frontiers | Frontiers in Future Transportation

ORIGINAL RESEARCH
published: 11 July 2022
doi: 10.3389/ffutr.2022.911923

Cooperative, Connected and Automated Mobility Service Continuity in a Cross-Border Multi-Access Edge Computing Federation Scenario

Seyed M. Hosseini[1], Mohannad Jooriah[1], David Rocha[1], João Almeida[1], Paulo Bartolomeu[2], Joaquim Ferreira[3], Carlos Rosales[4] and Marta Miranda[4]*

[1]Instituto de Telecomunicações, Universidade de Aveiro, Campus Universitário de Santiago, Aveiro, Portugal, [2]Instituto de Telecomunicações, Departamento de Eletrónica, Telecomunicações e Informática, Universidade de Aveiro, Campus Universitário de Santiago, Aveiro, Portugal, [3]Instituto de Telecomunicações, Escola Superior de Tecnologia e Gestão de Águeda, Universidade de Aveiro, Campus Universitário de Santiago, Aveiro, Portugal, [4]Centro Tecnológico de Automoción de Galicia (CTAG), Polígono Industrial A Granxa, Pontevedra, Spain

The paradigm shift in transportation systems towards *Cooperative, Connected and Automated Mobility* (CCAM) aims to improve vehicle maneuverability, reduce pollution, and increase safety. CCAM is primarily responsible for ensuring the best mobility environment, making it one of the main trends in the automotive industry. However, taking advantage of CCAM in *Cross-Border Corridors* (CBCs) faces many challenges, which go beyond infrastructure deployment cost, and all of which are related to supporting *Service Continuity* (SC) for mobile users, especially in light of the diversity of territories, network coverage areas, international roaming agreements, and type of cooperative maneuvers. As a solution to these challenges, the paper proposes and implements a new architecture for CCAM SC in CBCs that combines a federation of *Multi-access Edge Computing* (MEC) concepts to maintain SC.

Keywords: cooperative, connected and automated mobility, 5G for CCAM, service continuity in cross-border corridors, multi-access edge computing, MEC federation, inter-PLMN handover, home routed vs. local breakout roaming

OPEN ACCESS

Edited by:
Jianhua He,
University of Essex, United Kingdom

Reviewed by:
Mohammad Reza Jabbarpour,
Niroo Research Institute, Iran
Sebastian Euler,
Ericsson, Sweden

****Correspondence:***
João Almeida
jmpa@ua.pt

Specialty section:
This article was submitted to Connected Mobility and Automation, a section of the journal Frontiers in Future Transportation

Received: *03 April 2022*
Accepted: *21 June 2022*
Published: *11 July 2022*

Citation:
Hosseini SM, Jooriah M, Rocha D, Almeida J, Bartolomeu P, Ferreira J, Rosales C and Miranda M (2022) Cooperative, Connected and Automated Mobility Service Continuity in a Cross-Border Multi-Access Edge Computing Federation Scenario. Front. Future Transp. 3:911923. doi: 10.3389/ffutr.2022.911923

1 INTRODUCTION

The automotive industry is moving towards a vision in which vehicles are increasingly automated and connected Llopis-Albert et al. (2021). As the demand for more connectivity increases; what is expected from a vehicle has essentially evolved from a device used only to transport people from *A* to *B* to a fully automated vehicle capable of sensing its environment, potentially reducing accidents, preventing injuries, and saving lives and the environment Krishna et al. (2021). Hence, *Cooperative, Connected and Automated Mobility* (CCAM) is designed to support the automotive industry in the direction and vision of connected and automated driving. CCAM shifts the mobility pattern towards *Mobility-as-a-Service* (MaaS) to unify multiple methods of transport services into a single mobility service accessible on demand Alonso Raposo et al. (2018). However, the CCAM vision is only achievable if there are harmonized solutions that support automated cooperation, connectivity, and mobility in *Cross-Border Corridor* (CBC) for *User Equipment* (UE) (e.g., an automated vehicle). More precisely, when a UE crosses the border of a country, it needs to be constantly connected to the

TABLE 1 | List of acronyms.

CAM	Cooperative awareness message
CBC	Cross-Border Corridor
CCAM	Cooperative, Connected, and Automated Mobility
C-ITS	Cooperative Intelligent Transportation System
CPM	Collective Perception Message
CPS	Collective Perception Service
DC	Data Center
DENM	Decentralized Environmental Notification Message
E2E	End-to-End
GNSS	Global Navigation Satellite System
HO	Hand-Over
HR	Home-Routed
IoT	Internet of Things
LBO	Local Break Out
M2M	Machine-to-Machine
MaaS	Mobility-as-a-Service
MEC	Multi-access Edge Computing
MNO	Mobile Network Operator
MQTT	Message Queuing Telemetry Transport
NSA	Non-Standalone
NTP	Network Time Protocol
OBU	On-Board Unit
PDR	Packet Delivery Ratio
PLMN	Public Land Mobile Network
QoE	Quality of Experience
QoS	Quality of Service
RSU	Road-Side Unit
SC	Service Continuity
TCP	Transmission Control Protocol
TS	Trial Site
UDP	User Datagram Protocol
UE	User Equipment
uRLLC	ultra-Reliable Low-Latency Communication

network to exchange data about its critical information and consume dedicated services (e.g., road status, media streaming), by switching to another *Public Land Mobile Network* (PLMN), possibly from a different *Mobile Network Operator* (MNO) that belongs to a different country.

The CCAM operation must be carried out in a way that satisfies the strict requirements of the corresponding services in terms of latency and privacy. From this point of view, three main quality requirements are mandatory for the CCAM Service Continuity (SC):

- ***Low Latency***, due to the nature of the service. To address this requirement, all services required by the vehicle will be deployed on the *Multi-access Edge Computing* (MEC) devices to offer cloud computing capabilities at the edge of the network and, therefore, in close proximity to the mobile devices Porambage et al. (2018).
- ***Availability***, to make sure that the services can process the UE's data at any point of the vehicle journey. To comply with the availability, the provided services need to move from one MEC to the others. In other words, services need to follow the vehicle as it moves **Table 1**.
- ***Cybersecurity***, including data security and access control to ensure the safe and secure operation of CCAM vehicles and mobility systems, while executing the needed services. To meet this need, the system needs a harmonized approach and tools to ensure that only authorized users are able to access and invoke services at the same time.

According to the above, we propose a CCAM architecture implemented on top of the 5G infrastructure and MECs to meet the stated requirements. 5G, which is the fifth generation technology standard for broadband cellular networks, brought significant advances to the various domains of mobile communications, such as public transport, public safety, and automotive Ahmad et al. (2020). 5G not only supports communication, but also increases *Quality of Experience* (QoE) and *Quality of Service* (QoS) for mobile entities (users/devices) Mao et al. (2017). Thanks to the *ultra-Reliable Low-Latency Communication* (uRLLC) currently available on 5G, it is possible to enable seamless services that have strict reliability (e.g., 99.999%) and latency requirements (e.g., 1ms) Popovski et al. (2018). However, providing CCAM capability on 5G and MECs goes through a series of challenges that clearly go beyond infrastructure deployment costs, and all of which are related to supporting the continuity of service, i.e., the uninterrupted user experience of a service 3GPP (2020).

In the following, we briefly highlight the main contributions of this paper:

- Design and implementation of a seamless architecture for the CCAM SC in border areas, especially in *Portugal-Spain Trial Site* (PT-ES TS), based on the 5G features and MEC concept.
- Introduce a reliable authentication method to build mutual trust for MEC Interconnection.
- Provide an experimental evaluation of the proposed architecture in a real-world environment by comparing the observed latency values in a single PLMN scenario with the inter-PLMN Handover (HO) in *Home-Routed* (HR) roaming configuration.

The rest of the paper is structured as follows: **Section 2** focuses on the background by reviewing several recently published works and projects. **Section 3** presents the proposed architecture of the CCAM system, which includes the deployment scenario, inter-PLMN handover, and MEC federation strategy. **Section 4** examines the security implementation of the proposed architecture. Performance evaluation and results dissection are presented in **Section 5**. Finally, **Section 6** concludes this paper with a summary of its contributions and conclusions.

2 BACKGROUND

Minimizing delays and maintaining service continuity during the handover process to achieve better performance for mobile users has attracted the attention of many researchers and organizations in the domain of telecommunications and mobile communications Chipta et al. (2021); Safa Abd ELWahab and Abbas (2020); Rahman et al. (2019); Lal et al. (2017); Pomalo et al. (2020). In this context, continuity enables services to "follow" their respective UEs/users during their journey by migrating all (or portions) of services to the optimal radio base station node, for example, NodeB and eNodeB in

3G/4G and gNB and ng-eNB in 5G, ensuring them the best QoE and QoS in heterogeneous environments Sultan et al. (2021).

Follow Me Cloud (FMC) has been introduced by Taleb and Ksentini (2013) to solve the problem of service continuity between a distributed MNOs and a network of regional *Data Centers* (DC) on 4G/LTE networks. In the FMC, service migration and continuity are supported by replacing IP addressing with service identification. However, the migration of IP services due to movement of the receiving UE is followed by a change in its IP address, resulting in a session break and the need to establish a new one. To engage 5G with FMC, Aissioui et al. (2018) proposed the *Follow Me edge-Cloud* (FMeC) concept based on MEC architecture with mobility services to sustain requirements of the 5G automotive systems. Assuming that automotive services are deployed on MEC entities, FMeC ensures low-latency access to these services by guaranteeing that the UE on vehicles always connects to the nearest automotive service instance.

