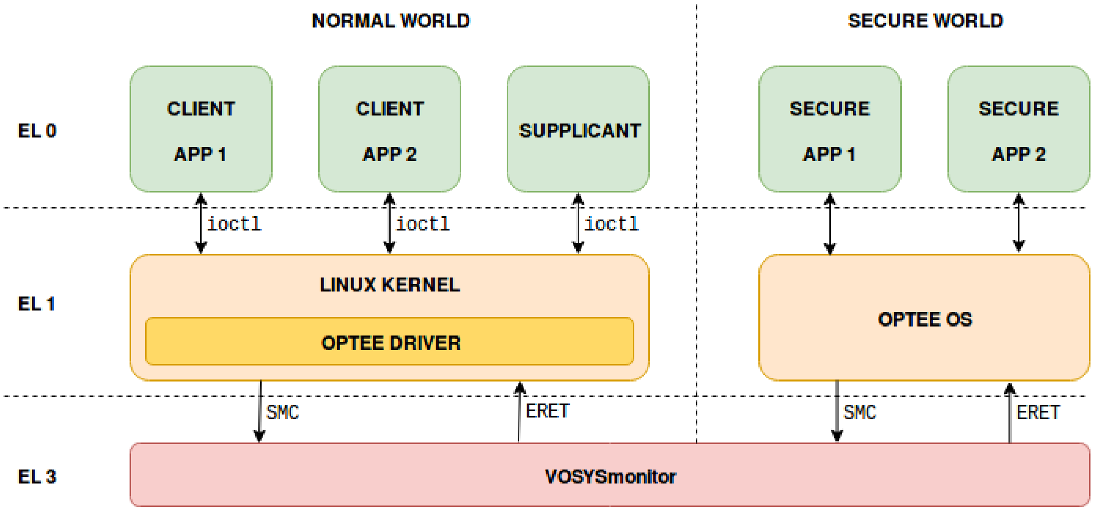

Figure 11. Interfaces between the various layers in the OPTEE-VOSySmonitor stack

With more details, the total required SMC functions that have been integrated into VOSySmonitor for OPTEE to operate, regardless of the supported use case, are depicted in Figure 12. They are differentiated between those issued from the normal world and those issued from the OPTEE core OS (towards the monitor).

Regarding normal world calls, the SMCs are grouped between those specified by the SMC calling convention, and the OPTEE-specific ones, which request an action from the secure world. Also, with red are depicted the only SMCs that are standard, in the sense that they do not block interrupts until the execution returns to Normal World.

Regarding secure world calls, the SMCs are grouped between those that complete an action that was previously requested and those named “RPC requests” that actually request a service from the normal world. RPC requests are, for example, issued when the Trusted Application wants to carry out an operation on e.g. the normal file system of the Linux OS.

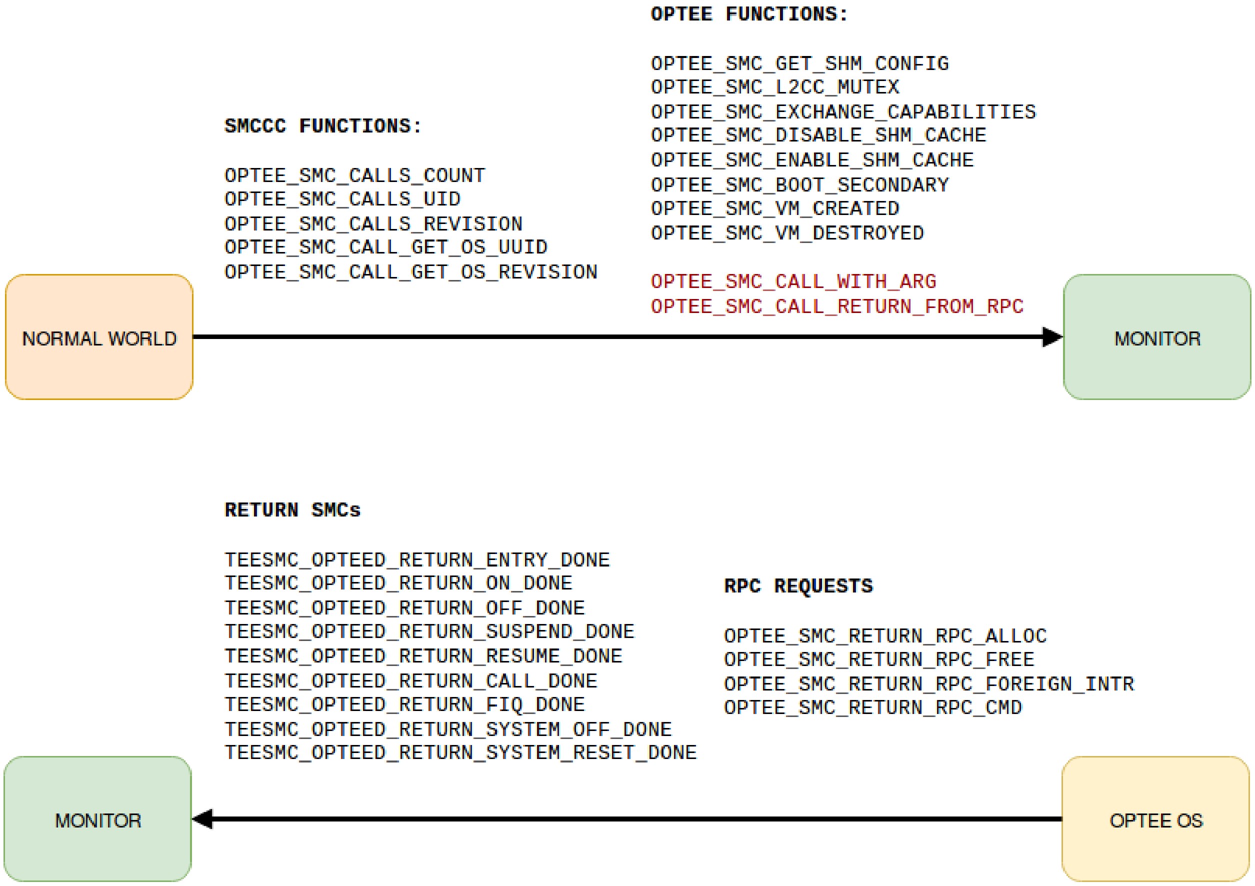
OPTEE FUNCTIONS:
OPTEE_SMC_GET_SHM_CONFIG
OPTEE_SMC_L2CC_MUTEX
OPTEE_SMC_EXCHANGE_CAPABILITIES
OPTEE_SMC_DISABLE_SHM_CACHE
OPTEE_SMC_ENABLE_SHM_CACHE
OPTEE_SMC_BOOT_SECONDARY
OPTEE_SMC_VM_CREATED
OPTEE_SMC_VM_DESTROYED
OPTEE_SMC_CALL_WITH_ARG
OPTEE_SMC_CALL_RETURN_FROM_RPC
SMCCC FUNCTIONS:
OPTEE_SMC_CALLS_COUNT
OPTEE_SMC_CALLS_UID
OPTEE_SMC_CALLS_REVISION
OPTEE_SMC_CALL_GET_OS_UUID
OPTEE_SMC_CALL_GET_OS_REVISION
NORMAL WORLD
MONITOR
RETURN SMCs
TEESMC_OPTEED_RETURN_ENTRY_DONE
TEESMC_OPTEED_RETURN_ON_DONE
TEESMC_OPTEED_RETURN_OFF_DONE
TEESMC_OPTEED_RETURN_SUSPEND_DONE
TEESMC_OPTEED_RETURN_RESUME_DONE
TEESMC_OPTEED_RETURN_CALL_DONE
TEESMC_OPTEED_RETURN_FIQ_DONE
TEESMC_OPTEED_RETURN_SYSTEM_OFF_DONE
TEESMC_OPTEED_RETURN_SYSTEM_RESET_DONE
RPC REQUESTS
OPTEE_SMC_RETURN_RPC_ALLOC
OPTEE_SMC_RETURN_RPC_FREE
OPTEE_SMC_RETURN_RPC_FOREIGN_INTR
OPTEE_SMC_RETURN_RPC_CMD
MONITOR
OPTEE OS

