AUTOMOTIVE EDGE
COMPUTING CONSORTIUM

AECC Technical Report

Automotive Edge Computing Consortium (AECC)

Technical Solution Working Group (WG2)

Driving Data to the Edge: The Challenge of Traffic Distribution

Contents

Executive Summary

Connected Vehicles are swiftly transforming the automotive industry, with emerging services driving major new requirements for data communications. In principle, every new vehicle manufactured will be continuously connected and will generate massive volumes of data to be transferred between vehicles and the cloud. New Connected Vehicle services are expected to make the Automotive sector the industry segment with the fastest-growing demand for mobile machine-to-machine connectivity. Stakeholders in this industry vertical include vehicle OEMs, technology solution vendors, network operators, cloud infrastructure and service providers. The challenge is in designing and deploying the communication networks and computing ecosystem required to efficiently deliver and process the new high-volume data requirements.

Considering the global nature of this challenge, stakeholders should consider how communication networks and computing resources could be orchestrated to enable secure, cost-effective data delivery and processing on a global scale. To address this challenge, the Automotive Edge Computing Consortium (AECC) has proposed a “Distributed Computing on Localized Networks” solution concept and architecture to ensure service flexibility, efficiency and continuous evolution of the automotive industry. The solution consists of three main aspects: the Localized Network, Distributed Computing and Local Data Integration. This Technical Report, which is a summary of the comprehensive study performed by Consortium members, focuses on three of the key issues pertaining to data integration within a Localized Network. These are:

Edge data offloading. A new architectural approach is required for cellular networks to support the offloading of data in an efficient and flexible manner to the appropriate local distributed computing environment. This occurs in the cellular network when it connects to the Mobility Service Provider (MSP) Edge Servers.

MSP Server Selection. A dynamic process is required to enable selection and use of computing resources by the set of connected services and applications. For multiple concurrent services used by a Vehicle System, connections may be required to multiple MSP Servers. Highly dynamic network topologies will need flexible addressing schemes to establish an easily maintainable system with seamless integration into existing infrastructure.

Vehicle System Reachability. Connected services must have the ability to contact a Connected Vehicle. This may be challenging due to the mobility of Connected Vehicles and end-to-end network segmentation. Out-of-service conditions may occur when a Vehicle System moves into an area without access network coverage or handover fails between different access networks. A mechanism is required to ensure the reachability of a Vehicle System according to the identified service requirements.

To help stakeholders systematically address these issues, the AECC has identified and evaluated a range of potential solutions. This Technical Report provides recommendations in terms of different deployment options. Furthermore, the AECC continues to work on other key issues and solutions relating to the Localized Network aspect and those of Distributed Computing and Local Data Integration. Additional key issues and corresponding studies will be released in future AECC publications. The AECC is also open to feedback on the findings and recommendations in this Technical Report and will take that into consideration in the continuing work.

The members of the AECC are working to articulate a path for addressing the critical industry needs. Ultimately, the actions taken will determine whether the promise of Connected Vehicles actually delivers the anticipated benefits to vehicle owners and users, vehicle OEMs and the ecosystem of service providers.

Terms and Abbreviations

Terms:

Cloud	A logical server that hosts services to store, manage and process data; system is composed of a set of remote servers accessed via the internet.
Connected Vehicle	Network attached vehicle that exchanges data with the cloud and other network attached devices and servers.
Center Server	Computing hardware and software deployed in cloud or on premise to provide Connected Vehicle services.
Distributed Computing	A computing system that divides a problem into many tasks that are processed by multiple computing instances.
Edge Computing	A type of distributed computing system where the computing process is allocated to computing instances located in the Network Edge in order to provide desired service levels.
Edge Server	Computing hardware and software deployed at a suitable location within the network to provide a good balance among performance, efficiency and availability for Connected Vehicle services.
Intelligent Driving	A service that augments an Advanced Driver Assistance System (ADAS) or an Automated Driving System with strategic decisions based on predictions of conditions along route alternatives that are gathered using connectivity to external sources.
Local Data Integration	A platform that integrates data on the Localized Network and the distributed computation system.
Localized Network	A local network that covers a limited number of Connected Vehicles in a certain geographical area.
Mobility as a Service	Integration of various forms of transport services into a single mobility service accessible on demand.
Mobility Service Provider	A platform-independent provider that provides customers with access to one or more Connected Vehicle services.
Network Edge	One or more locations within a network domain in close adjacency to the source of the data producer/consumer.
Telematics	The technology of sending, receiving and storing information using telecommunication devices to control remote devices/vehicles and to provide services based on this information.

V2Cloud	Communication between a vehicle and services hosted in the cloud.

Abbreviations:

3GPP	The 3rd Generation Partnership Project
5G	5th Generation
5GS	5G System
ADAS	Advanced Driver Assistance System
API	Application Programming Interface
APN	Access Point Name
C-V2X	Cellular Vehicle-to-Everything
CAN	Controller Area Network
CUPS	Control User Plane Separation
DNS	Domain Name System
DSRC	Dedicated Short Range Communication
ECU	Electronic Control Unit
eNB	Evolved Node B (LTE Base Station)
EPC	Evolved Packet Core
EPS	Evolved Packet System
FQDN	Fully Qualified Domain Name
gNB	Next Generation Node B (5G Base Station)
GTP	GPRS Tunneling Protocol
HTTP	HyperText Transfer Protocol
IaaS	Infrastructure as a Service
IoT	Internet of Things
LTE	Long Term Evolution (The 4th Generation Mobile Communication System)
M2M	Machine to Machine
MaaS	Mobility as a Service
MME	Mobility Management Entity
MNO	Mobile Network Operator
MSP	Mobility Service Provider
NAPT	Network Address Protocol Translation
NAT	Network Address Translation
NEF	Network Exposure Function
NR	New Radio
OEM	Original Equipment Manufacturer
OS	Operating System
OTA	Over the Air
PaaS	Platform as a Service
PDN	Packet Data Network
PDU	Packet Data Unit
P-GW	Packet Gateway
P-GW-U	P-GW User Plane
S-GW	Serving Gateway
S-GW-U	S-GW User Plane
SCEF	Service Capability Exposure Function

SIPTO	Selected IP Traffic Offload
SLA	Service Level Agreement
SSC	Session and Service Continuity
UE	User Equipment
UL-TFT	Uplink Traffic Flow Template
UPF	User Plane Function
UUID	Universally Unique Identifier
WLAN	Wireless Local Area Network
XMPP	Extensible Messaging and Presence Protocol

1 Introduction

Connected Vehicles are anticipated to be a significant factor contributing to mobile traffic growth, with forecasts projecting every new vehicle produced being "connected" by 2025 [1]. Millions of cars are already connected using 4G cellular access, and cellular broadband IoT connectivity (4G/5G) is expected to grow significantly through 2024 as outlined in the Ericsson Mobility Report [7] and visualized in the Ericsson Mobility Visualizer [8]. According to the Cisco Visual Networking Index, Connected Vehicles that incorporate applications such as fleet management, in-vehicle entertainment, internet access, roadside assistance, vehicle diagnostics, navigation and advanced driver assistance services will be the fastest-growing industry segment with respect to machine-to-machine connections [2]. Furthermore, many emerging automotive services, such as intelligent driving assistance and Mobility as a Service (MaaS), expect vehicles to be connected to cloud computing facilities. The AECC estimates that the related data traffic has the potential to exceed 10 exabytes per month by 2025, a volume 1,000 times larger than the present numbers as described in an AECC white paper [3].

Vehicle data communications and processing present a significant challenge when considering currently deployed architectures. Stakeholders in this industry vertical, such as vehicle OEMs, technology solution vendors, network operators, cloud infrastructure and service providers, must establish a practical platform architecture capable of supporting the variety of Vehicle-to-Cloud (V2Cloud) services. Vital considerations include the communication network architectures and computing infrastructure that will be needed to support these emerging services.

The cellular network is one of the major access networks for Connected Vehicles, and many specifications have been standardized in the 3rd Generation Partnership Project (3GPP). However, the present work within 3GPP has not fully addressed the challenge of automotive big data, and there is a high risk that future network deployments and business models will fail to support the emerging needs of connected vehicles. The cellular vehicle-to-everything (C-V2X) communication considered in 3GPP, for example, mainly covers latency-sensitive safety applications and does not address the big data capacity growth between vehicles and the cloud. The 5G cellular system will provide improved functionality for both capacity and low latency but the automotive industry will continue to use a mix of cellular access network technologies for the foreseeable future. In addition, increased data volume aggregated into data centers will cause network congestion that degrades the user experience of Connected Vehicles.

The AECC believes that the current mobile communication network architectures and cloud computing deployments are not fully optimized to effectively handle emerging requirements of Connected Vehicles on a global scale. In response, this Technical Report presents a proposal for how to design an appropriate system architecture and consider network deployments that will be able to efficiently accommodate the predicted high volumes of data traffic from Connected Vehicles. The AECC proposes the use of a "Distributed Computing on Localized Networks" solution concept to solve these issues. The concept focuses on three main aspects, which are the Localized Network, Distributed Computing and Local Data Integration.

The end-to-end system architecture provides a framework that supports the distribution of computation processes across a set of Localized Networks, as shown in Figure 1.