To support service continuity on the federated MEC infrastructure for resource-constrained devices (limited processing and storage capabilities), Farris et al. (2017) designed a container-based framework for MEC environments that guarantees a fast response time. In this framework, services can be run quickly and confidently from one computing environment to another due to the packaging of the code and all its dependencies in the container. Based on their evaluation, the *Total Migration Time* (TMT), which is described as the total time it takes a user to move to a different MEC/AP and access to the new node for the same service instance deployed in the previous serving edge node, is between 1 and 15 s, depending on the applications and equipment. By using Lyapunov's method, Labriji et al. (2021) answers the question of when and where computing services (virtual machines, VMs) that run on MECs should be migrated to ensure the continuity of vehicle service and, at the same time, reduce energy costs. This is important because the right choice can save up to 50% of energy expenditure, according to their reports.

To take advantage of blockchain, as an emerging distributed network architecture for service continuity in inter-MEC scenarios, several schemes have been proposed. El Ioini and Pahl (2018) proposed a container-based edge architecture based on a permissioned blockchain that uses the *W3C-PROV 5* data model of Belhajjame et al. (2013) to track the identities and provenance of all orchestration decisions of a business network. In this regard, containerization separates hardware resources from software solutions that allow packaged software to run on top of multiple hardware architectures Morabito (2017). In this context, Pahl and El Ioini (2019) introduced a secure edge management architecture to operate in untrusted environments, where the MEC providers might know each other. The proposed architecture allows the development of a distributed network of non-federated large-scale MEC infrastructure relying on two main tec hnologies: container technology for managing service deployment and blockchain for access control to the MEC assets.

To enhance the security and privacy of entities and MEC servers, authenticated users should be the only ones who have access to their respective stored data. In this regard, Bonnah and Shiguang (2020) introduced *DecChain*, a fully decentralized scheme against man-in-the-middle and playback attacks based on permissioned blockchain technology to improve the privacy preservation and authentication process. In their design, each entity must be identifiable by a selected identity or by a public key. To have a secure task collaboration mechanism between edge servers in a MEC environment, Rivera et al. (2020) proposed a permissioned blockchain scheme to enable secure task sharing in MEC based on *Hyperledger Fabric* blockchain, an umbrella of open source blockchains and related tools. Within their proposal, Hyperledger is used to add a security level to the task sharing/offloading processes among MEC servers.

Although the above solutions address various aspects of MEC service continuity, they cannot be considered as a viable solution for CCAM SC in cross-border areas, where MECs are dominated by different networks/countries, and the interconnections between them require a comprehensive platform. Therefore, EU has represented many funding opportunities for projects such as 5G-CARMEN, 5G-CroCo, and 5G-MOBIX, "to develop and test automated vehicle functionalities using 5G core technological innovations along multiple cross-border corridors and urban trial sites, under conditions of vehicular traffic, network coverage, and service demand, as well as considering the inherently distinct legal, business and social local aspects". However, the works published in the form of these projects still have open questions. For example, Hamid and *et al.* Barzegar et al. (2020) in the context of the 5G-CARMEN project explored the feasibility of SC for CCAM based on simulation. Although they have stated that the platform they have designed is a viable solution for continuing services in border areas, the following issues have not been addressed:

- A proper MEC selection in the CBCs to fulfil the latency requirements.
- Interconnection between MEC nodes, which are deployed on different MNOs' infrastructures in a cross-border scenario, regarding the security and latency requirements.
- Registration and identification to ensure that all communications between the UEs and MEC nodes are encrypted and that the UEs are able to connect to different MEC nodes that may belong to different MNOs.

In the proposed architecture, the above gaps are filled by monitoring messages transmitted by the mobile stations, using MQTT brokers to exchange messages across different MEC nodes, and assigning unique identifiers to all entities, respectively. Details are described in the next section.

3 COOPERATIVE, CONNECTED AND AUTOMATED MOBILITY SYSTEM ARCHITECTURE FOR 5G SERVICE CONTINUITY

Implementing and deploying a CCAM system requires a comprehensive architecture that incorporates the various components of the system, which eventually leads to the production of a *Cooperative Intelligent Transport System* (C-ITS). Achieving such a comprehensive architecture requires

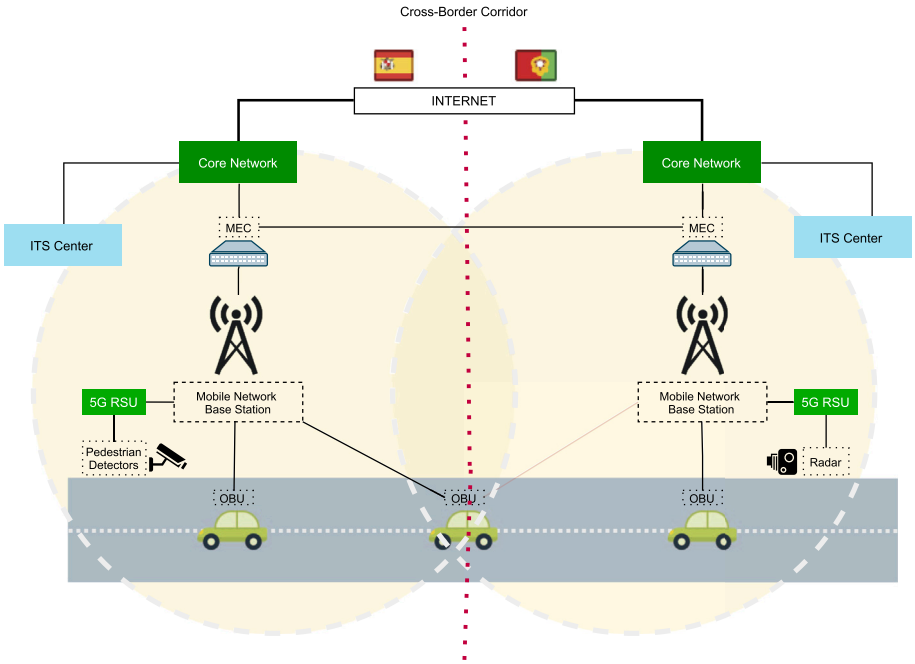

FIGURE 1 | Overview of CCAM infrastructure components at PT-ES CBC.

numerous standards ranging from hardware design to software development. With the sole purpose of providing an architecture for the continuation of CCAM services in CBCs, this section details the proposed architecture which is implemented through the *Portugal-Spain* (PT-ES) corridor.

The devised architecture uses a direct MEC connection between different MNOs, which provides fast authentication and authorization procedures when roaming from one cellular network to another (to meet the latency requirements of the CCAM system). Additionally, it provides a new registration and identification method for ensuring encrypted communications between UEs and MEC nodes. The rest of the section is as follows: First, it presents the deployment scenario, including the used hardware, software, and standards, and then explains the proposed architecture and how it handles the CCAM SC in a cross-borders.

3.1 Deployment Scenario

The deployment scenario is derived from the 5G-MOBIX project and has been developed from scratch, which includes the development and provisioning of software packages and procurement of hardware equipment to fulfill the SC along cross-borders using 5G core technological innovations. A collection of hardware elements that have been set up on the PT-ES border is depicted in **Figure 1** and listed below:

- ***5G RSUs*** (Road-Side Units), which are used as a connection link for sensors and devices, such as radars, cameras, or pedestrian detectors, to equip them with 5G capabilities. An RSU uses sensors data to produce *Collective Perception Message* (CPM) in order to share information about objects within its scope with other road users.
- ***ITS Centers*** are used as cloud ITS platforms with different objectives: to monitor connected vehicles; to generate road events and notify connected vehicles about them; and to generate and update the vehicle's *High Definition* map (HD map). The cloud platform (hardware and software) is provided by several partners: A-to-Be, CTAG, and *Infrastruturas de Portugal*.
- ***OBUs*** (On-Board Units), are in-vehicle devices responsible for providing ITS services to vehicles by interacting with the other active elements of the ITS. An OBU mainly shares periodic *Cooperative Awareness Messages* (CAM) and event-driven *Decentralized Environmental Notification Messages* (DENM), and receives the CPMs, HD maps, CAMs, and DENMs sent by other vehicles and devices.
- ***MECs*** are used to enable cloud computing capabilities at the edge of MNOs to provide rich computing resources for mobile users. A set of services is installed on the MECs, which are discussed next.
- ***Core Networks*** support user's mobility between the two networks across the border.

In addition to the above hardware, a set of tools and standards is used:

- ***MQTT Broker***: Almost all communication between the above hardware and devices is done through a lightweight messaging broker that implements the *Message Queuing Telemetry Transport* (MQTT) protocol and is therefore called the MQTT broker. MQTT is designed for constrained devices and low-bandwidth, high-latency, or unreliable networks. The design principles are to minimize

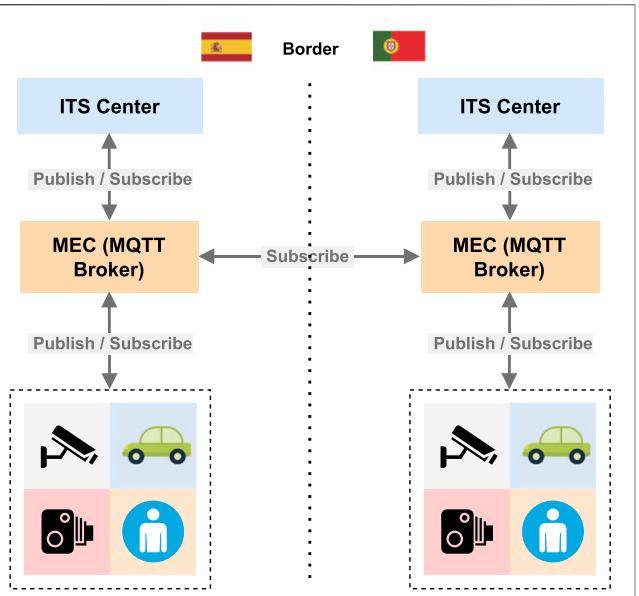

FIGURE 2 | Overview of the MQTT broker in the implemented scenario.

network bandwidth and device resource requirements while ensuring reliability and delivery assurance. These principles also make the protocol ideal for *Machine-to-Machine* (M2M), *Internet of Things* (IoT), and *Industrial IoT* (IIoT) devices where bandwidth and battery power are at a premium. The MQTT broker uses a topic-based publish/subscribe model to connect interested parties to each other, where a sender publishes messages on a topic (UTF-8 string) and a receiver needs to subscribe to that topic to receive the message (topic acts as a filter for messages). **Figure 2** illustrates an overview of MQTT broker in the implemented scenario.