Figure 12. Complete OPTEE SMC calls support in VOSySmonitor

3.5.3 OPTEE Secure Storage Service Description

The Secure Storage services implemented in OPTEE are based upon the GlobalPlatform TEE Internal Core API specification. Through these services, it is possible to store general-purpose data as well as key assets securely, by guaranteeing the confidentiality and integrity of the stored data and also guarantee the atomicity of the operations carried out on them. With confidentiality, the privacy of the data is guaranteed by restricting access to them only to authorized users. Then, integrity ensures that the data are complete, accurate and consistent throughout their lifespan. Last, by ensuring atomicity, updates on the data can only happen atomically in a way that the operation can never happen partially. The Secure Storage service of OPTEE which is relevant for NANCY is the REE_FS and is based on the normal world file system. Its architecture is depicted in Figure 13.

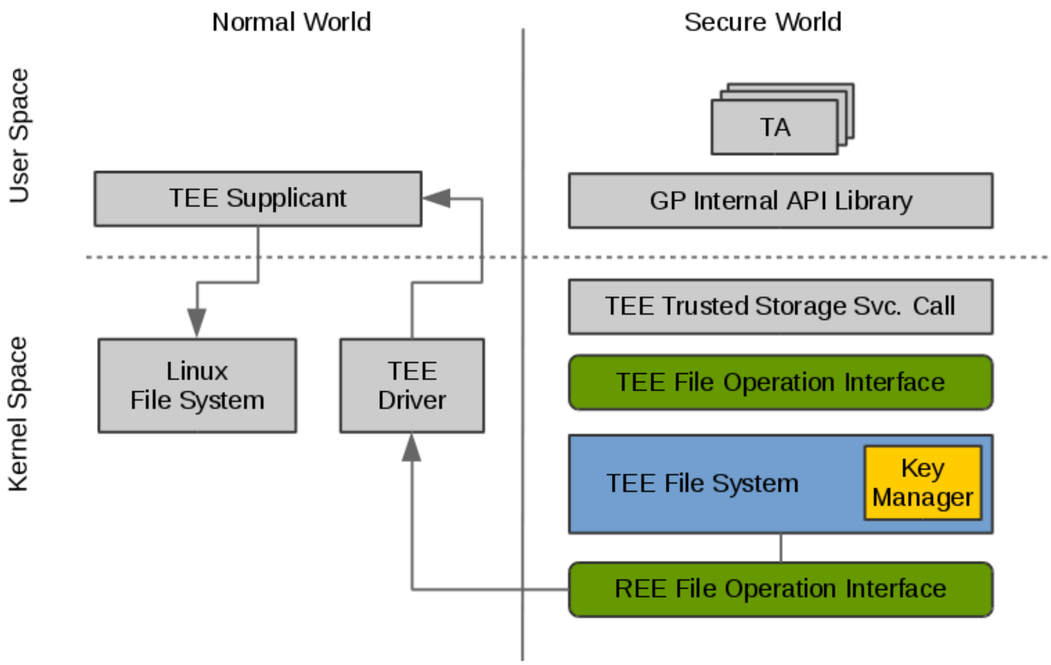

Figure 13. REE_FS Secure Storage service architecture of OPTEE

To get into some details regarding the basic flow of the OPTEE Secure Storage service [36], the first that happens during service initialization is the set-up of a new session, through which OPTEE loads the Trusted Application to the secure world with the help of the TEE Supplicant Linux module. Following this point, a Client Application deployed in the normal, Linux-based environment can request data operations (e.g., READ, WRITE, DELETE) from the Trusted Application service in the secure world. As soon as the request reaches the Trusted Application service, a series of TEE file operations will be invoked on the data. For instance, in the case of a WRITE operation, the TEE file system will encrypt the data which will then be forwarded to the REE file system for storage. The cryptographic assets used for the encryption are all stored internally, in the secure memory of the Trusted Application.

In simple words:

- The data operations are always invoked from a normal world Client Application. The Client Application is trusted, in the sense that it initially has access to the decrypted data, but these data are only local to the application and will be stored persistently in the secure medium.
- A series of OP-TEE components should be deployed in the board, which co-operatively with the Secure Monitor firmware (VOSySmonitor in our case) handles the invocation of the secure world, hosting the Trusted Application, upon demand.

- Every interaction between the normal and the secure world passes through VOSySmonitor first.
- The data is stored in an encrypted form in the persistent storage. This storage is usually accessible from the normal world, unless the board features specific Trustzone peripherals (such as TZPC) to specifically restrict access. In the scope of NANCY, such a scenario is not taken into consideration.
- All the cryptographic assets are internally secured in OP-TEE as they are stored in the secure memory because memory accesses in secure world are forbidden from the normal world in a Trustzone-based board.

3.5.4 OPTEE Secure Storage Example

To utilise the REE_FS Secure storage service, two simple client applications have been provided and included under /usr/bin as standard binaries of the Linux system. Below is demonstrated an example invocation of these binaries, for a scenario of storing users with their associated capabilities in the NANCY system:

- Create userA with the capability to access services A, B and C:

  ```
  # store "userA" "serviceA, serviceB, serviceC"
  Prepare session with the TA..Session ready!
  Store object in the TA secure storage..Object stored!
  Session closed
  ```

- Request to access userA and retrieve its capabilities:

  ```
