Inter-PLMN Mobility Management Challenges for Supporting Cross-Border Connected and Automated Mobility (CAM) Over 5G Networks

Konstantinos Trichias[1,2,*], Panagiotis Demestichas[1,3] and Nikolaos Mitrou[2]

[1]*Wings ICT Solutions, Greece*
[2]*National Technical University of Athens, Greece*
[3]*University of Piraeus, Greece*
E-mail: ktrichias@wings-ict-solutions.eu; pdemest@wings-ict-solutions.eu; pdemest@unipi.gr; mitrou@cs.ntua.gr
[*]*Corresponding Author*

Received 28 September 2020; Accepted 09 March 2021;
Publication 28 May 2021

Abstract

As the first 5G networks are being deployed across the world, new services enabled by the superior performance of 5G in terms of throughput, latency and reliability are emerging. Connected and Automated Mobility (CAM) services are perhaps among the most demanding applications that 5G networks will have to support and their deployment, performance and potential for improvement has been well investigated over the past few years. However, CAM operation in multi-operator environments and the inevitable inter-PLMN handover caused by the inherent mobility of CAM services have not been studied in length. Moreover, the multiple domains, multi-vendor components and inherent high mobility of the cross-border vehicular environment, introduce multiple challenges in terms of network management and dynamic slicing, making *Zero-touch network and Service Management (ZSM)* solutions an attractive alternative for these environments.

Journal of ICT Standardization, Vol. 9_2, 113–146. *River Publishers*
doi: 10.13052/jicts2245-800X.924
This is an Open Access publication. © 2021 *the Author(s). All rights reserved.*

The work presented in this study attempts to analyse the requirements for cross-border CAM operation for the ***five main CAM use cases*** selected by 3GPP, based on input from key European stakeholders (Network Operators, vendors, Automotive Manufacturers etc.). A detailed analysis and categorization into four categories of the main challenges for cross-border CAM service provisioning is performed, namely ***Telecommunication, Application, Security/Privacy and Regulatory*** issues, while potential solutions based on existing and upcoming technological enablers are discussed for each of them. The role of standardization and relevant regulatory and administrative bodies is analysed, leading to insights regarding the most promising future research directions in the field of cross-border CAM services.

Keywords: 5G, connected and automated mobility (CAM), mobility management (MM), inter-PLMN HO, cross-border challenges.

1 Introduction

The European Commission's (EC) vision to launch initial 5G services by 2020 and to cover major urban areas and main transport paths by 2025 [1] is starting to take shape. This EC action plan [1] has set forth a clear roadmap for public and private investment into 5G infrastructure along the main EU transport paths, to enable a series of advanced vertical use cases and services across Europe including Connected and Automated Mobility (CAM), Transport and Logistics (T&L), Infrastructure monitoring and security, Smart/Liveable cities and more. Such services span multiple vertical aspects (security, safety, efficiency, entertainment and more) and touch upon multiple modes of transportation (vehicular, railways, shipping, etc.).

The critical role of this multi-modal mobility in the European financial and business ecosystems is evident in the increasing trends in major sectors such as commuting and commerce, which makes the support and availability of such advanced services across European member states a critical success factor. Commuting is an inherent part of the European lifestyle and economy. In certain regions it affects up to 50% of the population, it can involve more than 60 minutes per day and can be associated with diverse and considerably high cost. The cost of commuting in EU ranges from 0.6% of the average net monthly salary up to 7.5% [2]. On the other hand, EU exports and imports constitute a large part of the European economy, as in 2018, they were at the level of 5.5 trillion Euros and accounted for about one-third (1/3) of the global volume [3]. To support such advanced, demanding and differentiated mobility and transport services seamlessly across different member states, 5G

networks are continuously evolving with enhanced mobility support features e.g., Vehicle to Everything (V2X) and enhanced Handover (HO) support, which are necessary in order to support CAM applications and functionalities as the driving force behind the above vertical services.

With that in mind and targeting to support the development of the EC strategic action plan [1], the Trans-European Transport Network (TEN-T) initiative has been created [4], defining nine critical corridors for transportation across Europe where advanced CAM services are expected to be fully supported by 2025, creating novel business opportunities. To complete this long-term vision, the EU has put forth the idea of Connecting Europe Facility (CEF) [5], combining digital, transport and energy infrastructures across Europe, providing a true unified digital and technological end-to-end European ecosystem, in which (Beyond) 5G connectivity is going to play an integral part.

However in order to establish uninterrupted and smooth connectivity along the entire corridors (each spanning multiple European nations), capable of supporting the stringent requirements (e.g. end-to-end latency < 20 ms, reliability of 99.999%, mobility support up to 250 km/h, etc.) of the CAM applications, robust Mobility Management (MM) mechanisms need to be in place, capable of supporting CAM functionality even during an inter-Public Land Mobile Network (PLMN) HO of the service, i.e. when a mobile user and/or vehicle crosses the borders and starts being served by the neighbouring Mobile Network Operator (MNO) and its PLMN. In such cases multiple connectivity aspects need to be addressed, such as service and session continuity, core/MEC (Mobile/Multi-Access Edge Computing) interconnection, application state transfer and more, in order to guarantee the desired Quality of Service/Experience (QoS/QoE) and the satisfaction of the stringent CAM requirements and targeted Key Performance Indicators (KPIs).

Despite the significant enhancements on MM in the latest releases of 3GPP (3rd Generation Partnership Project) Technical Specifications (TS) for 5G [6, 7] and even the specialized features defined to support V2X services [8], the support of inter-PLMN CAM functionality has been largely out of scope resulting in a significant number of unresolved challenges that would have to be addressed in order to guarantee a safe (i.e. preventing accidents involving automated vehicles) and smooth cross-border CAM operation, utilizing 5G connectivity. The work presented in this paper aims to identify, analyse and categorize the most prominent cross-border challenges for CAM, going beyond just technical issues and addressing the support of the entire CAM ecosystem. This analysis is based on the examination and categorization of the most prominent CAM use cases to be supported in

cross border scenarios according to 3GPP and a survey among key European stakeholders (MNOs, Original Equipment Manufacturers (OEMs), vendors, etc.). Relevant standardization work is also taken into account and the most recent 3GPP mechanisms for roaming improvements over 5G Stand Alone (SA) networks are also investigated leading to useful insights regarding the remaining challenges.

The remainder of this paper is organized as follows: Section 2 presents the most prominent CAM use cases to be supported in cross-border environments, the respective KPIs that need to be attained and the main obstacles for CAM service provisioning at the borders. In Section 3, an overview of the identified cross-border MM challenges, their categorization as well as potential solutions for each of them are discussed, while in Section 4 the most recent and relevant standardization features/mechanisms for roaming enhancements in 5G networks are presented. Finally, Section 5 discusses the insights and conclusions drawn from this study and proposes the most relevant future research direction on inter-PLMN/inter-MNO MM for the provision of CAM services.

2 Cross-Border Aspects Consideration

2.1 Main Obstacles of CAM Cross-border Operation

The concepts of inter-PLMN (cross-border) functionality and roaming in all existing mobile networks up to and including 4G-LTE, is inherently contradictory to the need of CAM applications for ubiquitous service continuity and extreme low latency, as traditionally users of mobile networks will experience a service interruption (and reconnection to the visiting PLMN) for a significant amount of time (in the order of (tens of) seconds) during roaming. While this may be sufficient or non-problematic for e.g. infotainment applications resulting in nothing more than the user's slight irritation, such a QoS is absolutely unacceptable for critical CAM applications such as automated driving, remote driving, etc. as it would result in an uncontrolled vehicle during roaming and most likely in an accident. Thus, it can be understood, that guaranteeing service continuity and minimizing the HO latency between neighbouring 5G networks is the key for ubiquitous, uninterrupted CAM support across different states/countries, and it becomes crucial for the commercial success of such services.