- ***Localization***: To ensure that the messages are sent only to the relevant devices, a topic structure consisting of a quadtree path based on *Spherical Mercator* projection is used to indicated a specific area, named a **tile**[1]. This structure enables the system to calculate the relevant geographic tiles for a specific location based on the latitude and longitude values. As an example, **Figure 3** shows the world divided into four tiles/squares on the left, corresponding to zoom level 1, and level 2 on the right, where the four initial tiles are again divided into four smaller squares, resulting in a total of 16 tiles. This process is repeated the number of times necessary to obtain the desired zoom level (localization accuracy). For interurban environments, a smaller zoom level is often more convenient, as the vehicle speed is usually higher. In contrast, the zoom level increases for urban areas (smaller quadtree size); thus, the number of messages spread in that area is reduced, as well as the number of messages received and processed by vehicles. Since the deployment scenario is in an interurban environment, a tile structure with a zoom level of 18 is considered, corresponding approximately to a 150 meter tile size. Based on this structure, we define the topics for communications as follows:

its center/ < message direction > / < message type id > / < tile > / < sender id >

In the above structure, *its_center* is a fixed string at the beginning of the topic to distinguish ITS messages from other possible messages in the broker; *message_direction* can be *inqueue* for messages published from ITS stations to the broker and *outqueue* for messages published by the broker and intended to the ITS stations; *message_type_id* defines the type of message, for example *Cooperative Awareness Message* (CAM), *Collective Perception Message* (CPM), and *Decentralized Environmental Notification Message* (DENM); *tile* presents the quadtree path of the sender; and *sender_id* is the unique numeric identifier of the sender. An actual topic for a CAM message published to the broker by an OBU with station ID equal to 3306 using zoom level 18, would look like:

its center/inqueue/cam/0/3/3/1/1/0/0/1/1/3/0/3/0/1/3/3/0/1/3306

- ***CAM Message***: The standard CAM is one of the reference architecture components for road users and roadside infrastructure defined by the *European Telecommunication Standards Institute* (ETSI) for transmitting geographically aware information about each other's position, dynamics, and attributes ETSI (2014). Hence, the vehicle (OBU) continuously transmits CAM messages to the current tile, that it is inside, and subscribes to its tile and all the surrounding ones, allowing the location of the vehicles to be determined so that the ITS center (MNO cloud) and other vehicles can take the necessary actions.
- ***CPM Message***: A technical report recently approved by ETSI defines the *Collective Perception Service* (CPS), including standardizing the format and generation rules of *Collective Perception Messages* (CPMs) ETSI (2019). CPMs contain information about the objects detected by an ITS station's sensors with adequate confidence. In the proposed architecture, an RSU equipped with a traffic radar generates and publishes CPM messages to the MQTT broker to be consumed by all ITS stations subscribing to the relevant topics.

All the aforementioned components are used to accomplish the following scenario: "maintaining continuity of service (in particular, MQTT service) for vehicles (OBUs) crossing the PT-ES border during an inter-Public Land Mobile Network (PLMN) handover (cross-border) and roaming including the case where the PLMNs involved are operated by different MNOs (NOS and Telefónica)".

3.2 Inter-Public Land Mobile Network Handover and Multi-Access Edge Computing Interconnection Proposed Architecture

Roaming services allow users to access mobile network services outside of their home network areas and countries under roaming

[1]https://www.maptiler.com/google-maps-coordinates-tile-bounds-projection

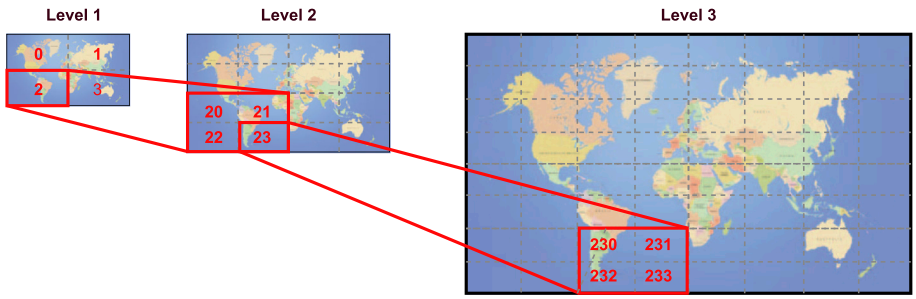

FIGURE 3 | Tiling Structure.

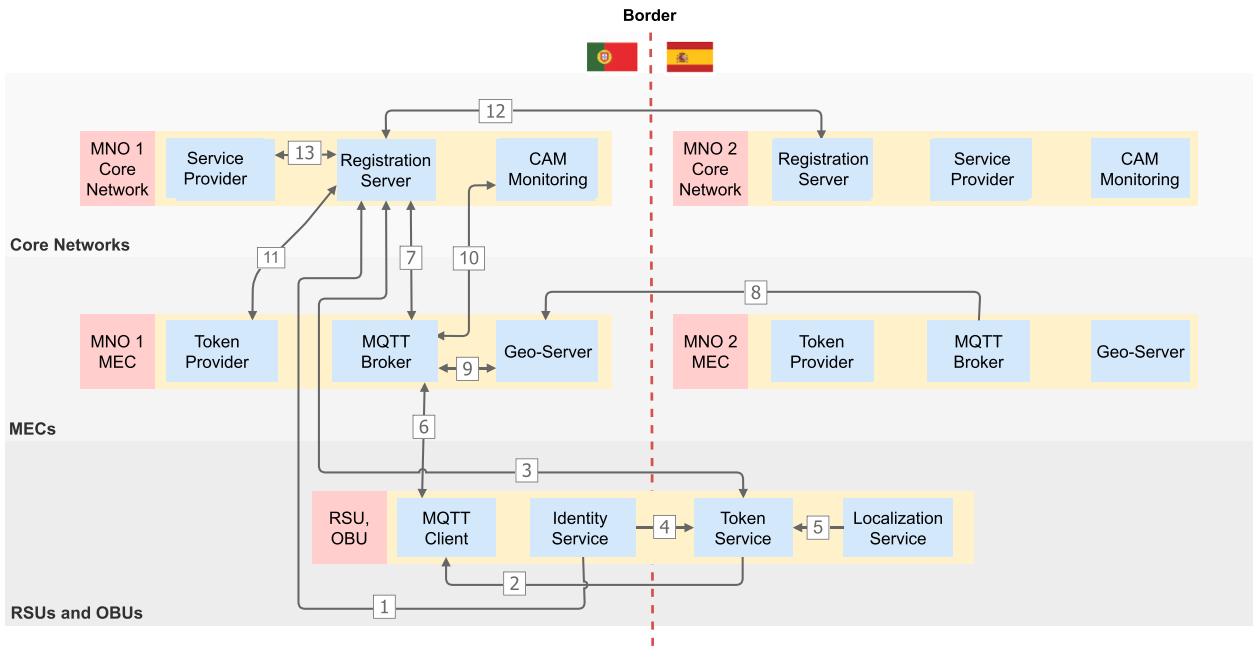

FIGURE 4 | Proposed architecture for CCAM SC in CBCs.

agreements between network operators. The access policies of roaming services determine two types of supported roaming modes:

- ***Home-Routed*** (HR) where the mobile terminal accesses the visited network through *Packet Data Network Gateway* (PDN-GW) of its home network and continues to use the services provided by the home network. This roaming solution is dominant in commercial networks and is also used in the proposed architecture.
- ***Local Break Out*** (LBO) where the mobile terminal accesses the visited network through the PDN-GW of the visited network and uses its services in addition to the services of the home network.

HR or LBO roaming combined with the seamless Inter-PLMN S1 handover using the S10 interface at the network level Kakes et al. (2022), allows the connection continuity between the OBU and the MQTT broker of the home network throughout the border zone (in case of HR) or a transparent new connection to the visiting network's MQTT broker at the applications layer of the OBU device (in case of LBO). The diagram in **Figure 4** illustrates the proposed architecture for the described scenario, which includes components at three different levels:

3.2.1 Road-Side Unites and On-Board Units

The OBUs and RSUs are at the lowest level and send and receive messages continuously. They consist of the following components:

- ***IdentityService***: All OBUs and RSUs need a unique identity to communicate with others. Therefore, this component is responsible for creating and storing a unique identity. It should be noted that the identity is sent to the *Registration Server* inside the *Core Network* after creation for future use (1). Its implementation is stated in **Section 4**.
- ***Token Service***: This component is responsible for providing tokens for *MQTT Client* (2) on the device by sending a token request to *Registration Server* (3), including the identity of the entity (4) and the location of the vehicle (5).
- ***Localization Service***: This component is located in OBUs and RSUs to translate vehicles' and RSUs' coordinates to the corresponding tile and as well finding the adjacent tiles. This information is included in the token request whenever the *Token Service* requests a new token from the *Registration Server*.
- ***MQTT Client***: This component is placed on all devices and runs an MQTT client instance to connect to the MQTT broker (6) on the MEC based on URL or IP address, port, and a credential (or token), with the responsibility for subscribing and publishing messages in the desired geographical tiles.