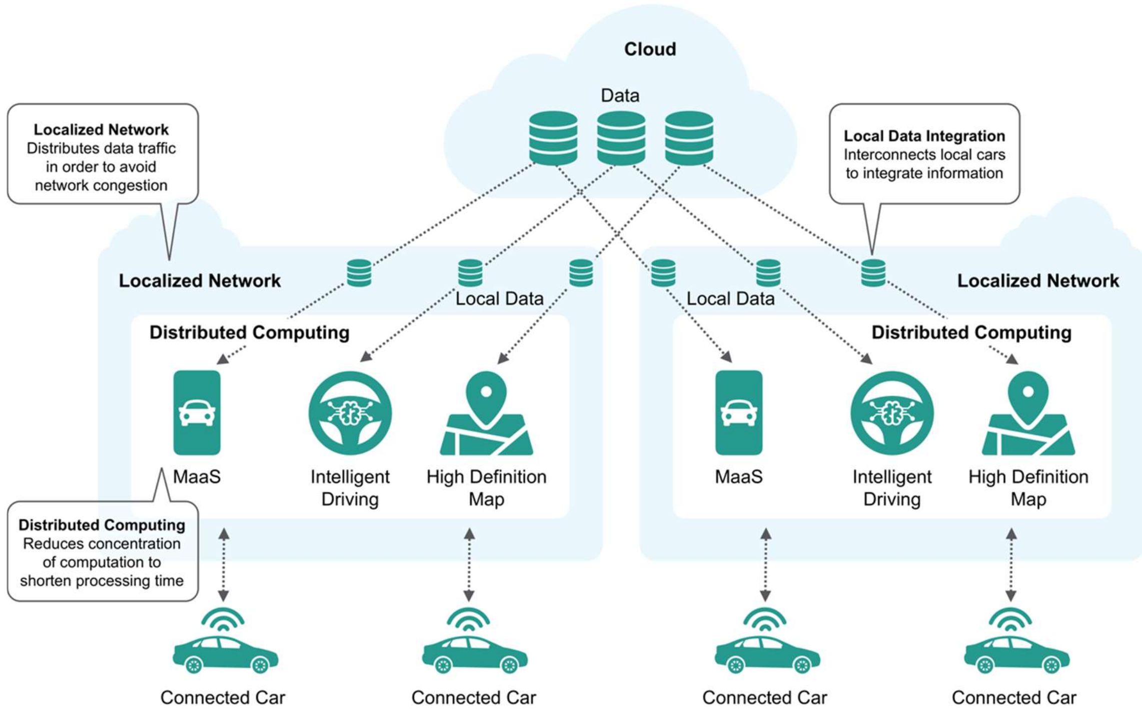

Figure 1. Three pillars of the AECC concept.

This Technical Report provides a summary of the initial areas of study, as the AECC continues the work to define how to build a Localized Network that can support the distributed data processing needs of Connected Vehicles.

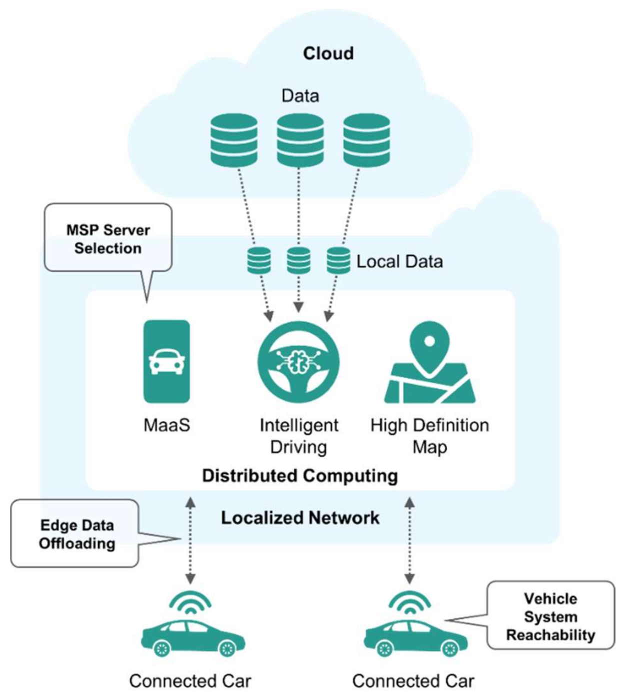

Figure 2. Three key issues addressed by this Technical Report.

The AECC has identified a set of key issues, three of which were prioritized for study as shown in Figure 2. The first issue is that of "edge data offloading," where cellular networks have to support the offloading of data in an efficient and flexible manner to the appropriate local distributed computing environment. Second, the computing resources should be selected and allocated in a dynamic manner together with the ability to reroute data traffic in order to satisfy the requirements of services. Third, services should have the ability to contact a Connected Vehicle. In order to address these issues, the AECC identified and evaluated a range of potential solutions and has provided recommendations in the form of different deployment options.

2 System Overview

2.1 Architectural Requirements

The AECC proposes a system that will support the deployment and execution of AECC-defined services using a distributed computing and networking architecture, including the Vehicle System, Network (Cellular Network, WLAN, MSP Enterprise Network, etc.) and Center/Edge Servers operated by a Mobility Service Provider (MSP).

The AECC system architectural requirements related to the Cellular Network shall apply to both EPS and 5GS. Also, it shall apply to the non-standalone NR deployments, where the core network is EPC and the UE connects to anchor eNB, providing the control plane, and gNB used for data communication.

The Vehicle System in the AECC system will connect to a WLAN when applicable. The WLAN may use Wi-Fi (IEEE802.11) as an access technology or 3GPP-based access technology (e.g., NR in mmWave carriers). The WLAN can connect to the cellular core network or to an internet service provider network.

The Vehicle System in the AECC system will connect to the MSP Enterprise Network when applicable. The access technology in the MSP Enterprise network may use Wi-Fi (IEEE802.11) or 3GPP-based access technology. The core network in the MSP Enterprise Network may be based on proprietary technology or 3GPP-based core network technology (e.g., EPC, 5GC).

The AECC system includes a distributed computing environment that will be used to support the various applications. Computing functions are expected to be performed within the Vehicle System, the MSP Center Server and the MSP Edge Servers.

2.2 Reference Architecture for Data Traffic Distribution

2.2.1 Cellular Network Reference Models

For the case where LTE is the only radio access used, the EPS architecture reference model is assumed by the AECC [3].

For the case where non-standalone NR is used as the radio access, AECC assumes the EPS architecture reference model according to 3GPP Release 15 and later (see [4]), with a non-standalone architecture option. Figure 3 and Figure 4 show a non-roaming architecture as an example.

The 5GS architecture reference model used by AECC is 3GPP 5GS Release 15 (see [5]) or later. It includes standalone NR deployment and multiple access dual connectivity options, with both NR and LTE radio connection to 5GC.

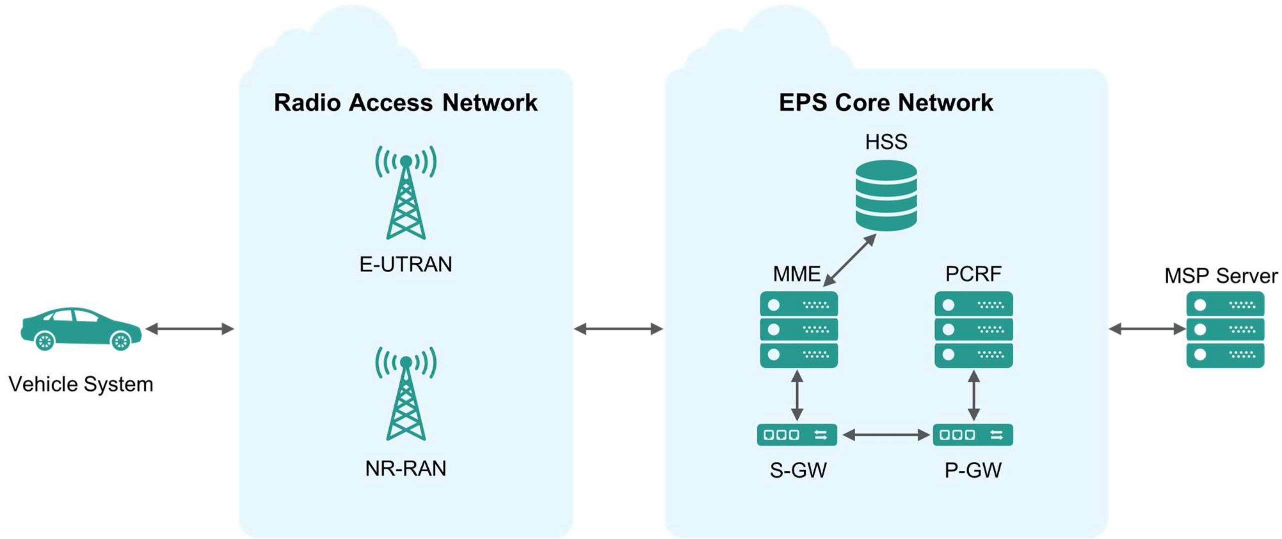

Figure 3. EPS architecture reference models with non-standalone NR radio access.