  # load "userA"
  Prepare session with the TA..Session ready!
  Find and load object "userA"..
  Object Found. Id=userA, Value=serviceA, serviceB, serviceC
  Session closed
  ```

- Request to access a (non-authorized) userB:

  ```
  # load "userB"
  Prepare session with the TA..Session ready!
  Find and load object "userB"..
  load: Failed to read an object from the secure storage
  Session closed
  ```

With the REE_FS service, the secure data are stored in an encrypted form in the Linux file system and they look like:

```
# ls /var/lib/tee/

0        1        2        dirf.db
```

3.6 Trustworthy Grant/Cell-free Cooperative Access Workflow

In the 6G multi-stakeholder vision, operators cooperate to offer the best possible service to the users in a seamless way. Under this vision, UEs are envisioned to be connected to the network in an operator-less fashion, enjoying the best capabilities of each of them. In this sense, T4.3: Trustworthy cell-free cooperative access, has worked on key components for enabling such scenarios as discussed in previous sections. In the rest of the section, we document the developed system in which any kind of device can gain connectivity towards the 5G infrastructure as there is an intermediate connectivity provide (MRAT-NCP) that offers means to establish a communication channel with it (e.g., PC5, WiFi, etc).

As a requisite, we assume operational the NANCY's Identity Management explained in D5.2 'NANCY Security and Privacy Distributed Blockchain-based Mechanisms', where NANCY subscribers have a unique ID and attributes allowing to authenticate towards third-party services in a privacy-preserving approach following the Self-Sovereign Identity (SSI) principles. Privacy-preserving schemes are developed in WP5. A blockchain-based infrastructure integrated with p-ABC credentials provides trustworthiness to the access mechanisms and protects the privacy of the remote user by using pseudonyms. These pseudonyms hide the real identity and enable SSI, requiring only an access token to be presented for specific resources or services authorization. Additionally, TEE is applied over the provider's OBU to securely store and access authentication data, acting as a secure cache to avoid multiple verification processes for the same token (please refer to Section 3.5).

Besides, the MRAT-NCP provider is the central entity in charge of managing all the connectivity core operations, such as relaying the data transmitted by a granted UE towards the 5G infrastructure or deciding to which cell to retransmit such data (multi-cell connectivity). Regarding the former, as explained in Section 3.2, we use the PC5 interface to extend the connectivity of a given 5G infrastructure towards remote UEs through the MRAT-NCP. However, other wireless technologies, such as WiFi, could be employed as well. Regarding multi-cell selection, a radio monitoring framework is enabled, which gathers signal quality parameters from the different available cells belonging to the registered operators. Real-time monitored data feeds the throughput forecast module. The outcome from this forecast service is employed by a decision engine to decide which cell from the available is the most adequate considering the throughput terms in a given SLA (please refer to D4.1 'Computational Offloading and User-centric

Caching’). To distribute the traffic among different base stations, diverse modes of transmissions may be applied, using load-balancing techniques in transport protocols such as mTCP or SCTP, which allows multipathing for data flow transmissions. The usage of cells will be transparent to the end user. Cell selection mechanisms will follow the methods explained in Section 3.3, where dynamic cell selection occurs based on throughput forecasts and service requirements.