3.2.2 Multi-Access Edge Computing

On the MEC node, a *MQTT Broker* is deployed, as well as a *Token Provider* for MQTT authentication and a *Geo-Server*, responsible for geographic dissemination of messages and interconnection with the broker running in the MEC from the other MNO:

- ***MQTT Broker***: This component is deployed on the MEC and almost all communications are done through it. Access to the broker requires a valid token and identity. Therefore, when it receives a connection request, it first checks the identity and token through *Registration Server* (7), and if the authentication is successful, allows the *MQTT Client* to send and receive messages.
- ***Geo-Server***: The component acts like an MQTT Client, subscribing to a specific topic (*inter_mecs*) in another MQTT broker (8), and whenever a message is received, it publishes that message in the MQTT broker running on its MEC environment with a different topic structure (*outqueue*) (9). It also republishes the messages sent to the co-located MQTT broker, from the *inqueue* to the *outqueue* topics.
- ***Token Provider***: After the *Registration Server* receives a token request and confirms the sender, it sends a request to the *Token Provider* located in the target MEC node. This component issues a new token in a secure way and forwards it to the registration server (11).

3.2.3 Core Networks (5G)

It is the responsibility of the core networks to establish reliable and secure connectivity to the network for MECs and end users in order to enable them to access services. This level includes the following components:

- ***CAM Monitoring***: This component is a part of the *MNO Core Network* and acts like an *MQTT Client*, where it subscribes to the following topic for detecting vehicles' locations and publishing some notification messages to them if needed (10). These messages are related to requests for new tokens and are issued when the device is in a border environment. The # at the end of the topic is a *wildcard* that allows the service to subscribe to multiple topics simultaneously.

its_center/inqueue/cam/#

- ***Registration Server***: As mentioned above, when a service or device needs to subscribe/publish a message to the MQTT server, it needs a valid token. For this purpose, the registration server is designed to provide valid tokens by forwarding the request to *Token Provider* if the authentication process is completed (11). There is a mutual connection between *Registration Servers* located in different MNOs' networks, that allows them to share tokens if needed (12). It should be noted that each Registration Server is connected to a database in which the identities, tokens and information of the entities are stored. The statelessness of the Registration Servers from MECs guarantees that it can be easily scaled up.
- ***Service Provider***: The *Registration Server* is in contact with the *Service Providers* to receive information about the requested service/topic or to confirm the identity if needed (13). It is important to note that all the topics that an entity can access have been predefined on the *Registration Server*. In other words, each topic is associated with a particular *Service Provider*, and every time a request for access to a topic is received, the *Registration Server* sends a request to the *Service Provider* to confirm the access to the requested topic by the entity.

As shown in **Figure 5**, to build a mutual authentication method in CBCs, the proposed method follows these steps: 1) The vehicle starts in the Portuguese area and makes a token request to the Portuguese Registration Server. 2) The Portuguese Registration Server returns an array of tokens that includes the connection information to the Portuguese MQTT Broker. 3) The vehicle establishes the connection with the Portuguese Broker and subscribes to the notification channel "notification/vehicleID". The MQTT broker is always connected to the Registration Server in the MNO's core network, in order to check the validity of the token. Furthermore, the CAM Monitoring service is always connected to the MQTT Broker in order to monitor the vehicle's location through the position extracted from the CAMs (these messages are constantly sent to the MQTT broker by the vehicle). When the vehicle enters the cross-border area, the CAM Monitoring service realizes that the vehicle has entered the predefined border zone and issues a notification to the vehicle 4) using the "notification/vehicleID" topic, informing that it must make a new token request. In step 5) the vehicle sends a new token request to the Portuguese Registration Server and in 6) and (7), the Portuguese Registration Server makes a new token request to the Spanish Registration Server, which returns a token that allows the vehicle to connect to the Spanish MQTT broker. 8) The Portuguese

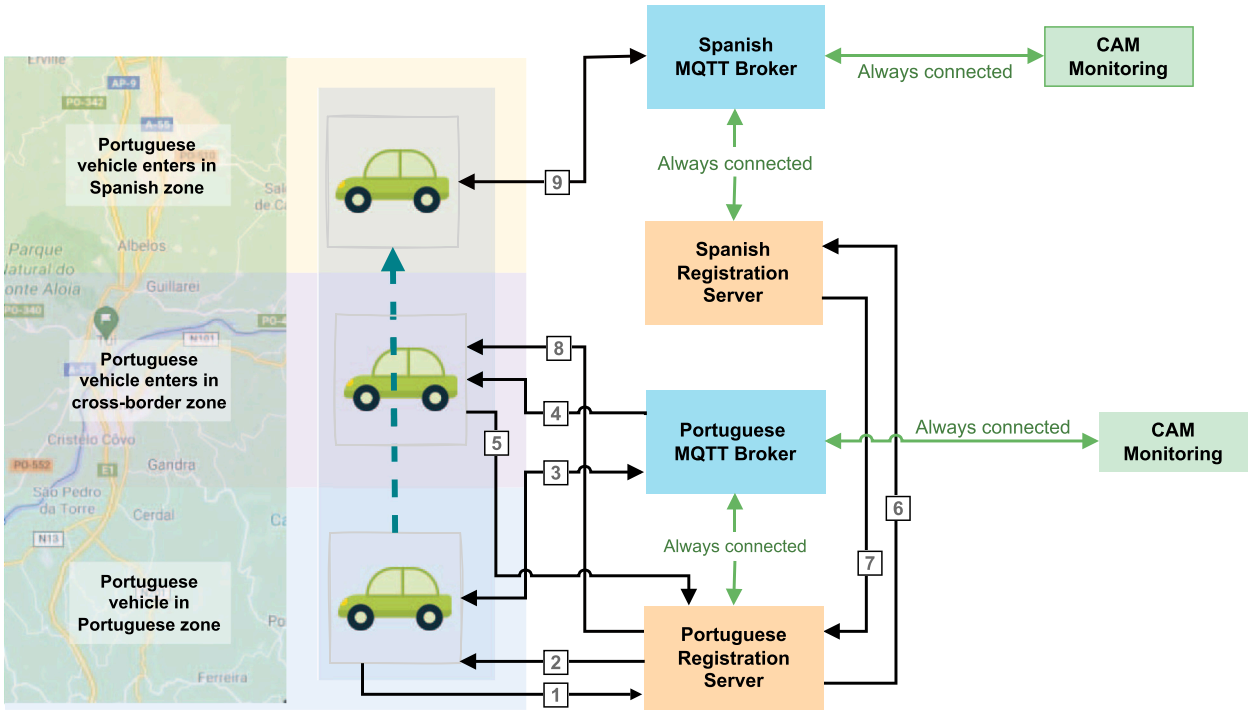

FIGURE 5 | Mutual authentication approach for Inter-PLMN Handover and MEC Interconnection.

Registration Server returns an array of tokens that includes the connection information of the Portuguese and the Spanish MQTT Brokers, with their respective GPS and CellId zones. 9) When the vehicle enters the Spanish area, it can use the token received from the previous step to connect to the Spanish MQTT Broker, in order to receive and publish messages.

The described architecture provides a concrete solution for the problem of inter-PLMN handover in cross-border areas, which is critical for the provision of low-latency and high-reliability applications such as CCAM services. The existing work on 5G for CCAM support doesn't appropriately address this roaming issue, so the novelty of this proposal relies on tackling the required inter-PLMN mobility by designing and implementing a real-time and secure message exchange mechanism across MEC nodes from different MNOs. As reported, real-time monitoring of the devices' mobility is introduced in order to anticipate the need of network handover, thus minimizing the interruption time and the end-to-end latency of the communications by selecting the closest MQTT broker/MEC node for message exchange. The authentication and authorization aspects of OBUs' and RSUs' communications are also carefully handled in the proposed architecture and will be described in more detail in the next section.

4 SECURITY IMPLEMENTATION

As CCAM builds an inclusive internet-based mobility system, all relevant operations must be sufficiently secure against cyber attacks. This subject becomes important where any failure in the system causes harm to citizens and the environment, leading to distrust in CCAM solutions and damaging the reputation of manufacturers. Consequently, aspects of cyber security should be considered at all levels of the CCAM ecosystem El-Rewini et al. (2020); Centenaro et al. (2020). Various reference standards for security requirements and security threats for road vehicles have been developed by institutions and associations around the world, such as *Society of Automotive Engineers* (SAE) Int (2021), *United Nations Economic Commission for Europe* (UNECE), and *European Telecommunications Standards Institute* ETSI (2020) (ETSI). These standards specify the security and privacy requirements of the entities involved in CCAM services, where all entities (OBUs, RSUs, MECs, ITS centers, etc.) must be identified. This means that every entity needs a unique identity.

Identity is crucial for the authentication of all objects, which allows the system to control the access assigned to each object before granting entities access to services/resources, thus building trust between different objects and edge infrastructures. In addition, the heterogeneous nature of the MEC infrastructure requires multilevel access along with seamless usage and continuity of services between them.