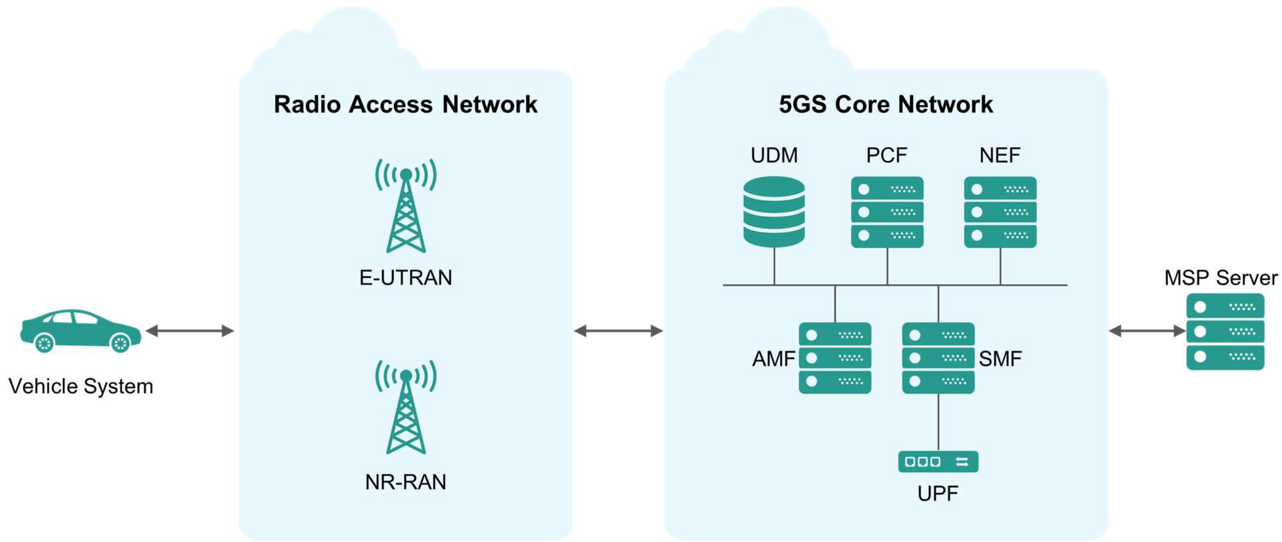

Figure 4. 5GS architecture reference models.

2.2.2 Distributed Computing Architecture Reference Model

The AECC System introduces a hierarchical data processing architecture shown in Figure 5, where the data will be processed at the Edge Servers located at the proper places in the network between the Cloud and Connected Vehicles.

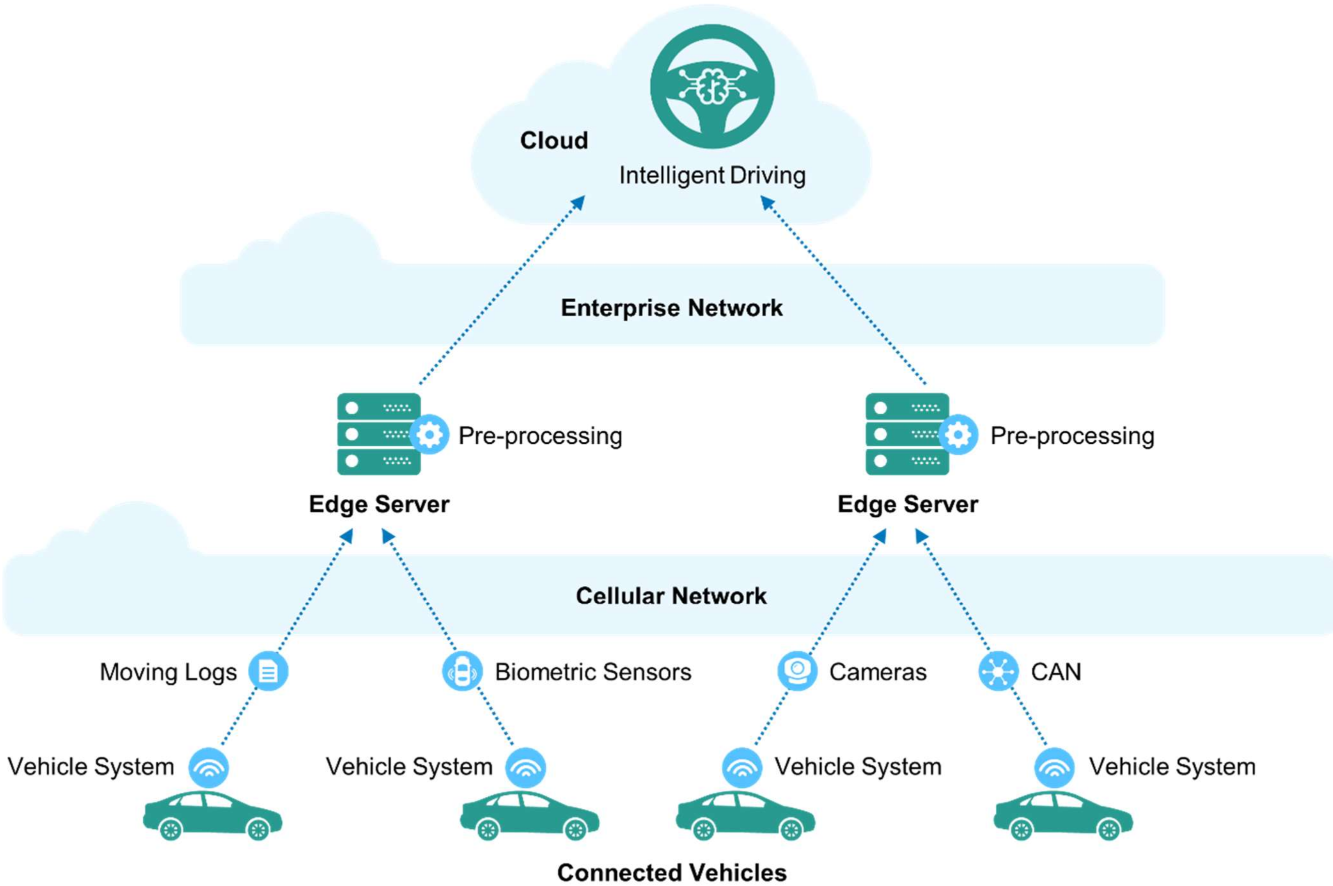

Figure 5. AECC System hierarchical data processing architecture.

2.2.2.1 MSP Server – Layered Model

The AECC system is intended to support Vehicle Systems and applications from multiple vehicle OEMs operating at the same time. The system needs to be able to accommodate a number of different approaches to perform the core task of creating a distributed computing environment where applications can be executed in a distributed manner.

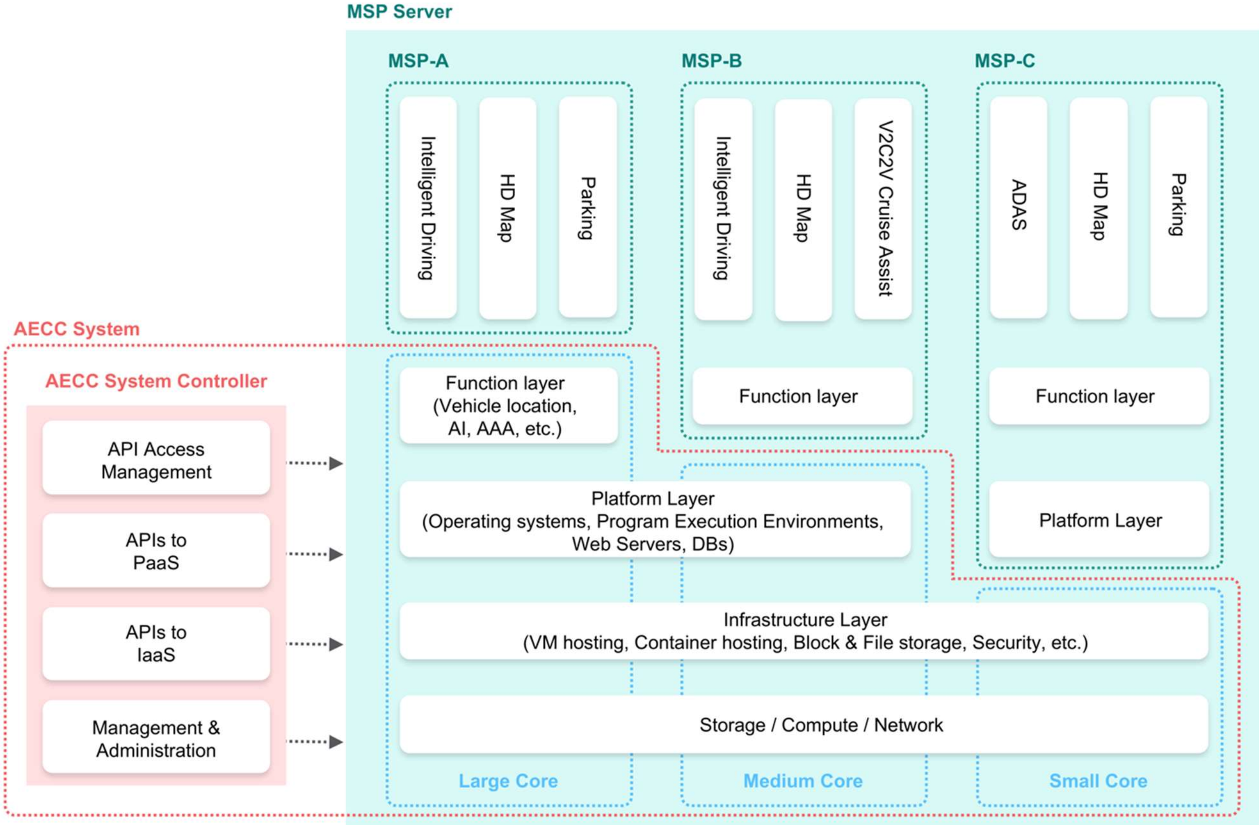

Figure 6. Layered-model architecture illustrated with example applications and different deployment options.