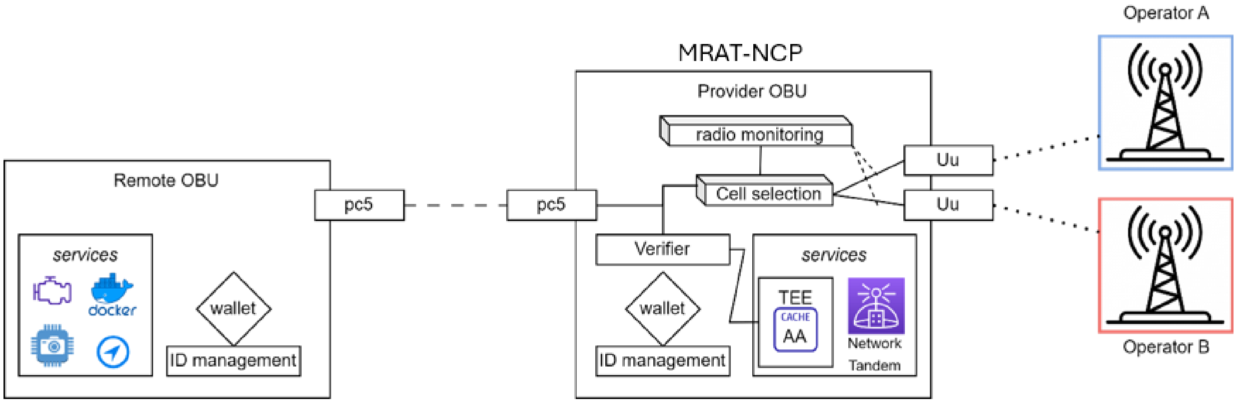

Figure 14. Cell-free access implementation architecture

Figure 14 depicts the cell-free access implementation architecture. A Remote OBU, with no 5G capabilities or without coverage from its home 5G operator is moving around. The Remote OBU aims to have connectivity for accessing vehicular services, but as it has no coverage it cannot register into the system. Following the Proximity Services (ProSe) paradigm, it detects a MRAT-NCP. Via PC5 link, it establishes a connection with the MRAT-NCP, which authenticates it by using the wallet, ID verifier, blockchain and TEE security to determine whether to allow the Remote OBU to access or not to the cell-free connectivity service. If allowed, an SLA is established, determining critical QoS aspects such as the throughput for the OBU retransmissions. SLA serves as the basis for the decision engine to select how to use available resources to retransmit the user data. The MRAT-NCP has several modems connected to different 5G networks; ideally, these modems have vSIMs allowing the customization and synchronization on-demand with the networks to configure the *Uu* link according to NANCY’s subscriber capabilities. As explained above, available cells for the MRAT-NCP are continuously monitored, extracting useful radio parameters that allow the throughput forecast module to determine the maximum bandwidth for each available cell. With this result, the cell selection engine uses networking techniques to redirect data flows from the PC5 interface towards the most adequate cell. Interfaces are monitored for accounting purposes, determining how much traffic has been forwarded as well as the time of use. As mentioned previously, the MRAT-NCP may charge for its services to the UE or the operator, in the last case being a grant-free service for the user. Finally, Figure 15 places all the involved components mentioned above within the functional view of the NANCY architecture.

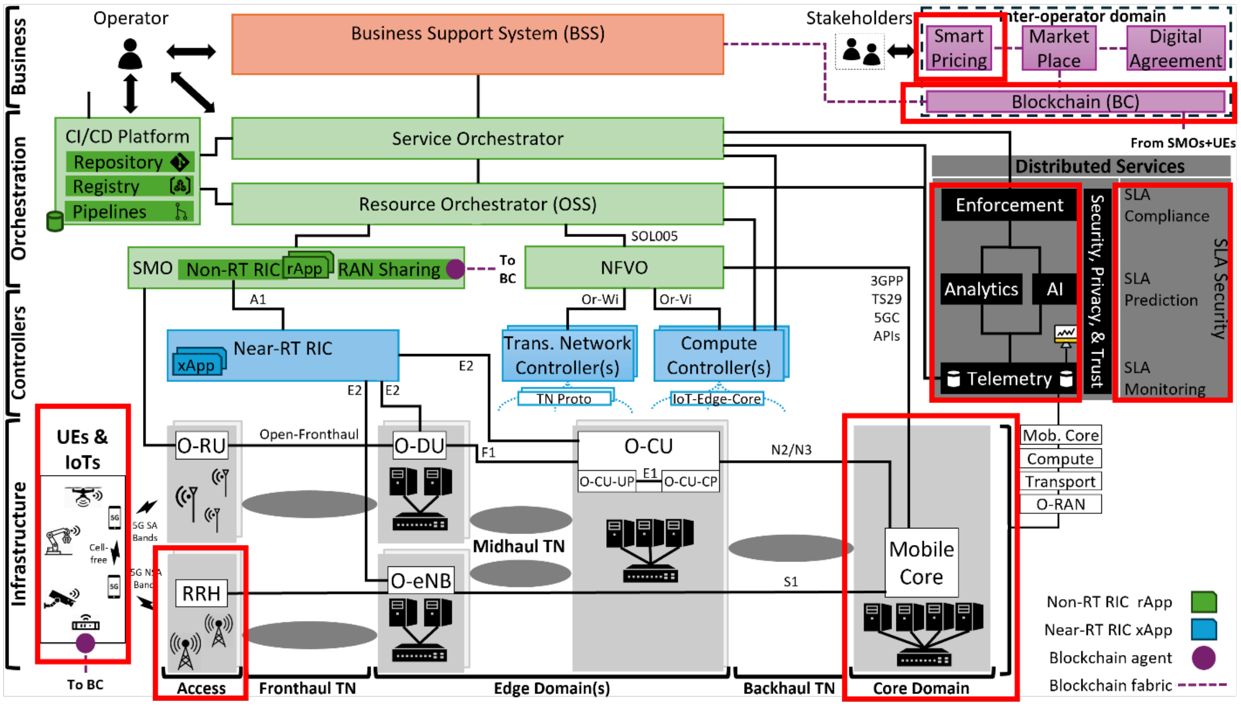

Figure 15. Mapping of cell-free access mechanisms' components on the NANCY implementation architecture