To meet the need for identity, the proposed architecture creates identities based on an *Asymmetric/Public-key Cryptography* mechanism, where each pair consists of a public key and a private key. The private key remains stored on the device and is only accessible by that device, and the ***identity*** is a part of the Base64 encoded public key, consequently, it will be a string that complies with the Base64 coding rules. To further

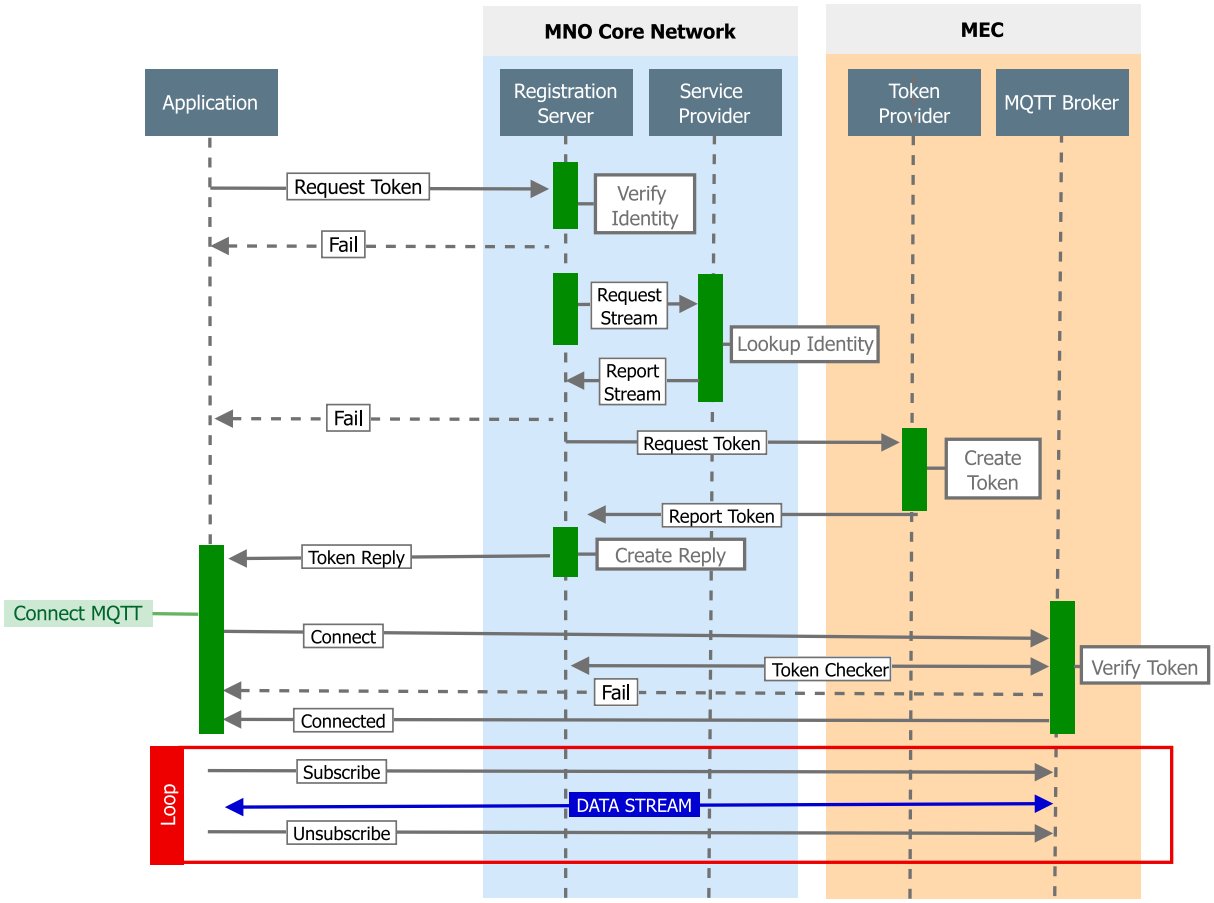

FIGURE 6 | Authentication and Authorization processing in the proposed architecture.

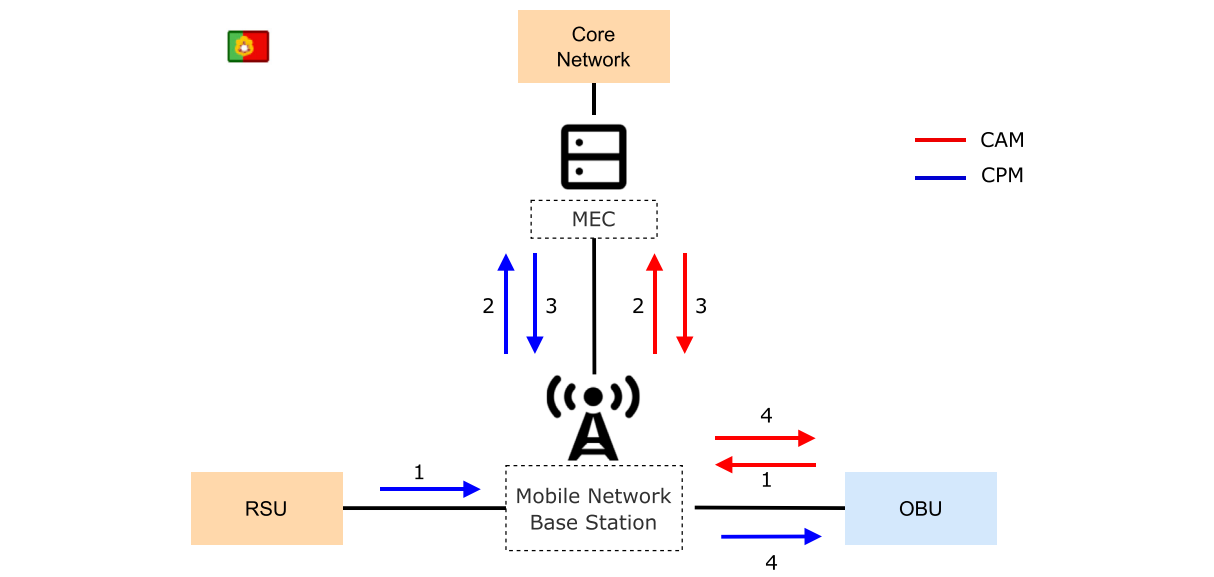

FIGURE 7 | CPM and CAM packets flow in the Single PLMN Scenario.

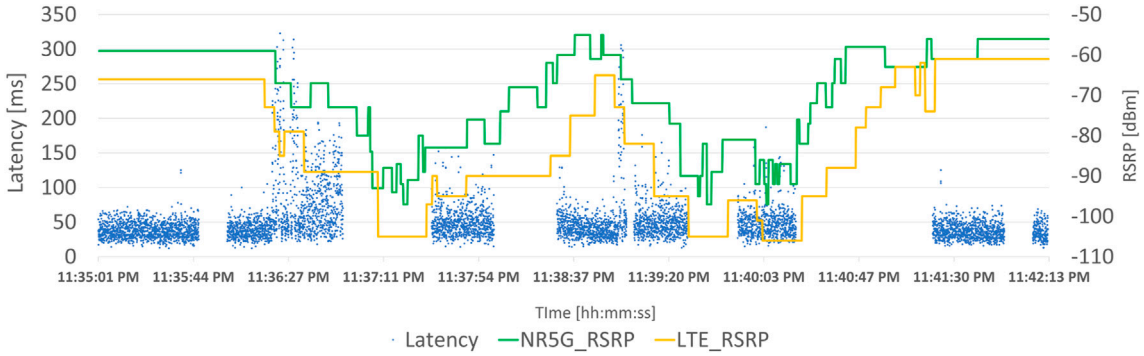

FIGURE 8 | Single PLMN Scenario: CPM latency and RSRP values for LTE and 5G NR signals.

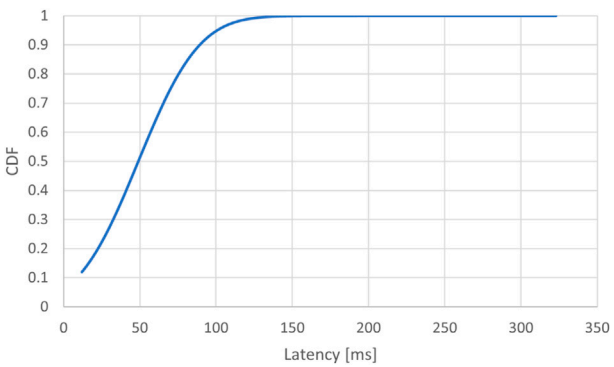

FIGURE 9 | Single PLMN Scenario: cumulative distribution of CPM latency.

support hardware devices, the following asymmetric encryption parameters apply to the identity key pair:

- Algorithm: *Elliptic Curve Digital Signature Algorithm (ECDSA).*
- Parameters: *NIST curve P256.*
- Hash used for signatures: *SHA256.*

Figure 6 presents the authentication and authorization processing in the proposed architecture. According to the scenario described, when an entity wants to access data streams of MQTT Broker (service) on the MEC to publish or subscribe to a topic, the system must ensure that the request is sent by a legitimate entity. In the proposed architecture, the authentication process is performed by a *Registration Server* (RS) located in the infrastructure. Technically, the RS is implemented as a RESTful HTTPS server to ensure that all communication between the applications and the RS is encrypted (the SSL/TLS certificate is installed on the RS). Subsequently, the RS authenticates the user's identity, and sends a stream request to the desired *Service Provider* (SP), which in our scenario is MQTT service provider. The SP looks up the identity and authorizes the device to subscribe or publish to a number of MQTT topics. If all the above steps are successful, the RS sends a token request to *Token Provider* (TP), which is placed in the MEC infrastructure. Finally, after the token is created, RS sends the token to the application, by which it is able to connect to the service. Each time the application loses connection, it checks whether the token is still valid, and if not, the above procedure must be repeated.

5 TESTS AND EVALUATION RESULTS

With the main goal of evaluating the performance of the proposed architecture in a real-world scenario, trials were conducted in the field under the presence of inter-PLMN handover events while crossing the border between two countries (Portugal and Spain). The main objective is to evaluate the service continuity of CCAM applications in these roaming scenarios, and for that purpose, the mobility interruption times and latency values of exchanged messages were tracked and analyzed to observe the impact of the HO events in the CCAM communications among vehicles' 5G OBUs and RSUs.

A first version of this system was deployed and is being evaluated within the scope of the 5G-MOBIX project. Currently, the HR roaming scenario is configured and operates by maintaining the connection to the MEC MQTT broker hosted on the outgoing MNO. In this case, the OBU devices inside the vehicles are always connected to the MEC MQTT broker of the corresponding home network, even if they are roaming in a visited network. This means, for example, that if the OBU in the vehicle is using a Spanish SIM card, it will always be connected to the Spanish MQTT broker, even when attached to the network of the Portuguese MNO. The performance assessment of this scenario is highly relevant because its conclusions will contribute to designing more advanced scenarios, such as the LBO configuration where vehicles will change the IP address and establish a new connection to the MEC MQTT broker hosted in a different MNO. This LBO scenario is programmed to be configured during 2022, which will allow the evaluation of the full authentication approach and security implementation in an inter-MEC roaming scenario.