The architecture in Figure 6 will evolve over time, and it illustrates the potential core set of functions available for use by MSPs in an AECC System. In the "small core" approach, the AECC system would offer a base set of capabilities covering the provision of hardware in the form of Storage, Computing and Network services. An Infrastructure Layer handles the provision and operation of services on top of the underlying hardware in an Infrastructure-as-a-Service (IaaS) approach. The small core approach enables MSPs to build their own Platform and Function layers, on top of which providers can run their applications.

In the "medium core" approach, the AECC system will bring additional value by offering a platform layer containing a set of services such as operating systems and programming language execution environments (Python, Go, etc.), as well as functions such as Message Buses, Databases and so on. The medium core approach enables MSPs to build their own Function layers, on top of which they can run their applications. Each MSP can create its own stack, which can then be deployed on the medium core, knowing that each AECC system instance (MSP-Center server/s and MSP-Edge server/s) will always offer a uniform set of Platform-as-a-Service (PaaS) and IaaS capabilities.

In the "large core" approach, the AECC system will bring additional value by offering a function layer containing a set of services such as vehicle location finding, artificial intelligence libraries, security functions and so on. The large core approach enables MSPs to build their own applications using the functions and capabilities provided by the platform. Each MSP can create its own application suite, which can then be deployed on the large core, knowing that each

AECC system instance (MSP-Center server/s and MSP-Edge server/s) will always offer a uniform set of Function, PaaS and IaaS capabilities.

Complementing each of these approaches is an additional AECC System Controller element. The purpose of the System Controller is to provide management capabilities to each of the layers within the AECC system, exposing interfaces that the platform operator can leverage to perform lifecycle management as well as APIs for use by the MSP. For example, the diagram above in Figure 6 shows how MSP-C will use the IaaS API in order to provision virtual machines for its needs. The API access management function would provide a mechanism to control API interfaces for enabling or disabling users, API tokens and so on.

The layered design shown in Figure 6 is intended to appeal to the broadest set of potential users to ease adoption. The layered approach also assists with system design longevity, enabling components within each of the layers to be replaced as new technologies and solutions become available, without requiring a redesign of the system architecture.

In general, additional options are possible, such as MSPs building their own infrastructures and Platform layers while using an AECC Function layer as a microservice or using AECC Platform layer elements mixed with MSP-owned and defined Platform layer elements.

3 Key Issues and Solutions

3.1 Edge Data Offloading

3.1.1 Key Issue

In order to alleviate the pressure of emerging high-volume data transfer identified in the AECC white paper [3], the Cellular Network (both EPS and 5GS), as shown in Figure 7, shall support data offloading to the designated MSP Edge Servers. The MSP Edge Servers are connected to the MSP Center Server via MSP Enterprise Network as defined in the AECC distributed computing architecture reference model (Section 4.2.2). In a Cellular Network, all traffic must enter and leave the network at specific data offloading points on the network side. According to the deployment of MSP Edge Server instances, these data offloading points shall be selected at appropriate locations in the Cellular Network to meet the service requirements on latency and capacity.

Note 1: The traffic flows of different services may selectively offload to different MSP Edge Servers to meet the various requirements of service use cases.

Note 2: The case of data offloading when using different access networks, such as WLANs, is discussed in Section 4.2, Access Network Selection.

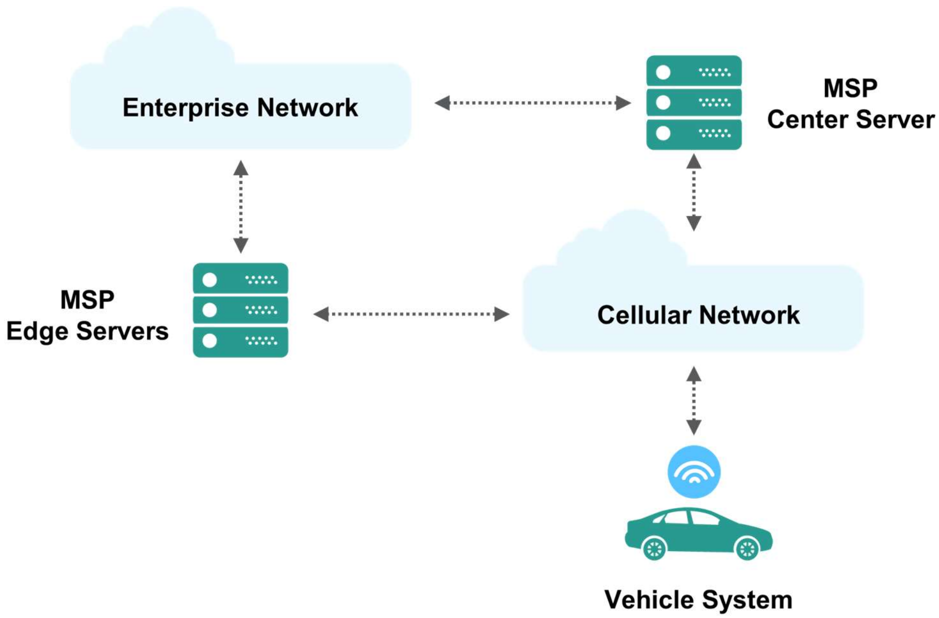

Figure 7. Connectivity between the Vehicle System and MSP Servers can be provided over a Cellular Network, in which case appropriate data offloading points must be selected in the Cellular Network.

3.1.2 Potential Solutions

3.1.2.1 Solutions Overview

Edge Data Offloading in the Evolved Packet System

In the Evolved Packet System (EPS), PDN-Gateways (P-GWs) act as data offloading points of the Cellular Network. The Control and User Plane Separation (CUPS) feature provides more flexibility when it comes to data offloading and splits the P-GW functionality into a control plane entity (P-GW-C) and a user plane entity (P-GW-U). Once a PDN Connection from User Equipment (UE) to such a P-GW-U is established, it cannot be re-anchored to a different P-GW. Provided the PDN Connection persists, all traffic will be offloaded to the initial P-GW-U (see Figure 8).

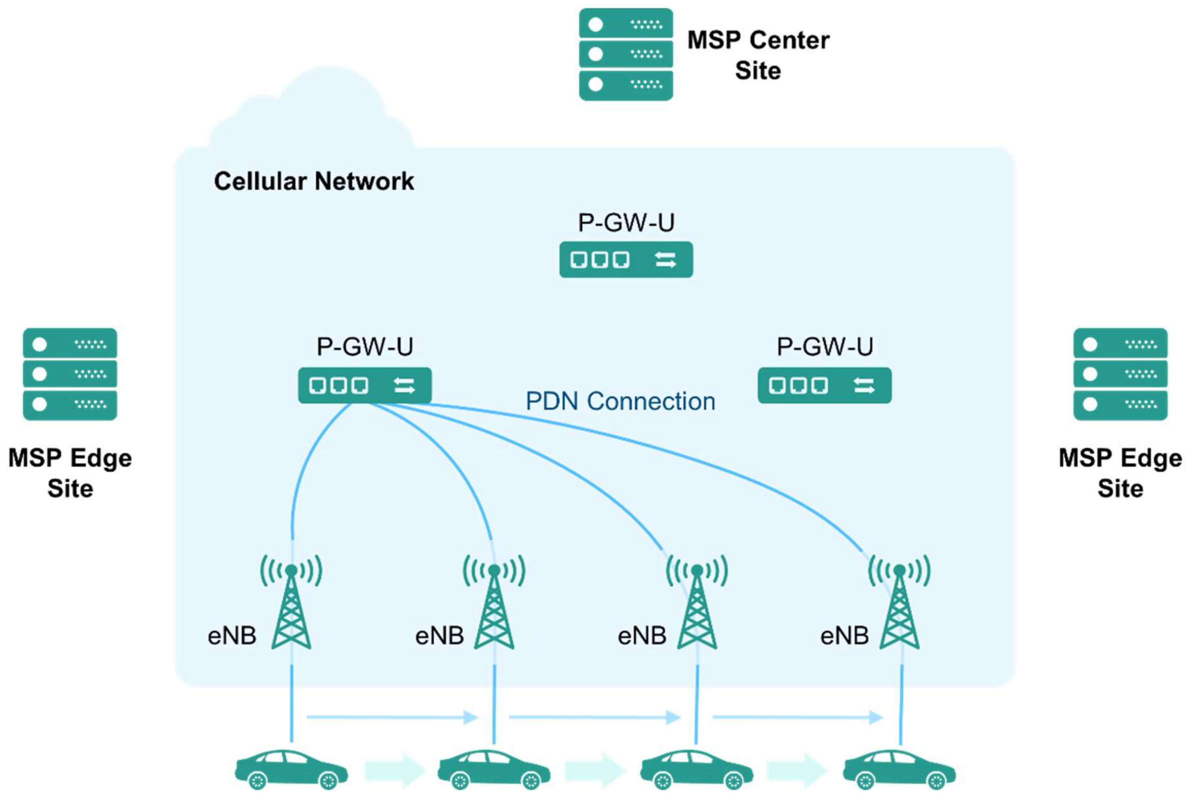

Figure 8. Vehicle moving with persisting PDN Connection in EPS.