4. Trustworthy Grant/Cell-free Cooperative Access in NANCY's Demonstrators and Testbeds

4.1 Spanish In-lab Testbed

The Spanish extension testbed will host the main functionalities of privacy-preserving cell-free access mechanisms. It will incorporate cross work package mechanisms to support the use case. The focus of this demonstrator is to grant connectivity to a remote user where a 5G connection is unavailable due to several reasons, such as being out of coverage, a broken modem, or an overloaded link layer. Access to the network will appear cell-free from the remote user's perspective, as the MRAT-NCP has contracted connectivity consensus with several operators, allowing privacy-preserving access through a PC5 interface.

Spanish extension testbed comprises in-lab and outdoor testbeds. From the in-lab perspective, it is where devices, connectivity, and procedures are configured and validated. Outdoor mainly comprises mobility use cases under a real 5G radio base station to test solutions.

The in-lab testbed consists of:

- On-Board Units (OBU): Cohda mk6 supporting 5G and LTE-based PC5 sidelink communication.
- LattePanda and Raspberry Pi 5 devices: Lightweight devices used as far edge devices to compute tasks, such as cell selection, throughput forecast, identity management, and TEE services.

Each OBU will be wire-connected to one of the constrained devices to offload heavy computational tasks, while the PC5 link is used to enable D2D communication between them. Such a scenario is depicted in Figure 16 where the employed hardware is also included.

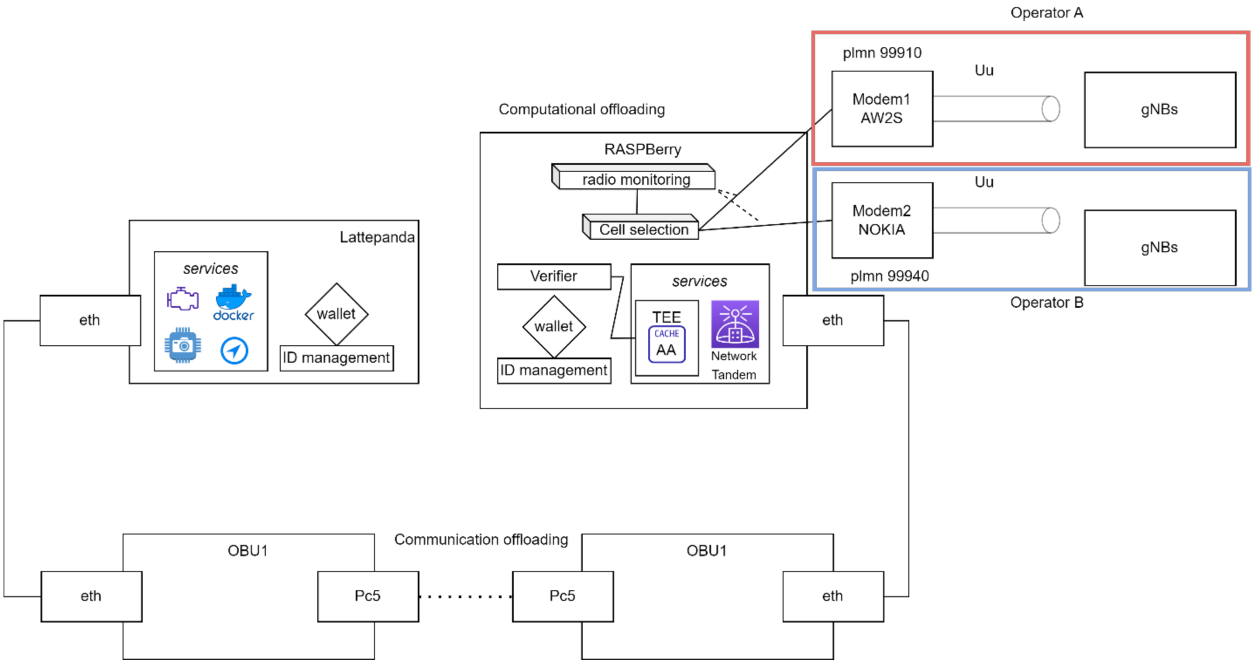

Figure 16. UMU's indoor testbed design

The implementation of this scenario is presented in Figure 17, which presents the different involved devices mentioned above.