To make matters worse, national borders are an extremely complex and multi-disciplinary/multi-stakeholder environment which requires

tight coordination among MNOs, road operators, infrastructure/application providers and public authorities, on a number of technical and non-technical aspects, in order to guarantee a smooth end-to-end experience for autonomous vehicles. The integration and interworking of Road-Side Infrastructure (RSI), such as edge/MEC nodes, Road-Side Units (RSU), cameras/sensors etc., with the 5G network, the autonomous vehicles and their onboard systems (On-Board Units (OBU), sensors, etc.) as well as the CAM applications and platforms, requires commonly acceptable guidelines (and standards) and end-to-end system design, tight synchronization among all involved components and common formatting rules, which are currently non-existent. Moreover, the diversified national traffic regulations, data management and protection rules and potential local restrictions on spectrum usage, admissible/allowable technologies, etc., create the need for a complex policy framework, which should be in effect on both sides of the borders.

Provisioning CAM services in cross-border environments over 5G networks, also has significant network management implications. The dynamic instantiation and reconfiguration of slices for vehicular users, the highly diversified requirements of the different CAM use cases, the extremely dynamic vehicular environment and the complex multi-stakeholder cross-border settings, require very quick reflexes in terms of network resource allocation, cross-domain slicing management, network functions allocation and more. A high automation level is required for proper network management in such an ecosystem, where ideally the CAM use case requirements will be automatically translated into optimal network configuration settings while network Life Cycle Management (LCM) would be used to constantly monitor and adapt the network management decisions. In this direction, Zero-touch network and Service Management[1] (ZSM), provides an attractive alternative which could fulfil the stringent network management requirements of CAM applications.

2.2 Cross-border Support for CAM Use Cases and 5G Related KPIs

The support of SAE Level 4 and 5[2] (i.e. fully autonomous vehicles) CAM use cases over 5G connectivity is a challenging endeavour on its own right, as the

[1] https://www.etsi.org/technologies/zero-touch-network-service-management

[2] https://www.technologymagazine.com/ai/understanding-sae-automated-driving-levels-0-5-explained

throughput, latency and reliability requirements of most of the critical CAM use cases are extremely stringent. Attempting to meet these requirements especially in cross-border conditions, significantly increases the difficulty level and raises the bar regarding the necessary infrastructure and system design that need to be accommodated at the borders. In order to be able to define in detail the challenges and obstacles that need to be overcome for the provisioning of a smooth CAM cross-border service, the various CAM use cases that are expected to be supported at the borders have to be understood along with their requirements, intricacies and expected KPIs.

As 3GPP started looking into network extensions to support V2X communications over 4G and 5G networks, they defined five main CAM use cases to be studied in order to develop the appropriate mechanisms/features that would enable the support of these use cases by 3GPP networks [12]. The requirement analysis performed on these five use cases provided the design guidelines for the network upgrades and set the performance targets that had to be fulfilled in order to support CAM functionality over 3GPP networks. As the currently ongoing three European trial projects addressing 5G enabled CAM functionality at cross-border environments, namely 5G-MOBIX [9], 5G-CARMEN [10] and 5G-CROCO [11], are also using variations of these five use case categories for their trials (as evidence by their respective deliverables [13, 14] and [15]), we will also consider them as the main use cases to be addressed in this study. These five main use cases are:

(i) **Vehicles Platooning:** referring to the capability of vehicles to travel in a coordinated group with extremely small distances between them, offering energy saving advantages and capability of reduced number of drivers (e.g. one truck driver driving a platoon of five trucks).
(ii) **Advanced Driving:** including autonomous driving functionalities such as, lane merging, overtaking, obstacle avoidance, etc.
(iii) **Extended sensors:** referring to the combination/fusion of information from on-board and road-side sensors and equipment to create a "global view" of the vehicular environment with enhanced perception regarding the location and attributes of surrounding vehicles, infrastructure, obstacles, etc.
(iv) **Remote Driving:** referring to the tele-operation of the vehicle by a driver in a remote location, including aspects such as remote assistance in case of accident.
(v) **Vehicle Quality of Service Support:** referring to the timely notification of CAM applications regarding expected/estimated changes in

Table 1 Main CAM Use Cases targeted KPIs

Use Case \ KPIs	Max E2E Latency	Data Rate	Reliability	Position Accuracy
Vehicles Platooning	20–40 ms	50–100 Mbps	99.999%	20–50 cm
Advanced Driving	<10 ms	50 Mbps	99.999%	10–20 cm
Extended Sensors	10–50 ms	up to 1 Gbps	99.99%	20–50 cm
Remote Driving	5 ms	up to 100 Mbps (Uplink)	99.999%	10–20 cm
Vehicle QoS Support	20–100 ms	up to 100 Mbps	99.99%	10–100 cm

the experienced quality of service which may impact their proper (autonomous) functionality.

By understanding the requirements of these five use cases and defining the network KPIs that need to be achieved at all times in order to guarantee their smooth and uninterrupted functionality even when crossing the borders, the exact technical, security, business and regulatory related issues that need to be resolved to accommodate such functionality will become clear. Based on the work carried out by 3GPP [12] as well as the KPI and metrics definition work carried out within 5G-MOBIX based on a survey of relevant participating stakeholder requirements (MNOs, OEMs, vendors, road/customs operators) [16], the targeted technical KPIs that 5G networks have to achieve in order to be able to accommodate the operation of the above five main CAM use cases even in cross-border conditions have been estimated and are presented in Table 1.

From Table 1 it can be observed that most CAM use cases require extremely low end-to-end latency and very high reliability, as it was expected, since the connectivity interruption or the delayed delivery of a critical message could lead to an accident, especially when taking into account the high mobility of the vehicles. In terms of throughput (data rates) most use cases are not that demanding, as usually the content exchanged among vehicles and infrastructure are small packets containing sensor information or driving directives. There are however certain scenarios belonging to these cases that have extremely high demands in BW (such as video sharing, raw data sharing) which also need to be accommodated. Finally, the position accuracy delivered by todays GPS systems (approximately 1–2 meters in most realistic scenarios) appears to not be enough for most of the CAM use cases and that is an area where 5G is expected to have a significant impact (once the position accuracy features of 5G become available).

3 Key Cross-border Challenges Analysis

The cross-border CAM applications operate in a challenging environment where different issues for connected and automated mobility must be addressed to ensure a timely, continuous and seamless operation. Specifically, different EU member laws, stakeholders, industries, operators and economies take place at the EU bridged by a common transit regulation. Thus, the cross-border functionality promotes integration and interoperability taking into account the coexistence and common usage of public and private resources.

The core idea behind this study is to investigate the potential cross-border issues and their potential impact, that arise from trying to provide CAM functionality over 5G networks at cross-border conditions. Specifically, the considered issues pivot around four main dimensions for the most common CAM use cases presented in Table 1:

(i) *Telecommunications issues* regarding issues arising from the implementation of core technological innovations from 5G, such as new frequency bands, Cloud Radio Access Network (C-RAN), Mobile Edge Computing and network virtualisation infrastructures.
(ii) *Application issues* regarding the proper deployment, execution and interconnection of CAM services across different technological, administrative and management domains.
(iii) *Security and privacy issues* spanning the communication and application threats at cross border environments, as well as concerns regarding proper data management and ownership.
(iv) *Regulatory issues* encompassing all potential road, traffic and bureaucratic regulations that CAM functionality needs to take into account.

In the following sub-sections, the most prominent issues of the four identified categories are presented and their potential impact to the proper CAM functionality provisioning at cross-border conditions is discussed. Potential solutions to resolve or mitigate the issues of each category are also discussed.

3.1 Telecommunication Issues

3.1.1 Roaming

International roaming support for V2X communication cases is required when vehicles travel to other countries. Specifically, when a User Equipment (UE), e.g., automated vehicle, crosses the borders, the switching to the new PLMN operated by the neighbouring MNO needs to be performed in an optimum way aiming to fulfil the strict requirements of the CAM use cases and

applications in terms of latency and service continuity. Roaming agreements between the MNOs is a prerequisite. Three distinct cases of roaming can be foreseen:

- *Roaming between MNOs with 5G Evolved Packet Core –Non-Stand Alone (EPC-NSA) network solutions support:* Taking into account vendors' roadmap, this scenario seems to be the most likely to happen at the first phase of 5G deployments, exploiting the existing LTE roaming agreements.
- *Roaming between MNOs with 5G SA core network solutions support:* Taking into account vendors' roadmap & the standardization status, this scenario will occur at a later phase.
- *Roaming between a 5G EPC (NSA) network and a 5G SA network:* Interworking functionalities need to be supported at this scenario; roaming extensions or new roaming interfaces (i.e., N26 interface) will be required.