For re-initiating the P-GW-U selection procedure, the PDN Connection must be reactivated or a new PDN Connection must be established. The latter case is done during a re-attach procedure, which automatically happens when connectivity is reestablished after it was lost, such as due to large radio coverage white spots. During the attach procedure, the MME will then select an appropriate P-GW-U for the PDN Connection, based on the operator's configuration, such as tracking area.

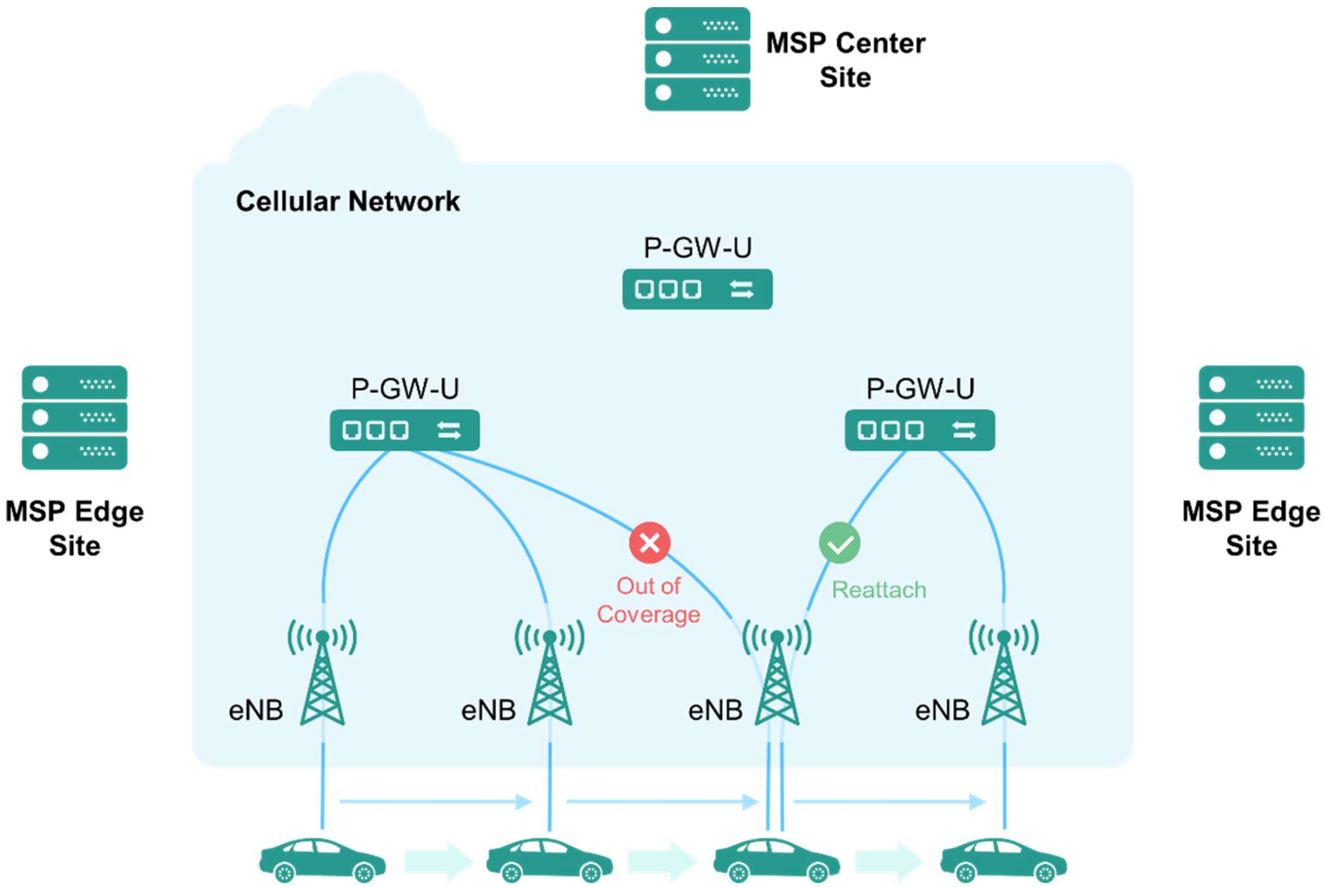

Figure 9. Vehicle moving with changing PDN Connections in EPS.

When running into a large coverage white spot, the PDN Connection is terminated and a new PDN Connection is created when returning to coverage. This assures proper selection of an appropriate P-GW-U. If a Cellular Network has several white spots between areas that should be served by different P-GW-Us,[1] mobility might not be an issue, as the P-GW-U is automatically reselected on a regular basis. However, with many P-GWs deployed and more continuous coverage, a PDN Connection reactivation must be triggered by the system. For this purpose, EPS provides an optional feature ("Selective IP Traffic Offload [SIPTO] above RAN") where the MME requests a PDN Connection deactivation with a subsequent reactivation to the UE (see Figure 10).

[1] Note: This is a typical case for spotty coverage in rural areas with a low degree of P-GW-U distribution.

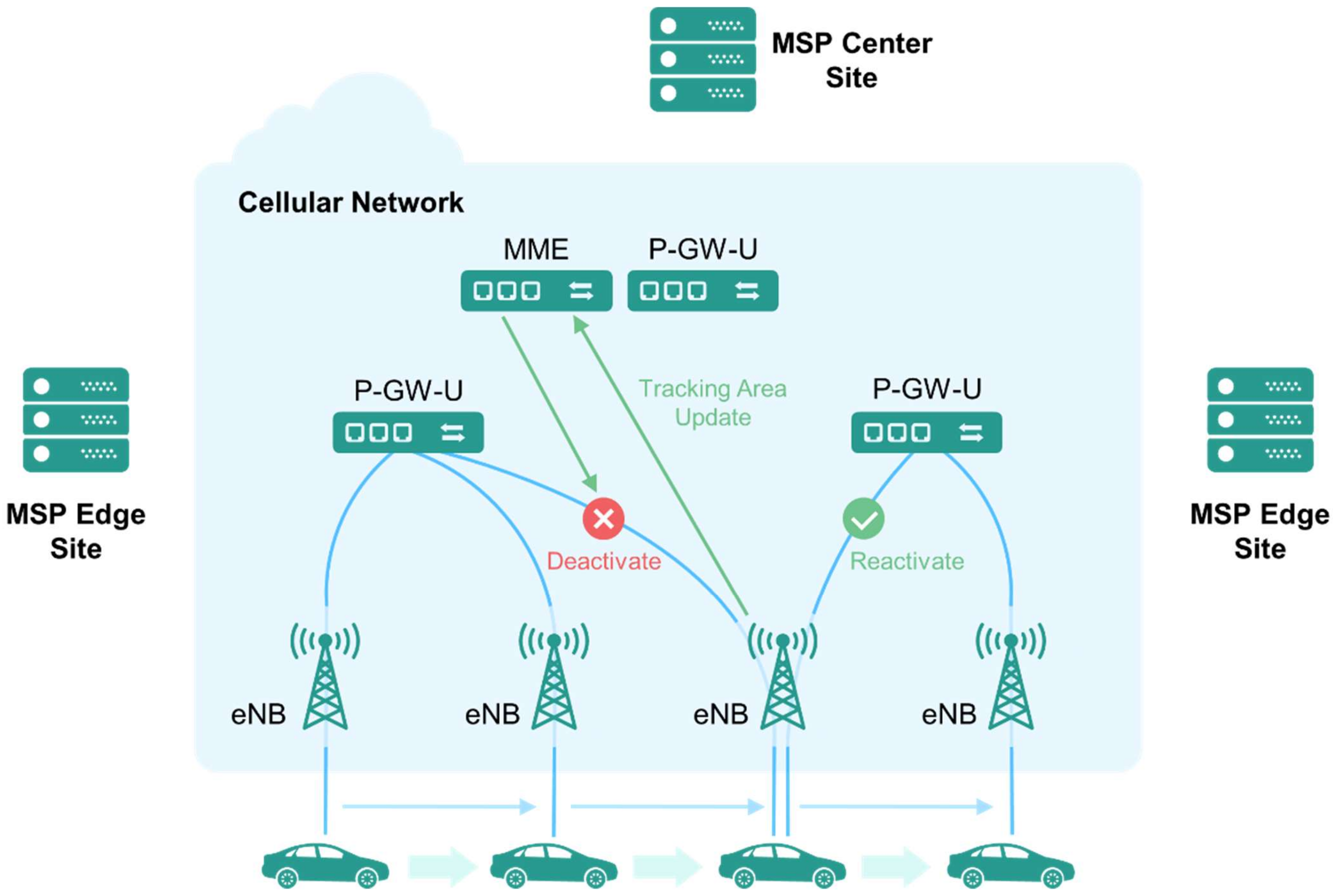

Figure 10. Reactivation of the PDN Connection with SIPTO.