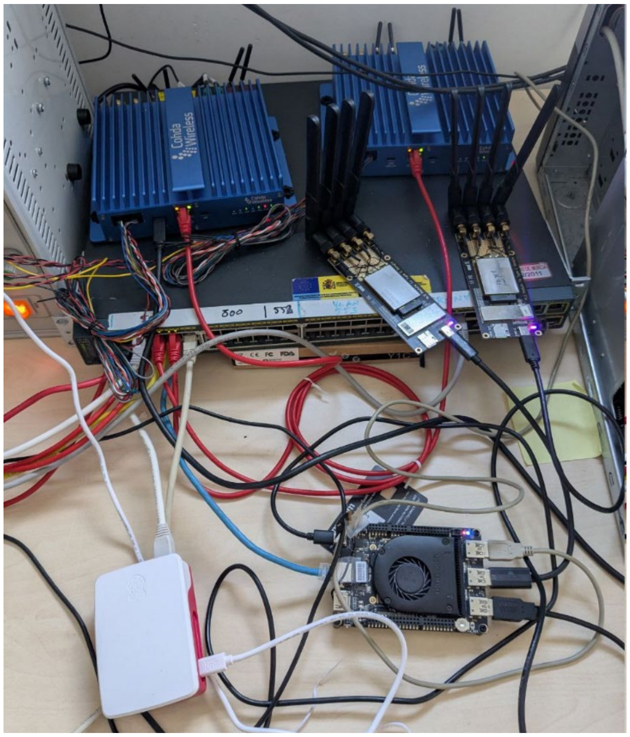

Figure 17. UMU's indoor testbed implementation

On the other hand, the UMU's outdoor testbed[1] includes:

- Two different operators: Covering different campus areas and with different schemes transmission schemes: TDD and FDD. Each operator has at least 2 different cells that cover almost the entire university campus.
- Electric vehicle: Corvus-utv which will carry one of the on-board units.

The UMU's outdoor testbed map is depicted in Figure 18, which also presents the Corvus-utv vehicle.

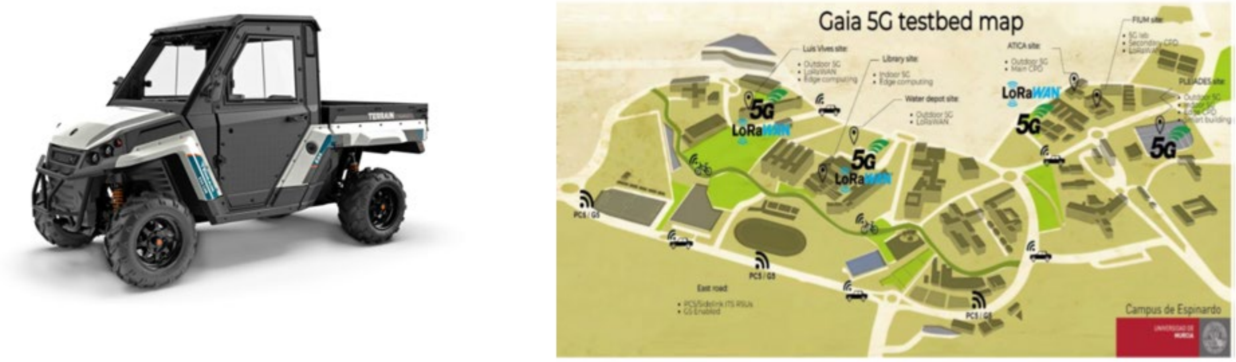

Figure 18. UMU testbed and experimentation vehicle

4.2 Spanish Demonstrator

Like the Spanish in-lab testbed, the Spanish outdoor demonstrator will also showcase 5G network coverage extension through cell-free mechanisms (Figure 19). In this case, the outdoor demonstrator will employ Unmanned Aerial Vehicle (UAV) nodes using V2X modules for connectivity. One of the UAVs will have an additional 5G module and thus will be able to connect to the O-RAN based 5G network on the ground. Using this setup, the remaining UAVs can be located farther away from the 5G base station. The V2X and/or 5G module is attached to the UAV through a Raspberry Pi via USB. This Raspberry PI also provides a certain amount of computing capabilities to support the service that is explained below.

The UAVs will make use of multi-hop communications across the V2X network to relay messages to and from the 5G network and the external data networks behind the 5G network. Therefore, a UAV that is not in the coverage area of the 5G base station will still be able to connect to the network and provide services to the users by forwarding messages via the V2X network, relaying

[1] https://ants.inf.um.es/en/gaialab

them in a hop-by-hop basis. This will require the development of a multi-hop algorithm tailored to the specifics of the use case and of the V2X communication stack and capabilities.

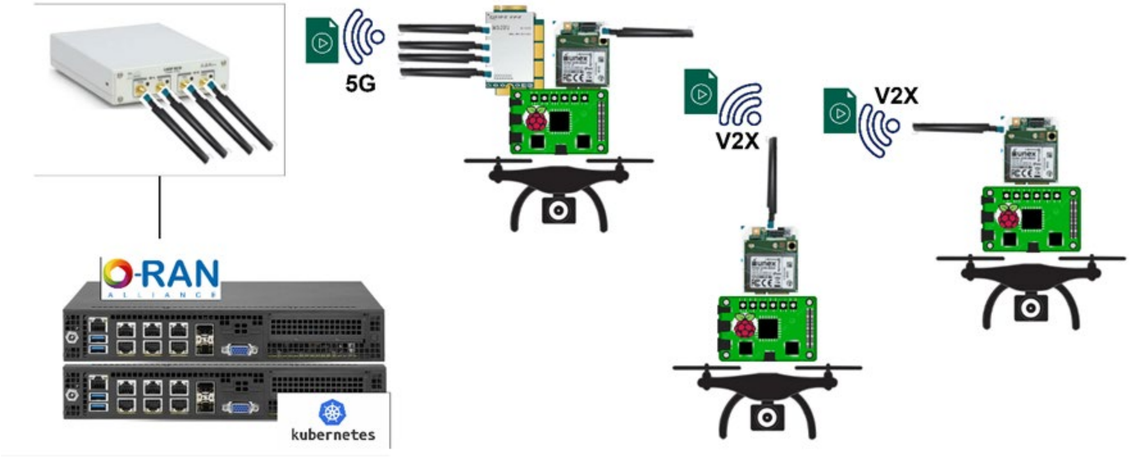

Figure 19. Spanish outdoor demonstrator design

The security of this network extension is achieved thanks to the installation of the Wallet and Blockchain Adaptor components in the required UAVs, that provide them with a decentralized NANCY's digital identity (DiD). UAVs will use this identity to register in the blockchain in the inter-operation domain. Therefore, the Spanish outdoor use case will demonstrate that the network coverage can be extended in a trustworthy manner, authenticating the communications of the nodes and ensuring that malicious nodes do not attack the V2X or 5G network.