Long roaming latency is expected since the current LTE roaming traffic is Home Routed (HR), meaning that subscribers always obtain service from the Home Packet Data Network (PDN) gateway (H-PGW) and through their home network. As the service is always managed through the same PGW (the H-PGW), service continuity while roaming can be ensured, but nevertheless with increased latency due to the user plane traffic being routed through the GRX (GPRS Roaming Exchange)/IPX (IP exchange) networks to the Home PLMN (H-PLMN). In addition, the Visited PLMN (V-PLMN) does not normally guarantee QoS for roaming UEs using home routing.

In order to deal with the above presented issues a number of ***potential solutions*** can be envisioned. In certain cases, Ultra Reliable Low Latency Communication (URLLC) resource discovery and allocation may take place within the V-PLMN before the roaming takes place [17], hence partially dealing with the latency concerns (valid for any use case with low E2E latency requirements – see Table 1). In a different more proactive approach, proper selection of roaming network mode (MNOs interconnected via GRX or direct connection) may take place to fulfil the latency requirements. In this case, a direct interconnection for instance could be useful for a border-passage with heavy traffic as it would by-pass the latency-intense GRX interconnection (although this solution is not very scalable). Finally, flexible network configuration may be considered to improve the QoS of services/users, probably considering a proper slice management with 5G SA Core solution. ZSM solutions have the potential to significantly improve roaming performance

by assisting with the autonomous (and potentially predictive) allocation of resources in the visited network, thus reducing the total roaming latency.

3.1.2 Handover (HO)

The HO process during which a UE changes its network service point (eNB/gNB) is perhaps the most critical one of the entire roaming process and defines in a great degree the service continuity and latency capabilities. The current 3GPP HO procedure is analysed in Section 4.1. Three distinct cases can be defined for potential HO scenarios.

HO with overlapping coverage

A bad or uncoordinated cellular planning can induce overlapping coverage issues, where the gNBs radio coverage are highly overlapping. In cross border scenarios (inter-PLMN HO) this scenario is very likely as the MNOs from both countries want to guarantee coverage in their country's territory and as a result a 'spill-over' of coverage from both sides creates unpredictable radio conditions, where the actual HO may take place well before or after the actual border. A high level of overlapping coverage may lead to:

- Interference among gNBs and consequently low SINR (Signal to interference and Noise Ratio) leading to QoS degradation.
- Signal levels are too close to each other leading to disturbance of the UE connection stability, especially, during handover (ping-pong effect).
- The connection drop rate will increase depending on handover rate
- Unjustified signalling traffic load increases.
- At cross border conditions, excessive radio coverage can generate unwanted roaming.
- Cells unbalanced traffic load
- Uplink/Downlink unbalanced cell radio coverage.

Consequently, CAM applications will suffer negative impacts from the resulting QoS degradation. In order to deal with the above presented issues a number of ***potential solutions*** can be envisioned. The use of intelligent algorithms (e.g., Artificial Intelligence (AI)/Machine Learning (ML) based resource allocation/slicing mechanisms) may help to anticipate the handover and trigger the relevant processes. In this case a request for HO parameter optimisation may be issued to the network and in case where ZSM is applied, such updates may be effectuated seamlessly and with minimal latency. In a dual SIM scenario, an intelligent switch will decide for the handover and manage this process to be as stable as possible. This solution may

lead to increased performance but is not very scalable, as multiple SIM cards from multiple MNOs would be required. As a more generic solution, network mobility solutions should be properly adopted for mobility-agnostic applications, while radio access network parameters configuration, such as transmission power, antenna tilt and height, frequency band, etc. should be thoroughly investigated and agreed upon among neighbouring MNOs, which currently seldom happens among neighbouring MNOs (potentially as part of a common framework).

HO with coverage gaps

The distance among the neighbouring countries eNBs/gNBs or the radio planning of the two neighbouring MNOs, results in areas close to the border where no MNO can provide service or UE connection to a network is not even possible. These areas of no coverage are identified as coverage gaps and result in complete service interruption, until connectivity can be re-established with one of the networks.

In order to deal with this issue a number of ***potential solutions*** can be envisioned. Satellite communications may be used to provide service in the areas that 5G connectivity experiences gaps. The moment the network parameters for the other MNO are met, the connection will change from satellite communication back to 5G. During the handover process all data flows will be considered. Such a solution would guarantee service continuity, however, delay sensitive applications may not be satisfied with the satellite provided latency. Handover to 4G if required, may be considered in order to at least guarantee minimal service provisioning. This solution is feasible in cases where the footprint of 4G coverage is different than that of 5G (due to network planning, antenna configurations, utilised spectrum, etc.) but will only result in basic connectivity and will not be able to meet the requirements (in terms of BW or latency) of the most stringent CAM applications Proactive resource allocation may be considered to try and mitigate those issues, while once again detailed network planning & optimization processes for all neighbouring MNOs are considered critical to mitigate this issue.

Hybrid HO

This issue involves the handover between cellular network communication technologies with different performance capabilities, i.e., different RAN and core technologies. This will be particularly common when combining 5G New Radio (5G-NR) with currently available 4G LTE networks. Both cases of HO between a 5G NSA (5G NR + EPC) and a 4G LTE and 5G SA (5G

NR + 5GC) and a 4G LTE network need to be considered. Performance degradation in terms of throughput (impact on enhanced Mobile Broadband (eMBB) services), delay (impact on URLLC services) and potential period of disconnection in the HO are some of the most severe anticipated consequences of such a HO.

In order to deal with the above presented issues a number of potential solutions can be envisioned. A Redundant connection using dual SIM has the potential to resolve this issue, however a proper management of data flows in the same end node, using an intelligent router or Software Defined Networking (SDN) capabilities, for instance, would be required. In general, the softwarization of 5G network functionalities (e.g. orchestration functions) have a significant potential to assist the HO management in such cases [18]. In the absence of this capability, the allocation of maximum resources in the target 4G network could be considered to reduce the impact on the CAM services (overprovisioning). In a different approach, network mobility solutions could be applied to make applications mobility-agnostic. In this paradigm, applications should be developed considering network disconnections (e.g., re-direct to visiting country IP-based platform, option of connection-less mode, etc.). This especially applies to IP-based applications in which re-addressing can be present in the handover. Finally, the use of intelligent algorithms may help to anticipate the network change and trigger the HO once the resources are prepared.

3.1.3 Inter-MEC connectivity

The interconnection of Edge nodes/MECs deployed at different MNOs network across borders is not trivial. The main problem is the high latency that can be expected between MECs as neighbouring MNOs are usually interconnected through 3rd party GRX/IPX networks. MECs interconnected through GRX/IPX networks or directly interconnected but with international traffic routed to the centre of the IP network, result in significant latencies, not suitable to serve stringent CAM applications/functions. High latency introduced by GRX/IPX networks impacts the QoS of applications requiring URLLC. The traditional routing via the MNOs core which may be located hundreds or thousands of km away becomes problematic as well. The lack of security in such interconnections also poses a significant issue.

In order to deal with the above presented issues the following approach can be envisioned. In cases where the neighbouring MNOs PLMNs are connected via a physical direct interconnection then their respective MECs may also benefit from this solution, as the traffic may be directly routed

between them. This solution, although effective is not particularly scalable as all MNOs of one country would need to have direct connections with all other MNOs of all their neighbouring countries. A direct interconnection with IP network configured with border link (international traffic not routed to centre of MNOs IP network) may be another solution to improve the experienced latency without the need for a physical direct interconnection.