The tests were performed on the border between Portugal and Spain, under the coverage of two *Non-Standalone* (NSA) 5G

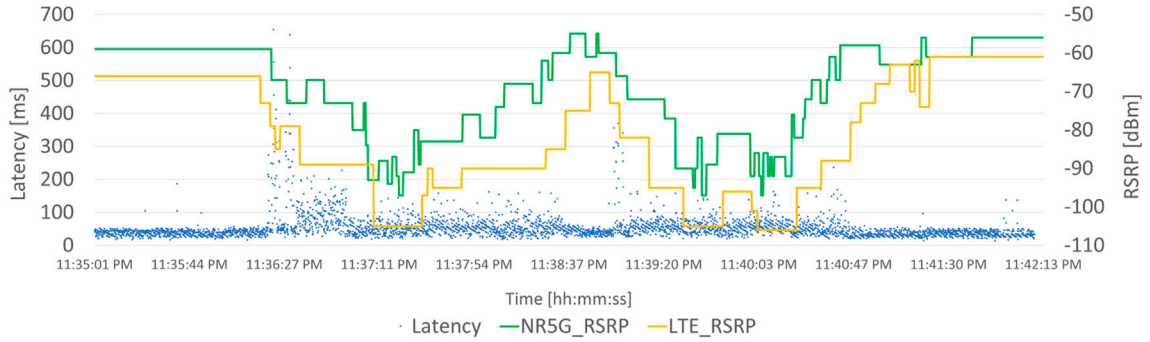

FIGURE 10 | Single PLMN Scenario: CAM latency and RSRP values for LTE and 5G NR signals.

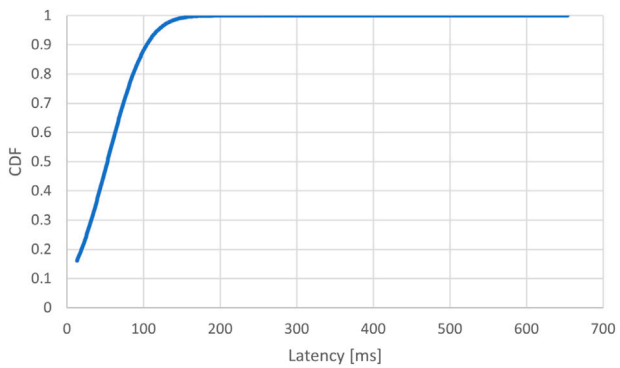

FIGURE 11 | Single PLMN Scenario: cumulative distribution of CAM latency.

TABLE 2 | Summary of the latency measurements for the Single PLMN Scenario.

Message type	Min (ms)	Mean (ms)	95%ile (ms)	Max (ms)
CPM	12.0	49.0	103.0	323.0
CAM	13.0	52.8	105.0	654.0

architectures and networks, one from the Portuguese network operator *NOS* and the other from the Spanish network operator *Telefónica*. Both networks were deployed and configured by *NOKIA* to perform S1 handover using the S10 interface Kakes et al. (2022). The MECs from both MNOs are directly interconnected via a dedicated fiber optics link. The presented evaluation scenario consists of three main elements:

- a 5G RSU deployed in the Portuguese side (A3 highway) of the cross-border bridge near the cities of *Valença* (PT) and *Tui* (ES). The RSU is equipped with a traffic radar to detect vehicles on the road and transmit CPM packets. These CPMs are always sent to the PT MQTT broker, since the RSU employs a PT SIM card and it is under the coverage of the PT gNB;
- a 5G OBU installed within a vehicle that moves around the border area for multiple times in the same track - the highway bridge (A3 in PT and A55 in ES). The connection to the MEC MQTT broker depends on the SIM card inserted into the OBU, so that in some tests the device connects to the ES MQTT broker, while it is connected to the PT one;
- two virtual machines host the interconnected MQTT brokers, each deployed in an MEC that belongs to the Portuguese or the Spanish MNO, respectively *NOS* and *Telefónica*.

Time synchronization among all these elements of the network is achieved through *Network Time Protocol* (NTP) servers from MNOs for the case of virtual machines hosted in the MECs, as well as local time servers based on *Global Navigation Satellite System* (GNSS) receivers for RSU and OBU devices. Timestamps of all transmitted and received messages are collected at the applications layer of each network node for posterior matching, comparison and analysis.

The results obtained for two different scenarios are presented below. The value of latency was considered to be the most important criterion, since for example *Packet Delivery Ratio* (PDR) was always greater than 99.9%.

5.1 Single Public Land Mobile Network Scenario

In the first scenario (Single PLMN), both the RSU and the OBU are equipped with PT SIM cards and are under the coverage of the PT network, which means that no inter-PLMN handover occurs. Both devices are always connected to the same network and to the PT MEC MQTT broker.

Figure 7 depicts this scenario, where the message flow of both CPM and CAM packets can be observed. As documented, CPMs (blue arrows) are composed by the RSU 1) and sent to the MQTT broker running at the MEC (2). These messages are then forwarded to the devices that have subscribed to the CPM's *outqueue* topic (3), (4), in this case the vehicle's 5G OBU. In the same way, CAMs (red arrows) are generated by the OBU 1) and sent to the MQTT broker (2), and then these messages are published among entities subscribed to the CAM's *outqueue* topic 3) (4), in this case corresponding to the same OBU device.

The latency values for message transmission in this scenario can be visualized in **Figures 8–11**. In **Figure 8**, the evolution of the CPM latency value between the RSU and the OBU is depicted

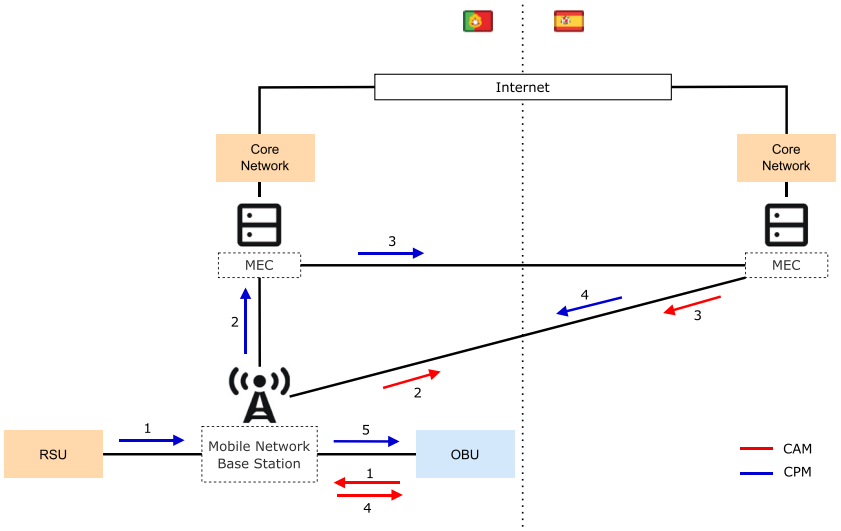

FIGURE 12 | Inter-PLMN Scenario: CPM and CAM packets flow before handover.

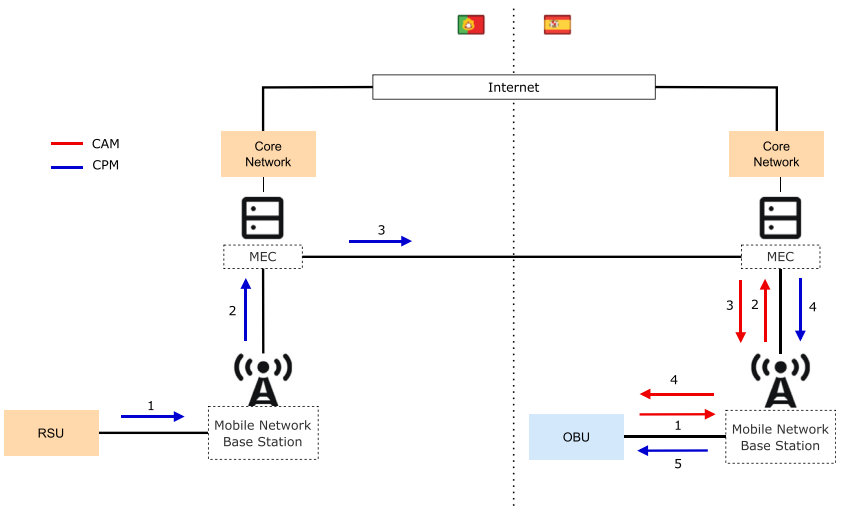

FIGURE 13 | Inter-PLMN Scenario: CPM and CAM packets flow after handover.

over the time of the trial. The periods without message transmission are due to the fact that no vehicles were passing under the radar coverage at those moments and therefore, no CPMs were being generated at the time. The *Reference Signal Received Power* (RSRP) values are also presented for both LTE and 5G NR signals. It is evident that most of the values are around an average end-to-end latency of 40 ms, but there are some peaks of up to 300 ms. There seems to be no significant influence from the observed RSRP values on the end-to-end latency. **Figure 9** illustrates the *Cumulative Distribution Function* (CDF) of measured latency which shows that it is below 100 milliseconds in approximately 95% of the cases. A similar latency analysis is provided for CAM packets sent and received by the OBU. As documented, the behavior is identical, although with higher latency peaks of up to 600 ms (**Figures 10**, **11**).

Table 2 summarizes the results obtained for the single PLMN scenario. It is evident that 95% of the values are less than approximately 100 ms, which is the maximum delay allowed for these types of safety-critical CCAM applications. However, there are some high peak values that exceed this maximum, a fact that deserves further analysis from the MNO's network side, in order to understand what is causing these higher latencies.