The UAV nodes of the V2X network extension will provide a field monitoring and surveillance video service. When this service is active in a UAV, it will record video, pre-process it, and serve it by sending it across the V2X network. The application that provides this service will be built in a modular manner, enabling the offloading of parts of the pre-processing or post-processing to a Kubernetes-based MEC platform that is collocated with the 5G transport network. Offloading and placement decisions can be carried out according to policies dictated by the orchestration layer (please refer to D4.1 'Computational Offloading and User-centric Caching'). Post-processing will include, for instance, AI-based object or face recognition functionality in the video or image file, which results in additional metadata that can be stored and transmitted along with, or independently from the video file. Users connected to the 5G network will be able to access the processed video content as a service.

5. Conclusion and Outlook

This deliverable presented the main activities carried out in NANCY’s T4.3, which is focused on the design and development of effective trustworthy grant/cell-free cooperative access mechanisms. Firstly, a series of cell-free access scenarios have been identified in order to frame the related developments carried out in NANCY. MultiRAT selection and coverage expansion are considered in advanced connectivity scenarios by means of a central element designed and implemented in NANCY: The MultiRAT-Nomadic Connectivity Provider (MRAT-NCP). This building block incorporates different components that enrich its functionality. It hosts a decision engine for selecting the most adequate 5G cell to be connected according to QoS considerations. It also provides PC5-based connectivity to remote UEs in order to extend the coverage of a given 5G cell. Besides, it is also capable of handling operations related to the NANCY ID in order to deal with user authentication and authorization processes, in a privacy-preserving way. Furthermore, to speed up these operations in a secure way, it implements a secure data-caching mechanism for storing user-related data. The different blocks and their interactions have been defined in this document, which also presents in-lab implementation results. Even though T4.3's activities come to an end when this report is submitted, its participants will keep working on the advancements made in this task, in order to incorporate and showcase them in the NANCY's demonstrators and in-lab testbeds.

Bibliography

[1] A. Dogra, R. K. Jha, and S. Jain, “A survey on beyond 5G network with the advent of 6G: Architecture and emerging technologies,” IEEE Access, vol. 9, pp. 67512-67547, 2020.

[2] R. E. Ahmed, "A Novel Multi-Hop Routing Protocol for D2D Communications in 5G," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), NV, USA, 2021, pp. 0627-0630.

[3] Z. Yang, Q. Zhang, and Z. Niu, “Throughput improvement by joint relay selection and link scheduling in relay-assisted cellular networks,” IEEE Transactions on Vehicular Technology, vol. 61, no. 6, pp. 2824-2835, 2012.

[4] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," IEEE Communications Magazine, vol. 52, no. 4, pp. 40-48, April 2014.

[5] K. P. Sharmila, V. Mohan, C. Ramesh and S. P. Munda, "Proximity Services based Device-to-Device framework design for direct discovery," 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), 2016, pp. 499-502.

[6] M. Shalaby, M. Shahein, M. Shokair, and A. Benaya, “The Cell-Free Networks Enhancement by Relays Implementation,” International Journal of Telecommunications, vol. 3, no. 1, pp. 1-11, 2023.

[7] Cheng Huang, Bangzhao Zhai, Aimin Tang, and Xudong Wang. "Virtual mesh networking for achieving multi-hop D2D communications in 5G networks." Ad Hoc Networks, vol. 94, p. 101936, Nov. 2019.

[8] S. Ranjan, P. Jha, P. Chaporkar, and A. Karandikar, “A novel architecture for multihop relaying in 3GPP LTE and 5G networks,” IEEE Conference on Standards for Communications and Networking (CSCN), 2019, pp. 1-6.

[9] T. Kerdoncuff, T. Galezowski, and X. Lagrange, “Mobile relay for LTE: Proof of concept and performance measurements,” IEEE 87th vehicular technology conference (VTC Spring), 2018, pp. 1-5.

[10] Q. Li, A. Charaf, N. Gresset, and H. Bonneville, “Radio resource management in next-generation railway system with heterogeneous multi-hop relaying deployment,” Communication Technologies for Vehicles: 16th International Workshop, Nets4Cars/Nets4Trains/Nets4Aircraft 2021, 2021, pp. 59-70.

[11] R. Sanchez-Iborra, L. Bernal-Escobedo, and J. Santa, “Machine learning-based radio access technology selection in the Internet of moving things,” China Commun., vol. 18, no. 7, pp. 13–24, Jul. 2021.

[12] P. Bhanu and J. Malhotra, “iMnet: Intelligent RAT Selection Framework for 5G Enabled IoMT Network,” Wireless Personal Communications, vol. 129, pp. 911-932, Dec. 2023.