3.2 Application Issues

3.2.1 V2X service continuity

Service continuity for CAM applications is of paramount importance especially in safety relevant use cases. Potential unstable communications performance among vehicles, servers and network functions during HO may lead to severe degradation of the application performance and to potential human injury. For instance, in cases of remote driving over a remote-control centre, service continuity must be ensured when roaming from one PLMN to another irrespective of whether the same or different remote-control centres are used (i.e., vehicle needs to be controlled without interruptions even when a change in the control room occurs). In the border surrounding area, V2V communication should be able to be supported for all vehicles irrespective of the PLMN they belong to (e.g., in V2V mode 3 the resources to be used for V2V communication are dictated by the gNB, which could be problematic as vehicles belonging to different PLMNs are controlled by different gNBs). The most common consequences of failing to guarantee this needed V2X continuity are data loss and delay due to roaming and handover, while autonomous manoeuvres may remain unknown, increasing the collision risk which will also be unknown. This type of performance is unacceptable for all safety critical CAM applications.

In order to deal with these issues a number of ***potential solutions*** can be envisioned. Special measures can be put into place to deal specifically with roaming safety critical applications, while for the rest of the applications the HO delay may be customized through resource pre-allocation and proactive planning [17], to meet their respective performance requirements. For critical applications it is important to have a "fail-safe" strategy in place, where the driver is immediately alerted, the autonomous CAM functionality is disengaged and the control of the vehicle is passed back to the driver, for the duration of the HO. Pro-active measures can also be of help in this case, as information about known events in the handover area may be transmitted prior to the vehicle entering this area where potential HO effects may apply.

In a similar spirit, if connectivity among vehicles is not continuous, on-board SW may assist by extrapolating the neighbouring vehicle position based on past trajectory to predict its potential position during handover. Finally, completely autonomous operation of a vehicle (not based on connectivity but rather its own sensors) and Vehicle-to-Vehicle (V2V) based operation should be feasible at least for the duration of the HO process.

3.2.2 Data interoperability

A major concern when large amounts of data is exchanged across multiple vehicle vendors, network domains, infrastructure systems or federated service providers is the inconsistent data schemes. In order to avoid issues during handover between different sides of the border, the various Intelligent Transport Systems (ITS) applications need to exchange a multitude of information on the border area, thus creating an overlapping area of concern. Due to different information sources (e.g., from equipment from different manufacturers or different application/functionality developers) two integrated applications or even the two countries' ITS centres may have different information at a given time. Such a mismatch may lead to inconsistent view of the border area, where the number of vehicles or their exact location and trajectory may not be certain. In turn this creates an additional trust issue (which of the two "views" should be trusted?).

The following ***potential solutions*** can be envisioned for these issues. A rather simplistic but straight-forward solution would be that one of the ITS centres would be nominated (pre-configured) as "Primary", and in case of inconsistent information, all vehicles would trust the information originating from that ITS centre, by default. In an alternative approach, techniques for difference resolution of Decentralized Environmental Notification Messages (DENM) in case of V2V communication could be re-used, i.e., existing techniques for dealing with the reception of DENM messages providing different information about a certain situation [19]. Perhaps the most thorough and complete solution would be the synchronization of neighbouring ITS centres, where such data values discrepancies would be immediately detected, and effective conflict resolution techniques would be applied. In this way, a common view of the border area could be decided among the two ITS centres and communicated to all relevant vehicles.

3.2.3 Protocol/APIs interoperability

Inconsistent Edge cloud Application Programming Interfaces (APIs) across different technology vendors and network domains may lead to significant

interoperability issues, resulting in problematic CAM application operation or even complete breakdown of their functionality. These CAM applications expect a consistent data format in order to be able to process the incoming data. Other applications / functions such as the extended perception function expects a homogeneous protocol to access and publish (API) sensor streams. Incompatible solutions in vehicles for raw sensor streams or processed data (events) will lead to malfunctioning of the CAM applications with potentially catastrophic results.

The following ***potential solutions*** can be envisioned to address this issue. The most straightforward and effective solution would be to standardize the used protocols and data formats, as was the case for Cooperative Awareness Messages (CAM) and DENM messages. Unfortunately, standardization efforts in such a diverse environment comprising infrastructure, platforms and SW development stakeholders is quite complicated. However, a step in this direction could be to involve MEC or centralized functionality which may be tasked with the translation of different messages to a unique format ensuring compatibility. Adoption of standardised messages in such an ecosystem such as the Manoeuvre Coordination Messages (MCM) for Advanced Driving, Collective Perception Message (CPM) for Extended Sensors and map message set, should become a priority.

3.2.4 Additional application challenges

Apart from the above-mentioned key issues, some additional challenges need to be noted. ***Clock Synchronization*** is a critical issue for delay-stringent CAM applications at the border, not only for the potential drift among the clocks of two neighbouring MNOs, but also because of the possibility of a different time zone between neighbouring countries. A clock misalignment or the failure to manage the different time-zones may result in loss of autonomous control of the vehicle. This is especially the case for platooning where the vehicles need orchestration actions with a common timeline and response time of each member. Additionally, ***Geo-driven discovery*** is a significant aspect that needs to be taken into account. For efficient and effective CAM functionality, all relevant vehicles around a certain area need to receive all up-to-date information based on their geo-location, thus including all relevant vehicles and excluding non-relevant vehicles which would overload the communication channels. Vehicles, road-side infrastructure, MEC and centralised systems need to support this type of geo-driven discovery, which becomes even more challenging in cross-border conditions.

Regarding the synchronization issues some ***potential solutions*** could be the use of a common time-reference source among all stakeholders and manufacturers, which is hard to enforce. Predictive analytics could also be used in this case, to anticipate the HO to a visiting network and obtain its timing information in advance in order to prepare and adjust the timing of the relevant CAM applications (account for the drift). Regarding the Geo-driven discovery, the most prominent solution would be to make sure that geo-distribution mechanisms are supported in Roadside, MEC and centralised network systems, both between these systems potentially belonging to different ITS centres, or MEC systems belonging to neighbouring networks. Vehicles should also be able to retrieve geo-location-based information of a predefined area potentially based on standardised V2V communication and pass the knowledge of the surrounding environment onto the participating network components (e.g., MEC) in order for all participating entities to form a single digital image of the immediate environment around the borders.

3.3 Security & Privacy Issues

3.3.1 Different personal data protection regulations in non-EU countries

Different data protection regulations apply when processing personal data subject in EU and non-EU countries, depending on the legal framework of each country. Therefore, many legal, organisational, and technical challenges need to be overcome for lawful processing of these data. Different level of data protection may cause services to be unavailable, which could require personal data protection. As a result, certain CAM application may not work properly once a border is crossed, diminishing the trustworthiness and penetration of said applications (e.g., data sharing for Extended Sensors including license plate video recognition may be more/less limited across the borders).

To counter-act this effect, harmonization of data protection regulation, or establishment of agreements between involved countries is necessary. The General Data Protection Regulation (GDPR) framework[3] applicable in EU countries would be a valid starting point, as already many countries that perform transactions and are in business with EU-based parties are forced to address similar concerns. Such negotiations would have to be extended in the CAM domain as well to guarantee the uninterrupted functionality of CAM applications and services.

[3] https://gdpr-info.eu/

3.3.2 Organizational procedures between different countries

CAM applications supporting cross-border functionality will eventually have to process data from citizens of different countries (e.g., license plate recognition when crossing the border). To this end, proper organisational procedures need to be put in place to handle data protection of the neighbouring country's citizens. These include (but are not limited to):

- Data processing cartography
- Systems' training
- Privacy risk assessment
- Data breach procedures

The management of personal data leaking incidents increases the complexity of this issue which could cause severe security concerns and render a CAM application unsuitable for cross-border functionality. As with the previous issue, any technical solution should be complimented with strong policy decisions in this case, resulting in a legal framework for harmonization of data protection regulation, or establishment of commonly acceptable agreements between participating countries.