When using only a single PDN Connection per instance of UE, even data exchanges between a Vehicle System and an MSP center site go via the current edge P-GW-U (see Figure 11, right car). This may require over-dimensioning the edge P-GW-U if the share of data is relevant and geographically varying. In that case, the load on the edge P-GW-Us can be reduced by using a second PDN Connection on the same UE, with a different APN that is configured for anchoring at a central P-GW-U (see Figure 11, left car). In that case, two IP interfaces must be managed on the Vehicle System.

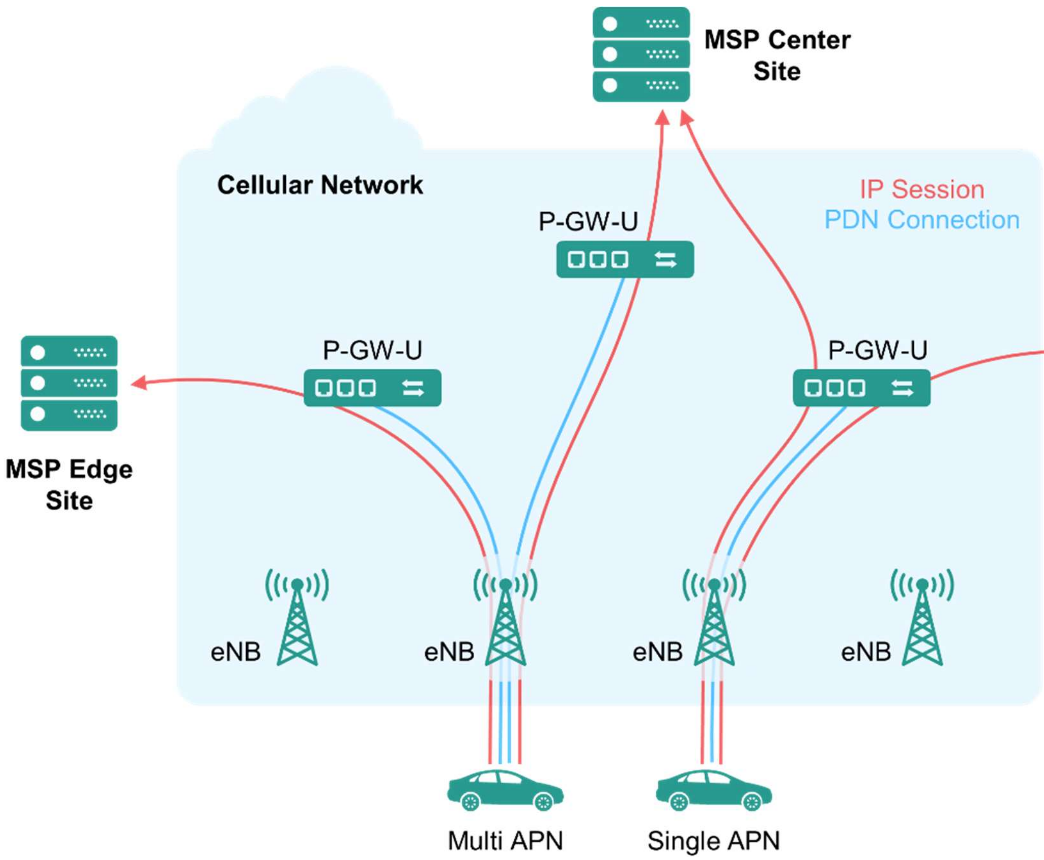

Figure 11: Offloading edge GWs with a second PDN Connection.

Edge Data Offloading in the 5G System

The 5G System (5GS) has the same paradigm of an existing central anchor point (the PDU Session Anchor in the User Plane Function [UPF]). This requires similar solutions with a single PDU Session that offloads at the edge. However, compared to the EPS, the 5GS supports multiple Session and Service Continuity (SSC) modes that control the behavior during mobility. Depending on the SSC mode, a PDU Session will persist until running out of coverage (SSC mode 1), a PDU Session may be released and immediately re-established to a new UPF during mobility (SSC mode 2, SIPTO-like behavior) or a new PDU Session may be established during mobility before releasing the old PDU Session (SSC mode 3). Just as in EPS, an additional PDU Session, anchored at a central UPF, can be used to reduce the load on edge UPFs.

While the features described above enable a Vehicle System to always have connectivity via appropriate data offloading points, ongoing sessions are interrupted during re-attachment procedures. The 5GS also offers mechanisms to maintain connectivity during mobility and still re-anchor the PDU Session at a different UPF. Namely, an uplink classifier (ULCL) policy can be provisioned in a UPF to offload the selected traffic to an Edge Server, and the SMF can dynamically insert and remove an uplink classifier into the data path of the PDU Session (see Figure 12). Typically, IP 5-tuples are used in such policies to decide which packets to offload to which edge site.

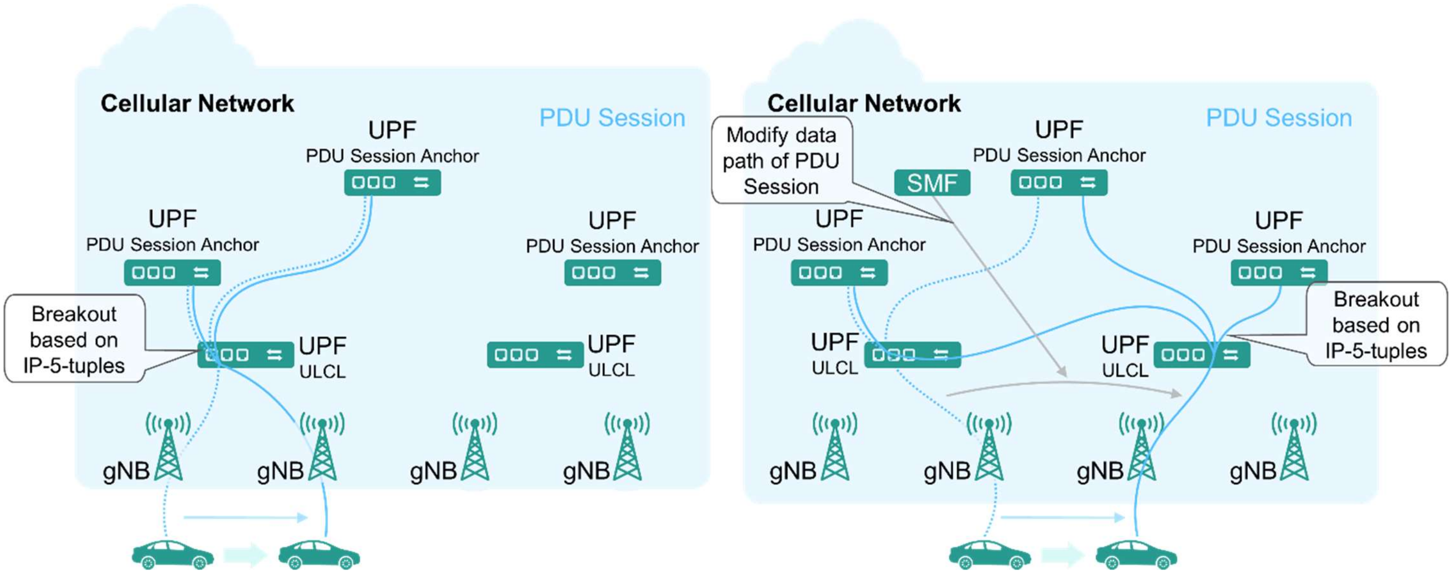

Figure 12: Selectively routing packets with Uplink Classifiers.

In this approach, while there are multiple PDU Session anchors, there is only one IP anchor. Even during mobility, the IP session is maintained while traffic to the old uplink classifier UPF is tunneled. This communication link is deactivated when not used anymore; e.g., when using timeout procedures (see Figure 13). For downlink traffic, the Vehicle System is reachable using the same IP via all UPFs, which must be considered in the IP configuration of the MSP Servers and the corresponding IP network(s).

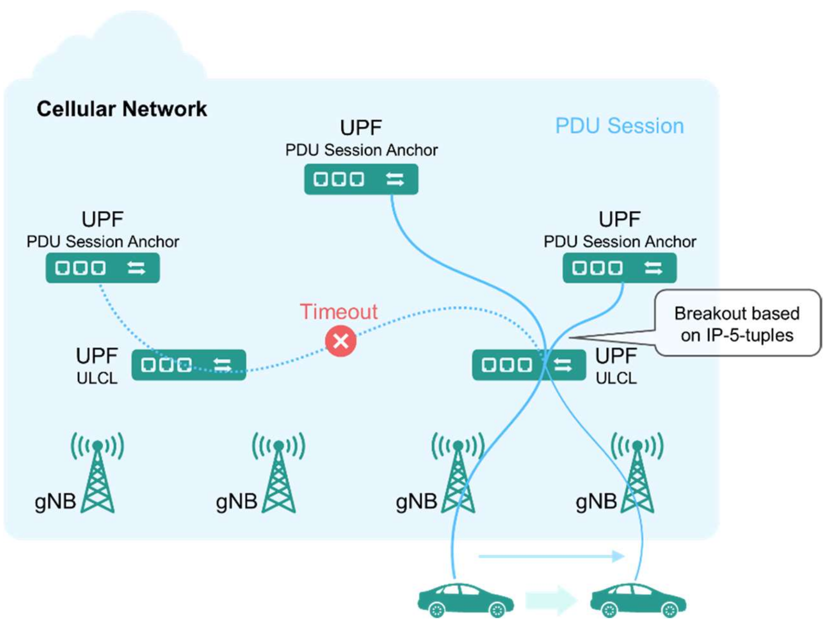

Figure 13: Terminating an unused link with timeout procedures.