5.2 Inter-Public Land Mobile Network Scenario

For the inter-PLMN scenario and in order to evaluate the interconnection between the MECs and the handover event, the OBU was equipped with an ES SIM card, and the connected vehicle left Portugal and traveled to Spain. In this

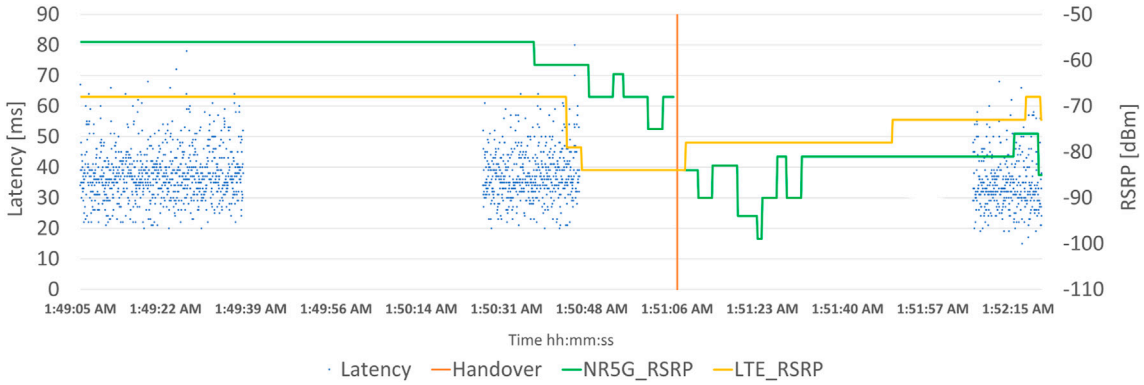

FIGURE 14 | Inter-PLMN Scenario: CPM latency and RSRP values for LTE and 5G NR signals.

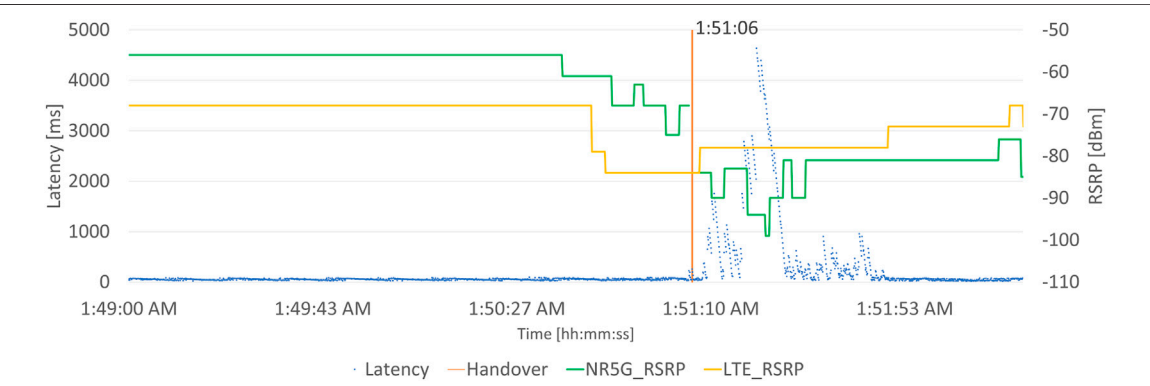

FIGURE 15 | Inter-PLMN Scenario: CAM latency and RSRP values for LTE and 5G NR signals.

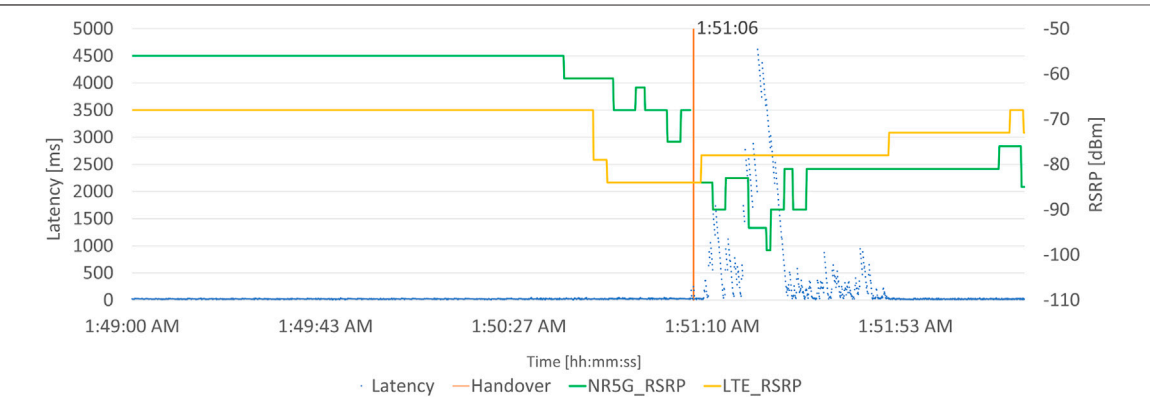

FIGURE 16 | Inter-PLMN Scenario: uplink CAM latency and RSRP values for LTE and 5G NR signals.

case, the OBU was always connected to the ES MQTT broker, while the network was transferred (handover) from the visited network (PT) to the home network (ES). **Figure 12** shows the flow of messages when the OBU is in Portugal and connected to the visited network (PT), while **Figure 13** presents the situation in which the OBU is already inside Spain and connected to the home network (ES). The blue arrows in these figures illustrate the order of CPM message transmissions, which are issued by the RSU 1) and sent to the MQTT brokers running at the MECs 2) (3) and finally to the OBU that has subscribed to the CPM's topic 4) (5). Furthermore, the red arrows in these figures illustrate the order of CAM message transmissions, which are generated by the OBU 1)

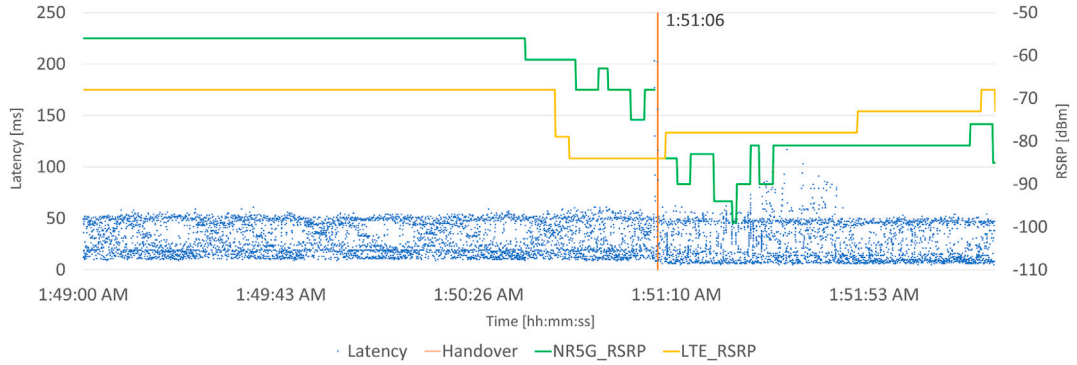

FIGURE 17 | Inter-PLMN Scenario: downlink CAM latency and RSRP values for LTE and 5G NR signals.

TABLE 3 | Summary of the latency measurements for the Inter-PLMN Scenario.

Message type	Direction	Min (ms)	Mean (ms)	95%ile (ms)	Max (ms)
CPM	Uplink	5.0	22.1	38.0	61.0
CPM	Downlink	3.0	10.2	15.0	18.0
CPM	E2E	15.0	37.1	54.0	80.0
CAM	Uplink	8.0	191.2	1,110.3	4,617.0
CAM	Downlink	5.0	29.2	52.0	203.0
CAM	E2E	18.0	222.3	1,121.8	4,633.0

and sent to the MQTT broker (2), and then distributed among entities subscribed to the current CAM's topic 3) (4).

Under these circumstances, **Figure 14** shows the evolution of the latency over time for the CPM packets, including a visual marker for the handover event. It is possible to observe the temporary loss of the 5G NR signal during the handover from the visited network to the home network, but no noticeable differences are observed in the end-to-end delay before and after the handover (always around 40 ms). However, at the exact moment of the handover no CPM packets were being transmitted due to the lack of vehicles to be detected on the road.

On the other hand, for the case of CAM packets (**Figure 15**), several latency peaks occur right after the handover event, reaching delays of more than 4 s. These abnormally high latency values last for approximately 1 minute, after which the latencies stabilize again around the average value of 40 ms. By analyzing the downlink and uplink components of the total delay of the CAM packet (**Figures 16**, **17**, respectively), it is possible to observe that the latency peaks are caused by large uplink delays, while the downlink latencies are mostly circumscribed to around 50 ms, rarely reaching the worst case of approximately 200 ms. Besides the handover event, the observed low RSRP values of 5G NR signal in the moments after the OBU attaches to the new network could also have a significant contribution to the large delay values present in the graph.

5.3 Discussion

Table 3 presents a summary of the latency results for the inter-PLMN scenario, clearly showing that the high delay values observed for the CAM packets after the handover event are due to the uplink traffic with a mean value of approximately 200 ms and a 95% of more than 1 s.

Despite these results showing a significant improvement when compared to traditional roaming scenarios in which a UE could loose network connection for several minutes while crossing countries' borders, the fact is that these high latency values don't fully satisfy the strict requirements for safety-critical CCAM applications. Further analysis of these delays should be performed at the network level by MNOs, with a closer look at the different stages of the handover procedure and packet transport during this transition from one PLMN to the other.

On the other hand, the mobility interruption time is very low, with the UE only loosing 5G NR signal for a few milliseconds during the handover event, showing that it quickly reattaches to the new PLMN with no packet loss caused by this transition. However, all tests were performed using MQTT, which employs TCP as the transport protocol, which means that possibly some packets were lost and then retransmitted. As a result, more trials have to be conducted, for instance using UDP protocol, in order to verify if the HO event decreased the *Packet Delivery Ratio* (PDR) at the moment of the PLMN switching.