3.3.3 Technical difficulties for cross-border lawful data processing

The technical mechanisms that are applied in order to support the legal requirements on lawful data processing could encounter difficulties in a cross-border scenario, as neighbouring countries may need to comply to different legal frameworks regarding the capabilities and permissions of these mechanisms. These mechanisms include (but are not limited to):

- Data encryption
- Anonymization/ pseudonymization
- Informed consent
- Privacy by design and by default

These protection mechanisms could be incompatible between EU and non-EU countries, which could result on more difficult handover procedures or limited functionality of a CAM application, once the border is crossed. Similar to the previous solutions a framework of collaboration among neighbouring MNOs needs to be established while it can be assisted by Artificial Intelligence (AI) mechanisms and predictive analytics where autonomous negotiations algorithms may agree on a minimum set of commonly agreeable configurations / settings for the functionality of the applications in questions

(e.g. list of encryption mechanisms that are considered acceptable in the respective countries, minimum capability negotiations, etc.).

3.4 Regulatory Issues

3.4.1 Autonomous vehicle regulation compliance

There are no national or international regulations specified for the roads and the corresponding autonomous vehicles moving on these roads. For instance, different vehicles will have different safety distance levels for emergency braking situations. In case of handing over the control of the driving from vehicle to driver, there should be standardized driver warning systems (which are not in place currently).

A situation where a connected and automated vehicle (CAV) has been homologated for the source country but not for the destination country may occur. As an example, an Autonomous vehicle A has successfully passed the minimum tests required to drive in autonomous mode in country A, but it has not passed the tests on country B, or the tests are different in the two countries; and therefore, autonomous vehicle A is not authorized to be driven in autonomous mode in country B. These tests ensure that the CAV is safe on that country, e.g. it takes into account the local laws, it has installed the maps for the route, etc. Lack of regulations may affect the vehicular hardware selection and its specifications; hence, compliance to several different systems of different brands can be costly from the perspective of OEMs.

In order to deal with the above issues, there should be a regulation in terms of hardware specifications and capabilities per country as well as border-conditions for cross-border functionality. By using a standardized software algorithm, an adaptive behaviour in each CAM application can be defined for each vehicle according to their capabilities and status. Additionally, driving license trainings can be rearranged according to SAE levels of autonomy of the vehicles and also for specific applications such as platooning.

In an alternate approach, geo-fencing or GPS may be used to restrict the operation of the vehicle in autonomous mode to the areas where it is legally approved. In case the destination of the travel is an area outside of the approved domain the vehicle shall ask the user to take control and then deactivate its autonomous driving or even perform a safe stop autonomously.

3.4.2 Road & traffic regulation compliance

Neighbouring countries may have different traffic rules. This means, the CAV software needs to be adapted to the target location, so that it knows how to

behave to respect local traffic law. In addition, roadside units of a specific region may need to supply different message types/content that may not be understandable by the foreign vehicles. In such cases the vehicle might break the law if this has not been taken into account in the design of the algorithm, or the autonomous driving function might be restricted to certain road types, e.g., highway chauffeur. The lack of understanding in safety related messages may lead to dangerous traffic conditions for all road users.

Different approaches can be envisioned to deal with the above-mentioned issues. The legislation of the destination markets shall be well known by developers so that the Autonomous Driving (AD) algorithm may (re)configure its behaviour depending on the vehicle location. This adaptation can be done in several forms:

- Create High Definition (HD) maps that take into account all countries where the vehicle will be allowed to drive and store not only the road but also all the traffic signs. Add the information about the type of road (urban, highway, etc.) to the onboard map database so that the vehicle does not depend on the road code to determine the road type.
- Traffic management centre and RSU at the border shall inform vehicles that they enter another country and also inform them about the traffic rules. Autonomy level of the vehicle can be changed accordingly.
- The CAV shall check its current location before AD can be activated to ensure it is prepared to drive autonomously on that location and type of road.

Alternatively, in a less technical approach, neighbouring country Road Administration Authorities may exchange a commonly agreed format of expected behaviour of CAVs on common international level traffic legislations and laws, in order to standardise the traffic rules.

3.4.3 Law enforcement interaction

The rapid deployment of autonomous vehicle technology will undoubtedly have a significant impact on public safety services, including law enforcement agencies. In fact, CAV's will reshape the nature of the interactions concerning police authorities. Police officers and other law enforcement authorities must be able to interact with CAVs on the road. To do this, new police interaction protocols have to be designed to communicate with CAVs. As an example, a police officer may need to stop a CAV for a security check, and to do that it has to send a stop request to the vehicle.

Besides the obvious solution of the police making use of autonomous vehicles capable of communicating (over the same protocols) with other

CAVs, a common message set/protocol dedicated to public safety/emergency response interactions should be standardised at European Level (and potentially even in international level). All security authority interactions with CAVs should be protected with highly graded encryption algorithms and should allow authorities to intervene to prevent dangerous situations (e.g., police officers having the capability to force stop a vehicle not obeying orders). Emergency bands and message sets may be defined for this purpose.

4 Relevant Standards and Open Challenges

4.1 3GPP based HO Functionality

In many cases the standardization of a commonly accepted solution is the only way to overcome a certain barrier/challenge, especially in cases where multiple different stakeholders are involved. 3GPP has been attempting to standardize Mobility Management solutions as part of all of its cellular network specification, thus facilitating the interworking of different vendors, MNOs and manufacturers of 5G equipment and devices. When it comes to the execution of a HO due to UE mobility, a standardized process of message exchange between the UE, the Source gNB (S-gNB) and the Target gNB (gNB) takes place. In case of an inter-PLMN HO, the networks' type (4G, 5G, etc.) and configuration as well as the exact roaming agreement between the MNOs play a crucial role to define the additional interfaces and communication paths (e.g. GRX/IPX, direct connection) needed for a successful inter-PLMN HO, otherwise a network reselection might also take place. In order to better understand the additional challenges introduced by an inter-PLMN HO and especially the potential interruption in communication that it may introduce, the 3GPP based HO procedure has to be broken down to its components and studied.

The main 3GPP document describing 5G's System architecture is the Technical Specification (TS23.501) [6], which includes the architecture and description of the Radio Access Network (RAN) and Core functions, while TS23.502 [7] describes the main procedures of 5G, including session management and HO procedures. The fundamental HO procedure as defined by 3GPP can be seen in Figure 4.1. The HO process is triggered when one of the periodic measurement reports that the UE sends to its Serving gNB (S-gNB) indicates that the signal strength towards the S-gNB is deteriorating while the signal strength towards a neighbouring gNB (Target gNB a.k.a. T-gNB) is improving. As a result, the S-gNB understands that the UE will

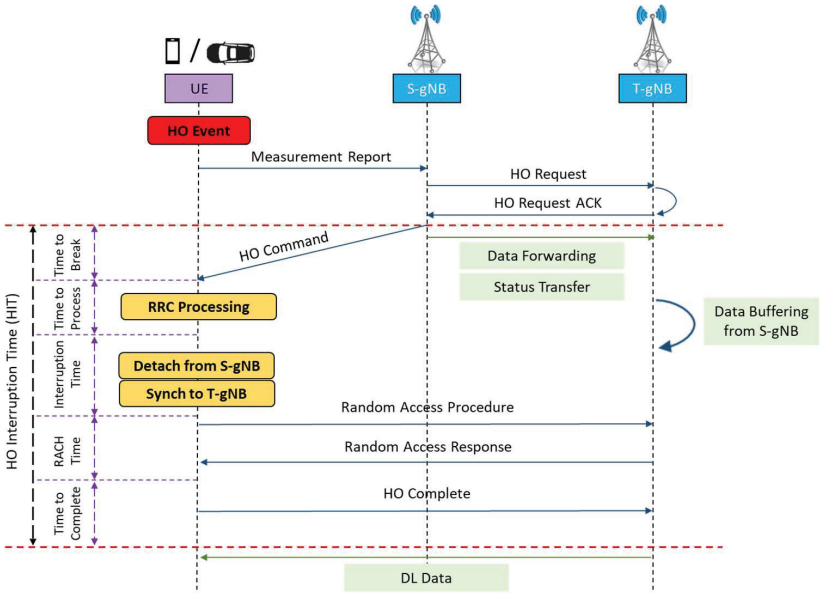

Figure 1 3GPP HO procedure and HO interruption time.

soon be out of its coverage range and issues a HO request towards the T-gNB, informing it about the imminent "arrival" of the particular UE within its coverage range. At that point, and assuming that the T-gNB has enough capacity left to serve the UE under discussion, the HO procedure is triggered. The main components that comprise the HO Interruption Time (HIT) caused from the HO procedure, are also depicted in Figure 1. Those components are:

- *Time to Break:* Time required for the UE to break its connection with the S-gNB.
- *Time to Process:* Time required for the UE to process the HO command and perform the reconfiguration of its Radio Resource Control (RRC) layer.
- *Interruption time:* Time required for the UE to synchronize and attach to the T-gNB.
- *RACH time:* Time required for the UE to perform the Random Access Channel (RACH) procedure in the T-gNB.
- *Time to Complete HO:* Time required to acknowledge the newly established connection towards the T-gNB.