[13] M. S. Allahham, A. A. Abdellatif, N. Mhaisen, A. Mohamed, A. Erbad, and M. Guizani, "Multi-agent reinforcement learning for network selection and resource allocation in heterogeneous multi-RAT networks," IEEE Transactions on Cognitive Communications and Networking, vol. 8, no. 2, pp. 1287-1300, Jun. 2022.

[14] T. Omri and R. Bouallegue, "Multi-RAT integration in Heterogeneous Vehicular Communication Networks (HVCNets)," International Wireless Communications and Mobile Computing (IWCMC), 2023, pp. 751-756.

[15] S. Barmpounakis, A. Kaloxylos, P. Spapis, and N. Alonistioti, "Context-aware, user-driven, network-controlled RAT selection for 5G networks," Computer Networks, vol. 113, pp. 124-147, 2017.

[16] T. Lam-Thanh, N. Tan, T. Phuong, D. Tran, and N. Quang-Sang, "Performance statistics of broadcasting networks with receiver diversity and Fountain codes," Journal of Information and Telecommunication, vol. 7, no. 4, pp. 477-493, Jun. 2023.

[17] T. Giannetsos and I. Krontiris, "Securing V2X communications for the future: Can PKI systems offer the answer?," 14th International Conference on Availability, Reliability and Security (ARES), 2019, pp. 1-8.

[18] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," Computer Networks, vol. 169, pp. 107093, Mar. 2020.

[19] M. Jangid, "Towards a tee-based V2V protocol for connected and autonomous vehicles," Workshop on Automotive and Autonomous Vehicle Security (AutoSec), 2022, pp. 1-8.

[20] S. Pinto and N. Santos, "Demystifying ARM TrustZone: A comprehensive survey," ACM Computing Surveys (CSUR), vol. 51, no. 6, pp. 1-36, Jan. 2019.

[21] J. González, P. Bonnet, and L. Bouganim, "Playing attack and defense with trusted storage," IT University Technical Report Series, Feb. 2014.

[22] S. Mahadevegowda, R. Gerdes, T. Chantem, and R. Q. Hu, "Secure CV2X using COTS smartphones over LTE infrastructure," International Conference on Security and Privacy in Communication Systems, 2022, pp. 588-607.

[23] V. Guita, D. Andrade, J. N. Silva, and M. Correia, "Anonymous trusted data relocation for TEEs," IFIP International Conference on ICT Systems Security and Privacy Protection, 2022, pp. 449-466.

[24] P. Lucas, K. Chappuis, M. Paolino, N. Dagieu, and D. Raho, "Vosysmonitor, a low latency monitor layer for mixed-criticality systems on armv8-a," Proceedings of the 29th Euromicro Conference on Real-Time Systems (ECRTS 2017), 2017.

[25] OP-TEE Developers, "About OP-TEE," *OP-TEE Documentation*. [Online]. Available: https://optee.readthedocs.io/en/latest/general/about.html. [Accessed: Nov. 26, 2024].

[26] GlobalPlatform, *GlobalPlatform*. [Online]. Available: https://globalplatform.org/. [Accessed: Nov. 26, 2024].

[27] OP-TEE Developers, "GlobalPlatform API," OP-TEE Documentation. [Online]. Available: https://optee.readthedocs.io/en/latest/architecture/globalplatform_api.html#globalplatform-api. [Accessed: Nov. 26, 2024].

[28] J. Gallego-Madrid, R. Sanchez-Iborra, J. Ortiz, and J. Santa, "The role of vehicular applications in the design of future 6G infrastructures," ICT Express, vol. 9, no. 4, pp. 556–570, Aug. 2023.

[29] R. Zi, X. Ge, J. Thompson, C. -X. Wang, H. Wang and T. Han, "Energy Efficiency Optimization of 5G Radio Frequency Chain Systems," in IEEE Journal on Selected Areas in Communications, vol. 34, no. 4, pp. 758-771, Apr. 2016.

[30] G. Xin, P. Fan, K. B. Letaief, "Semantic Communication: A Survey of Its Theoretical Development," Entropy, vol. 26, no. 2, Jan. 2024.

[31] Arvind Narayanan, Eman Ramadan, Rishabh Mehta, Xinyue Hu, Qingxu Liu, Rostand A.K. Fezeu, Udhaya Kumar Dayalan, Saurabh Verma, Peiqi Ji, Tao Li, Feng Qian, Zhi-Li Zhang, February 11, 2021, "Lumos5G Dataset", IEEE Dataport, doi: https://dx.doi.org/10.1145/3419394.3423629.

[32] I. Sutskever, O. Vinyals, Q. V. Le, "Sequence to sequence learning with neural networks," 28th International Conference on Neural Information Processing System, 2014, pp. 3104 - 3112.

[33] M. T. Luong, H. Pham and M. C.D, "Effective Approaches to Attention-based Neural Machine Translation," Conference on Empirical Methods in Natural Language Processing, 2015.

[34] P. Lucas, K. Chappuis, B. Boutin, J. Vetter, and D. Raho, "Vosysmonitor, a trustzone-based hypervisor for ISO 26262 mixed-critical system," 23rd Conference on Open Innovations Association (FRUCT), 2018, pp. 231–238.

[35] ARM Ltd., "SMC Calling Convention," *ARM Developer Documentation*, DEN0028B. [Online]. Available: https://developer.arm.com/documentation/den0028/b/ARM_DEN0028B_SMC_Calling_Convention.pdf. [Accessed: Nov. 26, 2024].

[36] OP-TEE Developers, "Secure Storage," *OP-TEE Documentation*. [Online]. Available: https://optee.readthedocs.io/en/latest/architecture/secure_storage.html. [Accessed: Nov. 26, 2024].