6 CONCLUSION AND FUTURE WORK

A combination of technologies and techniques is required to apply and meet various functional and quality requirements to ensure the continuity of the CCAM service in cross-border corridors. These

requirements include low-latency communications, high reliability in packet transmission and network availability, as well as security and privacy aspects. The key objective is to provide uninterrupted service to vehicles while crossing borders with minimal delays in accessing services. To meet the above requirements while ensuring the continuity of services is challenging. In this regard, MNOs have used a variety of methods to overcome the challenge of maintaining network connectivity when crossing borders, but they do not guarantee reliable service continuity, in particular for safety-critical use cases such as CCAM applications. Recent advances in cloud computing and the emergence of MEC with the use of 5G could assist CCAM service continuity in CBCs.

This work focuses on the service continuity challenge of inter-PLMN handover scenarios by proposing an architecture based on direct MEC interconnection between different MNOs, MEC federation of these edge-based services and fast authentication and authorization procedures when roaming from a network to a neighbouring one. The proposed system is evaluated in a real-world scenario within the scope of the 5G-MOBIX project, in the cross-border corridor between Portugal and Spain. This initial evaluation of the deployed architecture shows promising results with very low HO interruption times. However, there are high latency peaks, especially in the uplink traffic, less than a minute interval after the inter-PLMN handover takes place.

In the future, more trials will be performed to better understand the observed behavior during HO events, and different configurations will be tested to explore, for example, roaming from *Home Network* to *Visited Network*. In addition, this work will be extended to fully assess the authentication scheme and security implementation in an inter-MEC roaming scenario, where vehicles change IP address and establish a new connection to the MEC MQTT broker hosted in the incoming MNO. However, this complete architecture can only be tested when the deployed networks are configured to support LBO roaming scenarios.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

AUTHOR CONTRIBUTIONS

SH, MJ, JA, JF, CR and MM contributed to system design and implementation. SH, MJ, DR, JA and MM worked on trials execution, results collection and data analysis. SH, MJ, DR, JA, PB and JF contributed to paper writing and review.

FUNDING

The work presented in this paper is part of the European Project 5G-MOBIX. This project is funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 825496. The content reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

REFERENCES

3GPP (2020). *5G; System Architecture for the 5G System (5GS) (3GPP TS 23.501 Version 16.6.0 Release 16)*. Sophia Antipolis, France: Technical Specification, ETSI.

Ahmad, W. S. H. M. W., Radzi, N. A. M., Samidi, F. S., Ismail, A., Abdullah, F., and Jamaludin, M. Z. (2020). 5G Technology: Towards Dynamic Spectrum Sharing Using Cognitive Radio Networks. *IEEE Access* 8, 14460–14488. doi:10.1109/access.2020.2966271

Aissioui, A., Ksentini, A., Gueroui, A. M., and Taleb, T. (2018). On Enabling 5G Automotive Systems Using Follow Me Edge-Cloud Concept. *IEEE Trans. Veh. Technol.* 67, 5302–5316. doi:10.1109/tvt.2018.2805369

Alonso Raposo, M., Grosso, M., Després, J., Fernández Macías, E., Galassi, C., Krasenbrink, A., et al. (2018). *An Analysis of Possible Socio-Economic Effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe*. Europe: European Union.

Barzegar, H. R., El Ioini, N., and Pahl, C. (2020). "Service Continuity for CCAM Platform in 5G-CARMEN," in *2020 International Wireless Communications and Mobile Computing (IWCMC)* (IEEE), 1764–1769. doi:10.1109/iwcmc48107.2020.9148380

Belhajjame, K., B'Far, R., Cheney, J., Coppens, S., Cresswell, S., Gil, Y., et al. (2013). PROV-DM: The PROV Data Model. *W3C Recomm.* 14, 15–16.

Bonnah, E., and Shiguang, J. (2020). DecChain: A Decentralized Security Approach in Edge Computing Based on Blockchain. *Future Gener. Comput. Syst.* 113, 363–379. doi:10.1016/j.future.2020.07.009

Centenaro, M., Berlato, S., Carbone, R., Burzio, G., Cordella, G. F., Ranise, S., et al. (2020). "Security Considerations on 5G-Enabled Back-Situation Awareness for CCAM," in *2020 IEEE 3rd 5G World Forum (5GWF)* (IEEE), 245–250. doi:10.1109/5gwf49715.2020.9221064

Chipta, M., Uttarwar, M., and Chong, P. H. J. (2021). "Intelligent Handover Using User-Mobility Pattern Analysis for 5G Mobile Networks," in 2021 Conference on Information Communications Technology and Society (ICTAS) (IEEE), 5–10. doi:10.1109/ictas50802.2021.9395027

El Ioini, N., and Pahl, C. (2018). "Trustworthy Orchestration of Container Based Edge Computing Using Permissioned Blockchain," in 2018 Fifth International Conference on Internet of Things: Systems, Management and Security (IEEE), 147–154. doi:10.1109/iotsms.2018.8554470

El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., and Ranganathan, P. (2020). Cybersecurity Challenges in Vehicular Communications. *Veh. Commun.* 23, 100214. doi:10.1016/j.vehcom.2019.100214

ETSI (2020). *Cooperative ITS (C-ITS); Release 1*. Sophia Antipolis, France: TC ITS, Tech.

ETSI (2019). *Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Analysis of the Collective -Perception Service (CPS)*. Sophia Antipolis, France: Tech. Rep. ETSI TR 103 562 V2.1.1, ETSI.

ETSI (2014). Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. *Draft ETSI TS* 20, 448–451.

Farris, I., Taleb, T., Iera, A., and Flinck, H. (2017). "Lightweight Service Replication for Ultra-short Latency Applications in Mobile Edge Networks," in 2017 IEEE International Conference on Communications (ICC) (IEEE), 1–6. doi:10.1109/icc.2017.7996357

Int, S. (2021). *Road Vehicles — Cybersecurity Engineering*. Vehicle Cybersecurity Systems Engineering Committee.

Kakes, G., Alonso, J. R., Masmanidis, I., Nooren, P., Schwartz, R. S., and Trichias, K. (2022). *Network Directed Cross-Border Handovers for CAM Services in Neighbouring 5G NSA and SA Networks*. EuCNC & 6G Summit.

Krishna, K., Karumuri, N., Christopher, C., and Jayapandian, N. (2021). "Research Challenges in Self-Driving Vehicle by Using Internet of Things (IoT)," in 2021

5th International Conference on Intelligent Computing and Control Systems (ICICCS) (IEEE), 423–427. doi:10.1109/iciccs51141.2021.9432147

Labriji, I., Meneghello, F., Cecchinato, D., Sesia, S., Perraud, E., Strinati, E. C., et al. (2021). Mobility Aware and Dynamic Migration of MEC Services for the Internet of Vehicles. *IEEE Trans. Netw. Serv. Manag.* 18, 570–584. doi:10.1109/tnsm.2021.3052808

Lal, P., Yamini, V., and Mohammed, V. N. (2017). "Handoff Mechanisms in LTE Networks," in IOP Conference Series: Materials Science and Engineering (Bristol, UK: IOP Publishing), 052033. doi:10.1088/1757-899x/263/5/052033

Llopis-Albert, C., Rubio, F., and Valero, F. (2021). Impact of Digital Transformation on the Automotive Industry. *Technol. Forecast. Soc. change* 162, 120343. doi:10.1016/j.techfore.2020.120343

Mao, Y., You, C., Zhang, J., Huang, K., and Letaief, K. B. (2017). A Survey on Mobile Edge Computing: The Communication Perspective. *IEEE Commun. Surv. Tutorials* 19, 2322–2358. doi:10.1109/comst.2017.2745201

Morabito, R. (2017). Virtualization on Internet of Things Edge Devices with Container Technologies: a Performance Evaluation. *IEEE Access* 5, 8835–8850. doi:10.1109/access.2017.2704444

Pahl, C., and El Ioini, N. (2019). "Blockchain Based Service Continuity in Mobile Edge Computing," in 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (IEEE), 136–141.

Pomalo, M., El Ioini, N., Pahl, C., and Barzegar, H. R. (2020). "Service Migration in Multi-Domain Cellular Networks Based on Machine Learning Approaches," in 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (IEEE), 1–8. doi:10.1109/iotsms52051.2020.9340223

Popovski, P., Nielsen, J. J., Stefanovic, C., De Carvalho, E., Strom, E., Trillingsgaard, K. F., et al. (2018). Wireless Access for Ultra-reliable Low-Latency Communication: Principles and Building Blocks. *Ieee Netw.* 32, 16–23. doi:10.1109/mnet.2018.1700258

Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., and Taleb, T. (2018). Survey on Multi-Access Edge Computing for Internet of Things Realization. *IEEE Commun. Surv. Tutorials* 20, 2961–2991. doi:10.1109/comst.2018.2849509

Rahman, M. A., Salih, Q. M., Asyhari, A. T., and Azad, S. (2019). Traveling Distance Estimation to Mitigate Unnecessary Handoff in Mobile Wireless Networks. *Ann. Telecommun.* 74, 717–726. doi:10.1007/s12243-019-00713-x

Rivera, A. V., Refaey, A., and Hossain, E. (2020). *A Blockchain Framework for Secure Task Sharing in Multi-Access Edge Computing*. IEEE Network.

Safa Abd ELWahab, M. I., and Abbas, M. A. H. (2020). *A New Vertical Handover Prediction Method for Heterogeneous Wireless Networks*. Khartoum, Sudan: University Of Khartoum Engineering Journal, 10.

Sultan, J., Mohsen, M. S., Al-Thobhani, N. S., and Jabbar, W. A. (2021). "Performance of Hard Handover in 5G Heterogeneous Networks," in 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA) (IEEE), 1–7. doi:10.1109/esmarta52612.2021.9515745

Taleb, T., and Ksentini, A. (2013). Follow Me Cloud: Interworking Federated Clouds and Distributed Mobile Networks. *IEEE Netw.* 27, 12–19. doi:10.1109/mnet.2013.6616110

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.