Based on various scientific studies and test measurements such as the ones presented in [20] and [21], the average HIT is estimated to be 49.5 ms.

Leading to a similar service interruption time during a HO. Such an interruption can easily be handled by most non-critical applications as their latency requirements are not that stringent and the respective user will not even notice it (i.e. the QoE will remain practically unchanged), however this is not the case for critical CAM services (see also Table 1) where such a delay could prove catastrophic. It has to be noted that this interruption time will further increase in cases of inter-PLMN HO, as an additional latency component will have to be added due to the inter-PLMN communication taking place over non-latency critical interfaces such as the GRX/IPX, which are commonly considered "best effort". This analysis indicates that the cross-border operation of CAM application face significant hurdles in trying to achieve the necessary latency requirements and highlights the need for additional measures/mechanisms to combat the effects of cross-border mobility and inter-PLMN HO restrictions.

4.2 Mechanisms/Features for Improved Mobility Management

In light of the above, and in order to support URLLC functionality over 5G networks, the 3GPP has upgraded the existing MM mechanisms with certain features that are either trying to minimize (or even completely eliminate) the interruption time introduced by (inter-PLMN) HO or attempting to optimize the data routing across the different networks (PLMNs) targeting a more efficient use of resources and reduced end-to-end latencies. These mechanisms/optimizations termed *Session and Service Continuity* and *Home Routing vs Local Break-Out*, respectively, are presented and discussed below.

4.2.1 Session and service continuity

Session continuity is defined as the capability of a node to maintain its ongoing IP sessions while changing its (IP) point of attachment (when changing network). The simultaneous switching of the application server and host as well, while maintaining full operational capacity for the application is termed service continuity. Maintaining session and service continuity in cross-border conditions (i.e. when changing PLMNs) is perhaps the biggest challenge of the CAM stakeholders at this time, proven by the commissioning of three Innovation projects from the EU tasked with researching CAM functionality at cross-border conditions, namely 5G-MOBIX [9], 5G-CARMEN [10] and 5G-CROCO [11].

3GPP has defined three Session and Service Continuity (SSC) modes [6] for the 5G system, caring for different situations. With SSC mode 1, the Home

User Plane Function (UPF) acting as a Packet Data Unit (PDU) Session Anchor is maintained throughout session lifetime regardless and the UE's session IP address does not change. Such a choice provides IP continuity (i.e., zero interruption) but it leads to increased end-to-end delays due to the sub-optimal UE-UPF path. In SSC mode 2, the network may trigger the release of the PDU session and instruct the UE to establish a new PDU session from its new location. In this scenario, the IP address changes and a new PDU Session Anchor UPF may be selected. In this case, there is an interruption of connectivity (IP change), but an optimal UE-UPF path is selected, providing optimum latency. Finally, SSC mode 3 introduces the Make-Before-Break (MBB) mechanism, where the network ensures that there is no loss of connectivity, while at the same time optimizing the UE-UPF path based on UE mobility. The network allows the UE to establish connectivity via a new PDU Session Anchor UPF before connectivity between the UE and the previous PDU Session Anchor is released. As a consequence, there is a time at which the UE maintains two parallel PDU sessions with different Anchors in the network. SSC mode 3 involves changing the IP address, but supports service continuity through the MBB mechanism.

The SSC3 approach seems ideal for stringent CAM applications where both service and session continuity and low latencies need to be guaranteed when changing PLMNs, however such a solution requires a 5G SA architecture, i.e., utilizing a 5G Core (not EPC) on both sides of the border and it also requires more expensive and complex UEs with multiple Tx/Rx chains, capable of maintaining two parallel connections.

4.2.2 Home routing vs local break-out

According to the 3GPP defined roaming service access policies used by mobile terminals [6], two main roaming types exist:

- ***Home Routing (HR)***, where subscribers always obtain service from the home PDN gateway (H-PGW) and through their home network. As the service is always managed through the same PGW (the H-PGW), service continuity while roaming is ensured, but with increased latency and resources utilization due to the user plane traffic being routed through the GRX/IPX networks to the Home PLMN.
- ***Local Break-Out (LBO)***, where subscribers obtain service from the visited PGW (V-PGW). In effect, this provides better user experience and significantly reduced roaming service delay (payload traffic does not traverse through GRX but rather stays in V-PLMN network), at

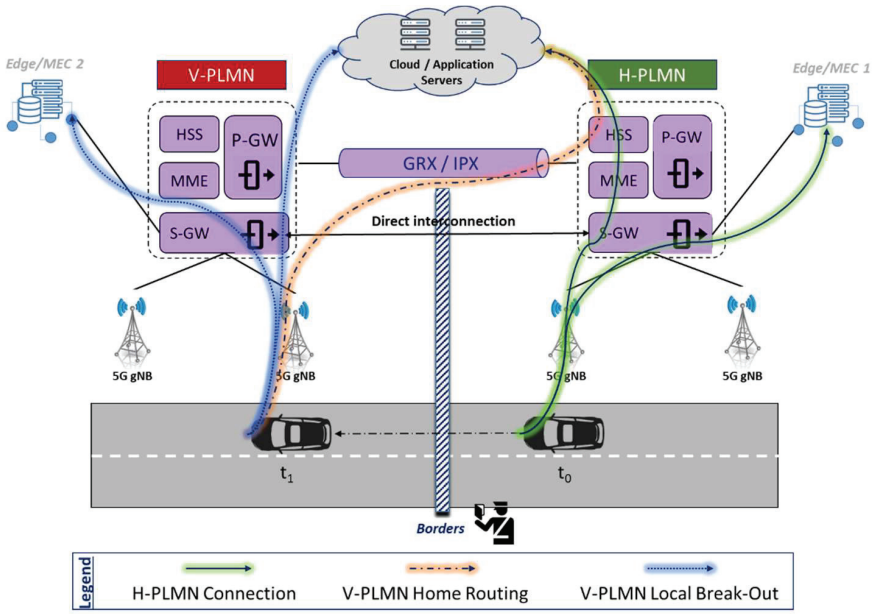

Figure 2 HR vs LBO routing over 5G NSA networks.

the expense of service control, policy control, charging and service continuity that will be disrupted as the sessions must be released and re-established during the handover. LBO, which is a spec compliant functionality, requires re-establishment of PDN session. For LBO to operate the involvement of Home Subscriber Server (HSS) and Mobility Management Entity (MME) modules is required.

In case of a 5G SA architecture using a 5G Core, the Access and Mobility management Function (AMF) determines if a PDU Session is to be established in LBO or HR. In the case of LBO, the procedure is as in the case of non-roaming with the difference that the AMF, the Session Management Function (SMF), the UPF and the Policy and Control Function (PCF) are located in the V-PLMN [7]. The Service Based Architecture (SBA) of the HR and LBO solutions over 5G NSA and 5G SA networks are depicted in Figures 2 and 3, respectively.