3.1.2.2 Solution 1 – Data offload with Single PDN Connection in EPS

In EPS, SIPTO above RAN enables dynamic reselection of GWs (S/ P-GW), and selection of GW-Us in the case of Control and User Plane Separation (CUPS) that are geographically/topologically close to the UE. The selection mechanism can consider UE mobility location (Tracking Area), APN or other parameters.

A UE does not need to be aware of whether the PDN Connection corresponds to the MSP Edge or Center server. One AECC dedicated APN can be provisioned to the UE for all AECC traffic flows – including traffic with and without offloading. When the UE uses this AECC APN, it does not need to know whether or not traffic on this APN will be offloaded. The network (MME) will choose appropriate GWs for AECC APN traffic. The GW (S-/P-GW or S-/P-GW-U) selection will be based on information such as SIPTO permission information per subscription per APN, UE location information and so on. The MME can also decide to move a PDN Connection from one GW to another (e.g., from a GW serving MSP Edge Server to a GW serving MSP Center Server) for AECC APN if needed.

The different types of AECC traffic flow will be offloaded to the applications on the MSP Edge Server or pass through to the MSP Center Server as shown in Figure 14.

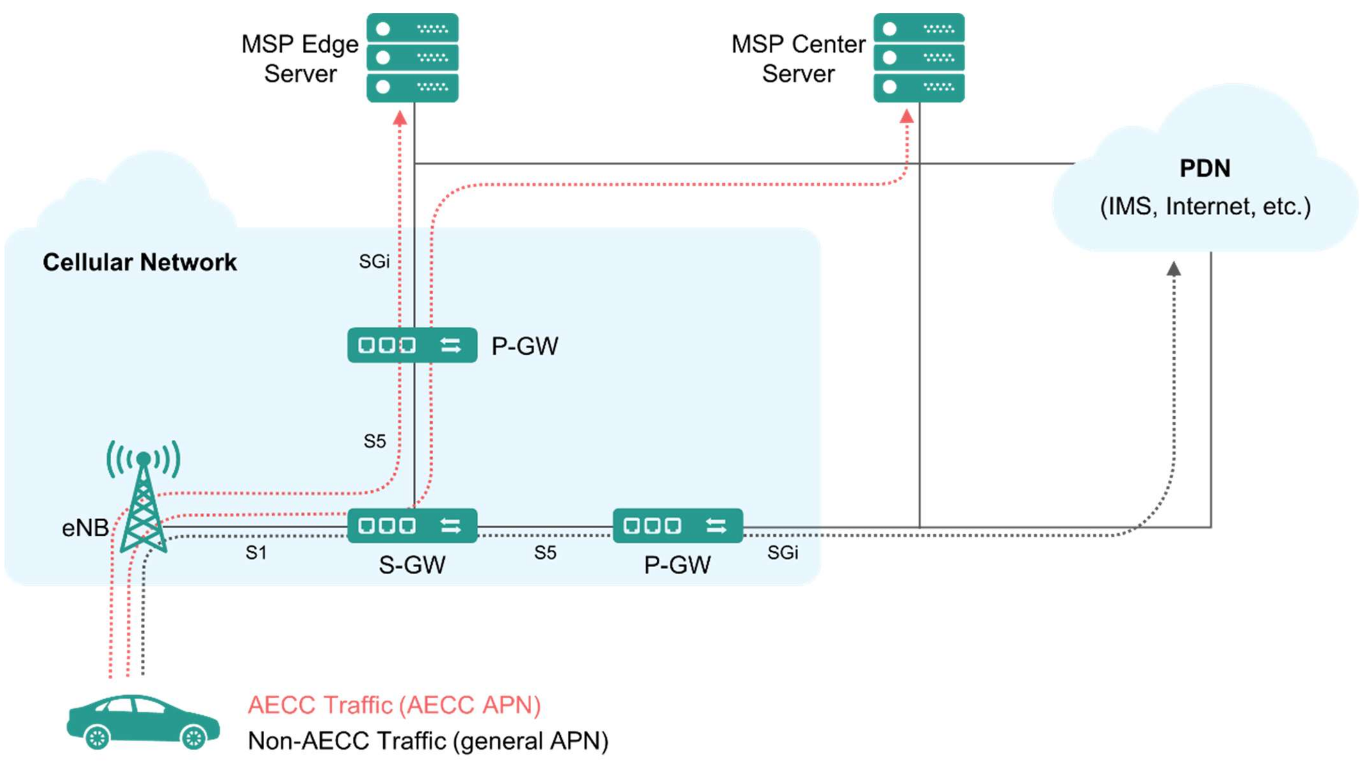

Figure 14. Data offload with Single PDN Connection for AECC-related traffic (red) and other traffic (black) in EPS.

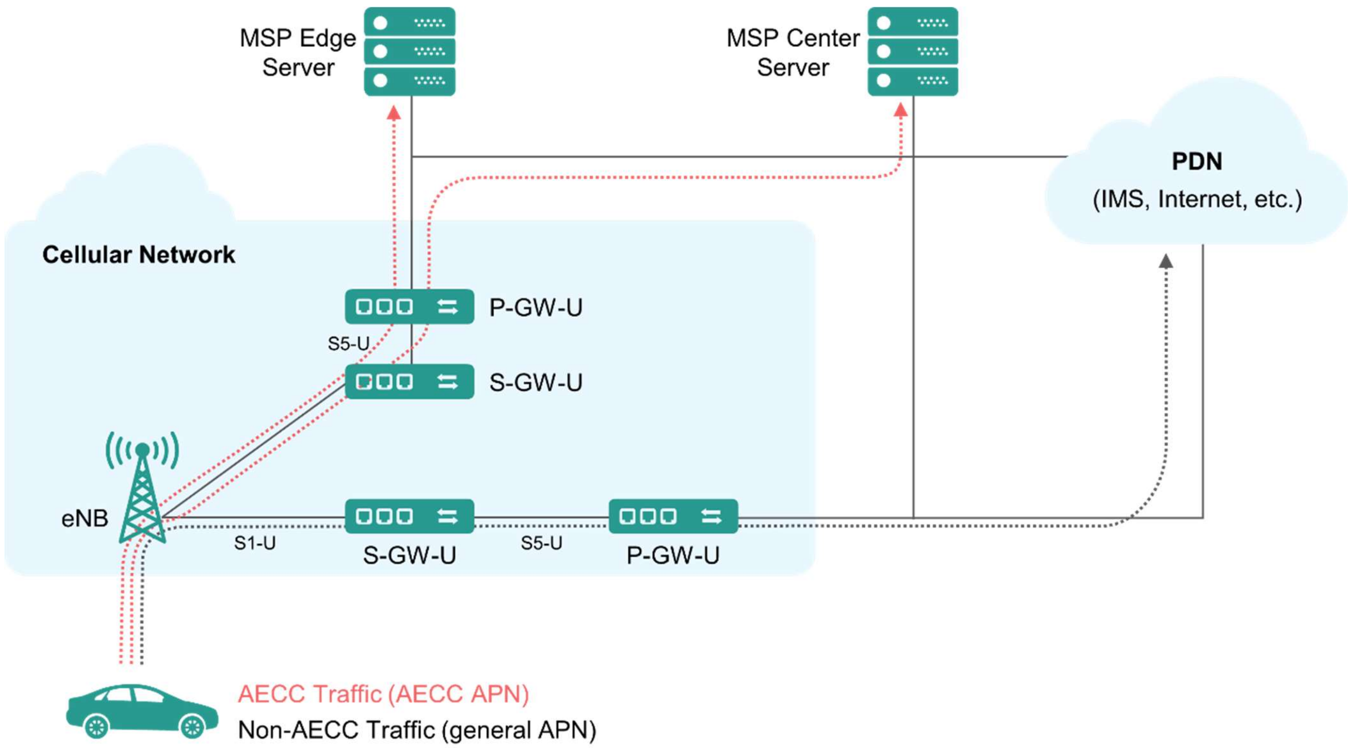

Figure 15. Data offload with Single PDN Connection for AECC-related traffic in EPS in the case where CUPS is deployed.

3.1.2.3 Solution 2 – Data offload with Multiple PDN Connections in EPS

SIPTO above RAN enables the Cellular Network to offload data traffic sent through a PDN Connection for an APN configured for SIPTO to a designated MSP Edge Server via a selection of P-GW (or P-GW-U in the case of CUPS). It is a function introduced and standardized since 3GPP LTE Release 10. SIPTO requires a dedicated APN for offloading the selected data traffic to the Edge Server, so it needs to support multiple APNs for different PDN Connections at the UE side to achieve a selective data offload.

Due to UE mobility, the serving MME may need to redirect a PDN Connection to a different P-GW that is more appropriate for the location of the UE, based on the tracking area of the Vehicle System. In this case, this solution cannot maintain session continuity while changing to the new P-GW.