These two options have their respective advantages when it comes to supporting CAM cross-border functionality. With Home Routing, the session continuity is ensured (SSC mode 1) as the vehicle may maintain its anchor point in the Home-PLMN (H-PLMN) and as such there will be no session

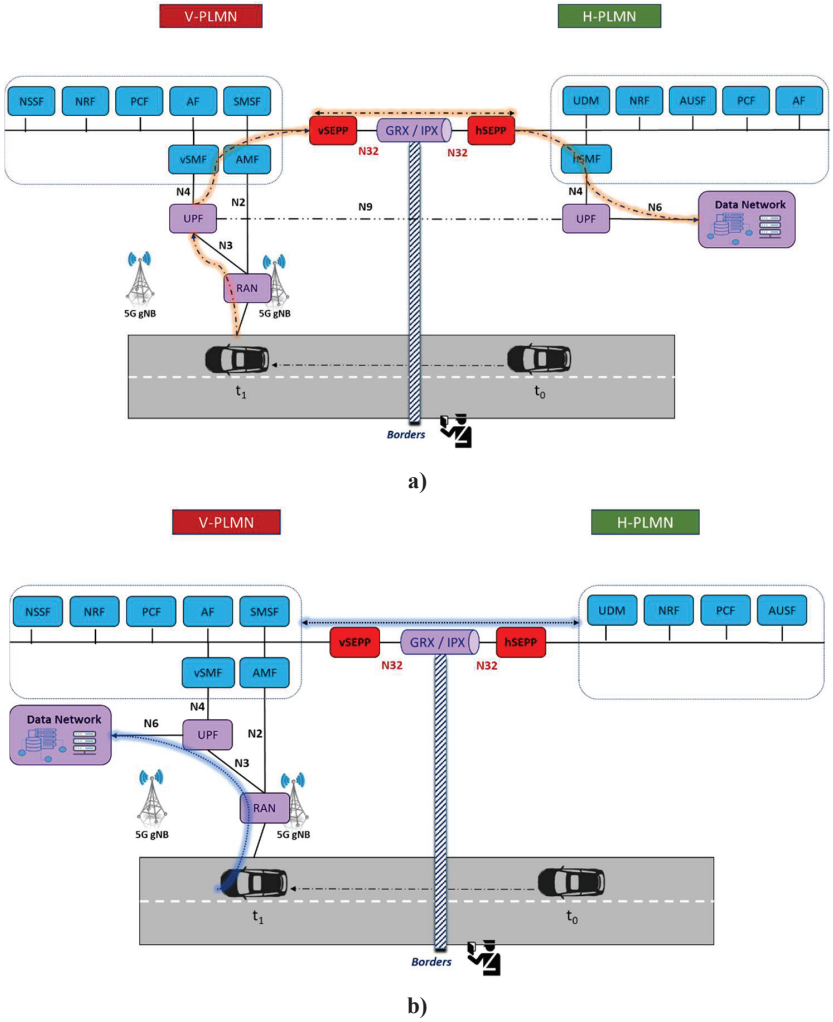

Figure 3 5G SA based roaming architecture with (a) Home-Routing (HR) and (b) Local Break-Out (LBO).

interruption during the inter-PLMN HO. However, such a solution is not particularly scalable when traversing multiple nations, as could be the case when travelling over the TEN-T corridors [4], as the anchor point of a vehicle could end up thousands of km away from its physical location, while at the same time increased end-to-end latency is introduced (unacceptable for critical CAM use cases).

With LBO on the other hand, an always optimum path to the desired data network is ensured, guaranteeing minimum latency and presenting a scalable solution when traversing multiple PLMNs, however the unavoidable session interruption during the inter-PLMN HO will be problematic for CAM applications. In case of 5G SA network deployment from both sides of the borders, the SSC mode 3 could prove to be the best solution for cross-border CAM support (assuming that it works seamlessly in an inter-PLMN environments), but as the full penetration of 5G SA network across Europe is still a long way from happening, interim solutions will be needed.

4.3 Improvements in Inter-PLMN Mobility Expected with 5G SA

The 3GPP has also established interfaces and mechanisms that will enhance the roaming procedures among 5G SA networks (using 5G cores) as depicted in the guidelines presented in [22], both in case of HR and LBO. The exact protocols, message flows and APIs for procedures on PLMN interconnection as well as the dedicated interface ***N32***, are specified in 3GPP specification TS29.573 [23]. The N32 interface, which is comprised of the Control plane interface (N32-c) and the Forwarding interface (N32-f), is used between the Security Edge Protection Proxies (SEPP) of the H-PLMN and V-PLMN during roaming scenarios. The initial handshake between the networks and the negotiation of the roaming parameters to be applied on the actual messages going over the N32 interface, is performed over the N32-c interface, which is then torn-down to give its place to the N32-f interface over which the actual communication between Network Functions (NF) of the two networks takes place. The N32-f connection uses HTTP/2 and is end-to-end between the two SEPPs and may use an established IPX path between the networks, or in case such a path does not exist an IPsec VPN will be established.

Besides the N32 interface, the N9 interface is also established in [6] to facilitate the direct communication among the UPF of the H-PLMN and the V-PLMN. As in LBO mode the SMF and all UPFs sessions are under the control of the VPLM UPF, while in HR both instances of the SMFs and UPFs are utilized, the N9 reference point for user plane traffic is only applicable to the HR scenario [23]. Both the N32 and N9 interfaces (depicted in Figure 3) aim to facilitate the direct communication among the necessary NFs of the two neighbouring PLMNs and as such streamline the roaming process between two 5G SA networks, improving the experienced QoS and the relevant KPIs. Such an improvement could be extremely beneficial for the operation of CAM services in cross-border conditions, however it requires

the almost full penetration of 5G SA networks, thus pointing to future deployments and highlighting the need for interim solutions to accommodate 5G NSA and mixed NSA/SA deployments by different MNOs.

5 Conclusions and Promising Research Directions

Based on the above presented study, the provisioning of CAM services in cross-border environments presents both significant challenges and interesting opportunities. While the provisioning of CAM services over 5G connectivity is a well-studied area with multiple trials and pilots showcasing its validity (e.g., in [24]), it was commonly assumed that CAM service provisioning occurred under a single 5G network (PLMN). The challenges that arise from attempting to provide enhanced CAM services at complex, multi-stakeholder environments such as national borders, remain largely unaddressed. In view of the EU vision for connected transport paths by 2025 [1] and the linked TEN-T initiative [4] of pan-European transport corridors, the investigation of such cross-border challenges becomes increasingly important.

The targeted survey [13, 25] which was performed in the context of the 5G-MOBIX project, highlights the expected performance requirements for each of the five main CAM use case categories envisioned by 3GPP, as expressed by key involved stakeholders such as MNOs, network vendors, OEMs and automotive authorities. These KPIs have to be met irrespective of the underlying network connectivity and the potential interruptions or delays that may be introduced by the inherent vehicular mobility, i.e., change of PLMN. This analysis establishes that while non-critical automotive applications (e.g., traffic information, obstacle notification, etc.) may be able to tolerate the service interruption and larger latency introduced by cross-border mobility, the more advanced CAM applications envisioned by the involved stakeholders (and 3GPP), have extremely stringent service requirements which cannot be met with the current Mobility Management mechanisms.

A detailed analysis of the factors that contribute to the experienced service interruption and/or reduced network performance when a user crosses national borders and is forced into an inter-PLMN HO has been performed and its output has provided significant insights into the challenges that need to be addressed for proper cross-border CAM service provisioning. ***Service and session continuity, MEC interconnection, inter-PLMN HO and data routing, MNO alignment, roaming configurations and data and protocol interoperability***, have emerged as the key technical challenges that

need to be addressed. A significant insight of the study is that in order to be able to provide advanced CAM services at the borders, a number of non-technical challenges also have to be addressed, such as ***spectrum allocation issues, data security and privacy approach (GDPR issues), regulatory compliance, road and traffic regulation heterogeneity*** and more. Moreover, the adoption of more advanced network management schemes such as ***ZSM***, are expected to provide the necessary automation, flexibility and reduced network management inter-working delays, necessary for cross-border operation.

A number of potential solutions are currently envisioned by researchers in order to mitigate or even completely resolve the identified challenges, as discussed in Section 3. These solutions range from enhanced MM mechanisms including e.g., ***SSC mode 3, V2V communication backup (sidelink) and novel interfaces (N9, N32) to predictive analytics mechanisms, resources pre-allocation and overprovisioning, application level proprietary solutions*** and more. The most prominent of these solutions are scheduled to be tested and validated in real-life cross-border conditions in the upcoming trials of the three H2020 ICT-18 projects [9][10][11]. In order to address the non-technical challenges, the idea of a common ***MNO (and other stakeholders) collaboration framework*** which could be dynamic in nature and would indicate commonly acceptable rules and guidelines that all involved parties would follow for the configuration and setup of their networks at the borders, constitutes the most promising way forward.

Currently the focus of the scientific research in this domain lies in the evaluation of the session and service continuity mechanisms, the MEC interconnectivity options and the data routing (HR vs LBO) options over 5G-NSA network deployments, while at the same time several proprietary application level solutions (e.g. dynamic functionality adaptation based on predictive QoS) are also being tested. As the penetration of 5G networks increases and SA deployments and new releases from 3GPP, i.e., Rel.16 and Rel.17, become available, it is essential for future research to focus on 5G SA mechanisms (SSC mode 3, inter-PLMN roaming, etc.) and interfaces (N9, N32) which have the potential to significantly reduce the service interruption and end-to-end latency. In parallel, co-existence mechanisms with legacy network and non-3GPP technologies have to be investigated especially due to the concurrent usage of non-licensed spectrum (5.9 GHz band), which becomes even more critical with the advent of enhanced PC5 (sidelink) functionality with 3GPP Rel.16.

Acknowledgements

This work has partially been performed within the 5G-MOBIX project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825496. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

References

[1] 5G for Europe Action Plan: https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan
[2] Comparing The Cost Of Commuting Across Each European Capital City, https://www.silverdoorapartments.com/blog/cost-of-commuting/
[3] World Trade Statistical Report 2018, https://www.wto.org/english/res_e/statis_e/wts2018_e/wts18_toc_e.htm
[4] Trans-European Transport Network (TEN-T) core corridors: http://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/map/maps.html
[5] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528878837354&uri=CELEX:52018PC0438
[6] 3GPP TS23.501, Technical Specification "System architecture for the 5G System (5GS)", v 16.4.0
[7] 3GPP TS23.502, Technical Specification "Procedures for the 5G System (5GS)", v 16.4.0
[8] 3GPP TR22.886, Technical Report, "Study on enhancement of 3GPP Support for 5G V2X Services", v.15.3.0
[9] H2020 ICT-18-2018 5G-MOBIX project: https://www.5g-mobix.com/
[10] H2020 ICT-18-2018 5G-CARMEN project: https://5gcarmen.eu/
[11] H2020 ICT-18-2018 5G-CROCO project: https://5gcroco.eu/
[12] 3GPP TS22.186, Technical Specification, "Enhancement of 3GPP support for V2X scenarios; Stage 1", v16.2.0, June 2019
[13] 5G-MOBIX Deliverable D2.1, "5G-enabled CCAM use cases specification", October 2019, https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.1-5G-enabled-CCAM-use-cases-specifications-V2.0.pdf

[14] 5G-CARMEN Deliverable D2.1, "5G-CARMEN Use Cases and Requirements", May 2019, https://5gcarmen.eu/wp-content/uploads/2020/03/5G_CARMEN_D2.1_FINAL.pdf

[15] 5G-CROCO Deliverable D2.1, "Test Case Definition and Trial Site Description – Part 1", January 2020, https://5gcroco.eu/images/templates/rsvario/images/5GCroCo_D2_1v2.pdf

[16] 5G-MOBIX Deliverable D2.5, "Initial Evaluation KPIs and Metrics", October 2019, https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.5-Initial-evaluation-KPIs-and-metrics-V1.4.pdf

[17] V. V. Paranthaman, Y. Kirsal, G. Mapp, P. Shah and H. X. Nguyen, "Exploring a New Proactive Algorithm for Resource Management and Its Application to Wireless Mobile Environments," 2017 IEEE 42nd Conference on Local Computer Networks (LCN), Singapore, 2017, pp. 539–542, doi: 10.1109/LCN.2017.86.

[18] Campolo, Claudia et al. "Slicing on the Road: Enabling the Automotive Vertical through 5G Network Softwarization." Sensors (Basel, Switzerland) vol. 18,12 4435. 14 Dec. 2018, doi:10.3390/s18124435

[19] F. Romeo, C. Campolo, A. Molinaro and A. O. Berthet, "DENM Repetitions to Enhance Reliability of the Autonomous Mode in NR V2X Sidelink," 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 2020, pp. 1–5, doi: 10.1109/VTC2020-Spring48590.2020.9129367.

[20] H. Park, Y. Lee, T. Kim, B. Kim and J. Lee, "Handover Mechanism in NR for Ultra-Reliable Low-Latency Communications," in IEEE Network, vol. 32, no. 2, pp. 41–47, March–April 2018, doi: 10.1109/MNET.2018.1700235

[21] N. Kumar, S. Kumar and K. Subramaniam, "Achieving Zero ms Handover Interruption in New Radio with Higher Throughput Using D2D Communication," 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1–8, doi: 10.1109/WCNC.2019.8885705.

[22] GSMA, Official Document NG.113 - 5G Roaming Guidelines, v2.0, May 2020, https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v2.0-1.pdf

[23] 3GPP TS29.573, Technical Specification, "5G System; Public Land Mobile Network (PLMN) Interconnection", v16.3.0, July 2020.

[24] H2020 5G-DRIVE project, "5G Harmonised Research and Trials for Service Evolution", https://5g-drive.eu/

[25] 5G-MOBIX Deliverable D2.2, "5G architecture and technologies for CCAM specifications", October 2019, https://www.5g-mobix.com/assets/files/5G-MOBIX-D2.2-5G-architecture-and-technologies-for-CCAM-specifications-V1.0.pdf

Biographies

Konstantinos Trichias M.Sc. (male) received a Dipl.-Ing degree in Electrical & Computer Engineering from the University of Patras, Greece, and his M.Sc. degree in Electrical/Telecommunications Engineering from the University of Twente, The Netherlands. He specializes on next-generation heterogeneous wireless and mobile networks, as well as the integration and smooth interoperability of the aforementioned technologies with novel networking paradigms such as SDN, ITS/V2X and IoT, targeting the successful integration of multiple vertical industries (smart cities/industry 4.0, automotive, etc.) into the 5G ecosystem. He has participated in several (inter)national research and industry consultancy projects from multiple positions (PM, TM, QM), and is currently serving as the Technical Coordinator of the H2020-ICT-18-2018 5G MOBIX and as Project Coordinator of the H2020-ICT-41-2020 VITAL-5G projects. He has served as a 3GPP RAN1 & RAN2 delegate on behalf of KPN/TNO and has numerous patent applications in the area of Radio Access systems.

Panagiotis Demestichas is a Professor at the University of Piraeus, School of ICT, Department of Digital Systems, Greece. He is also a co-owner of WINGS ICT Solutions (www.wings-ict-solutions.eu) and of its spin-out Incelligent (www.incelligent.net), in which he focuses on the development of technologies. WINGS focuses on AI-powered solutions for the environment (air quality), networks and infrastructures (water, energy, gas, transportation, construction), production and manufacturing (food security and safety, industry 4.0, logistics), service sectors (health, defense). Incelligent focuses on products for banking, the public sector and telecommunication infrastructures. Panagiotis conducts research on 5G, cloud and IoT, big data and artificial intelligence, orchestration/diagnostics and intent-oriented mechanisms. He holds a Diploma and a Ph.D. degree on Electrical Engineering from the National Technical University of Athens (NTUA). He holds patents, has published numerous articles and research papers, and is a member of the Association for Computing Machinery (ACM) and a Senior Member of IEEE.

Nikola(o)s Mitrou received his diploma degree in Electrical Engineering (1980) from the National Technical University of Athens (NTUA), the MSc

degree in Systems and Control (1981) from UMIST, Great Britain, and the PhD degree in Electrical & Computer Engineering (1986) from NTUA. He is a full Professor with the School of Electrical and Computer Engineering at NTUA since 2000. He has been the leader and/or prime researcher of many European and national projects in the fields of Broadband Telecommunications, Mobile and Multimedia Communications, Knowledge Representation & Management and has published numerous articles and conference papers in these fields.