The GW selection is configured by the MNO through tracking area configuration and mapping to GWs; that is, no direct control to external entities is provided in the current solution. For selecting which PDN Connection to use for a packet in the uplink, one can either push the selection process to the application layer in the UE or use UL-TFTs for doing an automatic mapping based on IP 5-tuples. For downlink, one can select a PDN Connection by using the respective IP address assigned by the corresponding GW.

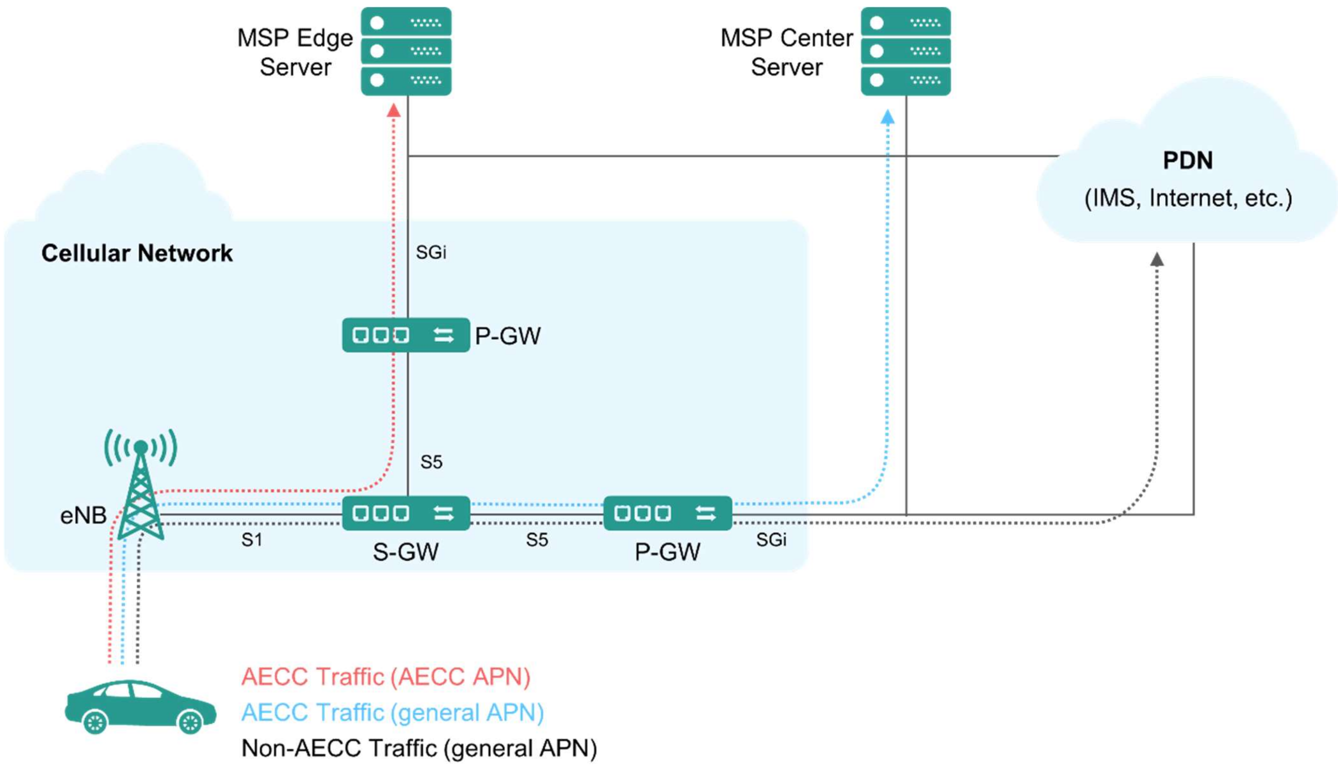

Figure 16. Data offload with Multiple PDN Connections for AECC-related traffic (red & blue) and other traffic (black) in EPS.

3.1.2.4 Solution 3 – S1/N3 GTP Packet Filtering in EPS and 5GS

Edge data offloading can be conducted based on S1 GTP packet filtering mechanisms. The whole solution should include:

- Packet filtering, also called a traffic filter policy
- Packet filtering management

To support edge offloading in the Cellular Network, a traffic filter solution to handle the traffic offloading of the data plane can be used. For the packet filtering policy, a set of traffic filter policies composed by traffic rules and traffic filters corresponding to the rules is shown in Figure 17.

For example, such a TrafficFilter policy could use IP header information (IP Address, Port, L4 protocol) or consider L4/L7 parameters when feasible. If the edge offloading resides on the S1 interface inside the Cellular Network, it can also support filtering based on GTP tunnel information such as GTP-U TEID and so on. The policy also includes actions such as forward, drop, passthrough and duplicate.

For the packet filter policy (TrafficFilter policy) management, the system uses an architecture solution to address policy management for edge offloading inside 4G or 5G Cellular Networks. The management plane of the AECC

System conducts the traffic rule management to influence the data plane of the AECC System to conduct traffic filtering and related actions.

The solution for the packet filter is shown in Figure 17.

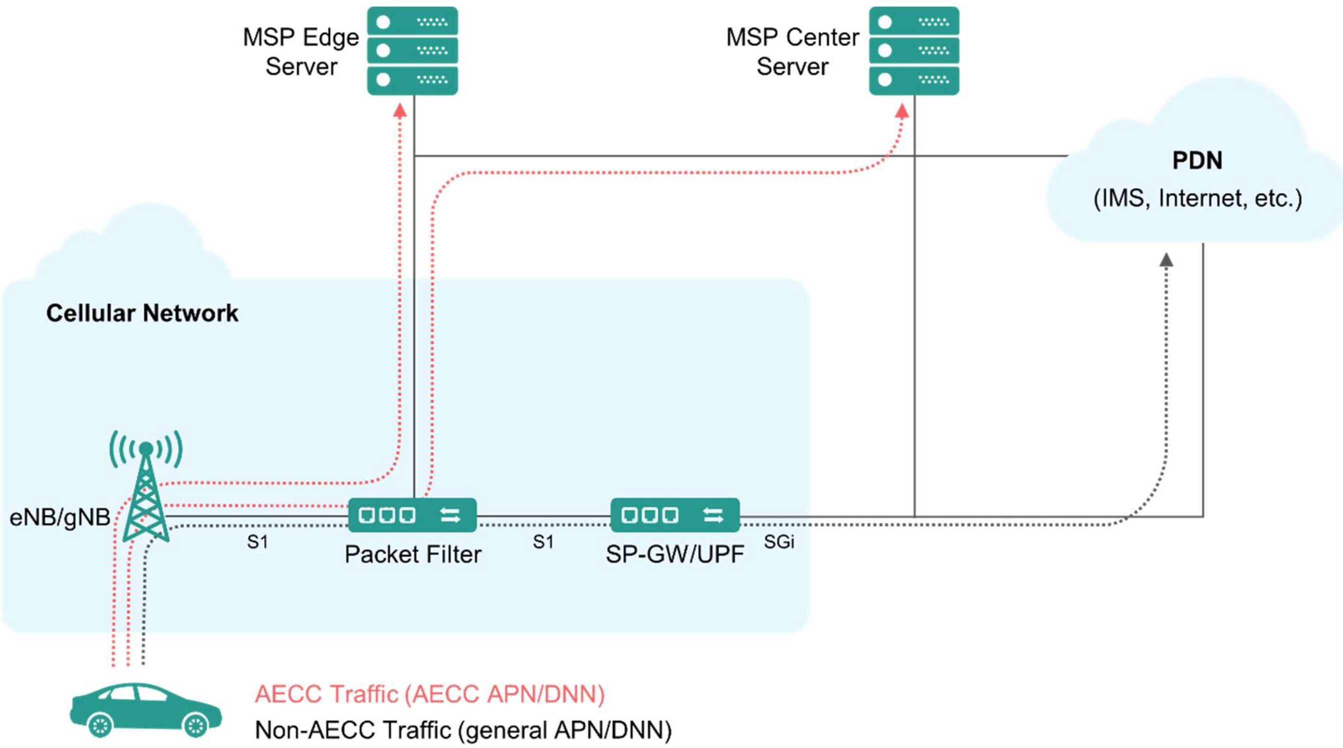

Figure 17. GTP Packet Filter implementing traffic filter policy.

Note 1: The Platform Manager will send the TrafficRule configuration to the edge server to instruct the packet filter to conduct edge data offloading. In Figure 17, the Platform Manager can reside inside MSP servers as a logical function block.

In Figure 17, a packet filter policy based on e.g. port numbers can be used to apply different edge data offloading behavior.

The key issue is solved in this case by intercepting S1-U (in EPS) or N3 (in 5GS) traffic and communicating directly with the MSP Servers from the intercepting entity.

This solution is applicable to both EPS and 5GS.

3.1.2.5 Solution 4 – Data offload with Single PDU Session in 5GS

In 5GS [5], the SMF is in charge of (re-)selecting a UPF for a PDU Session and can consider a number of parameters for the selection process. Among these is the tracking area identifier, which allows for a cell-specific UPF selection. In this approach, the selection process is used to offload all traffic to an edge UPF. Likewise, downlink traffic would always pass through this UPF. Different traffic flows might still be offloaded to different MSP Servers but would use the same breakout/UPF.

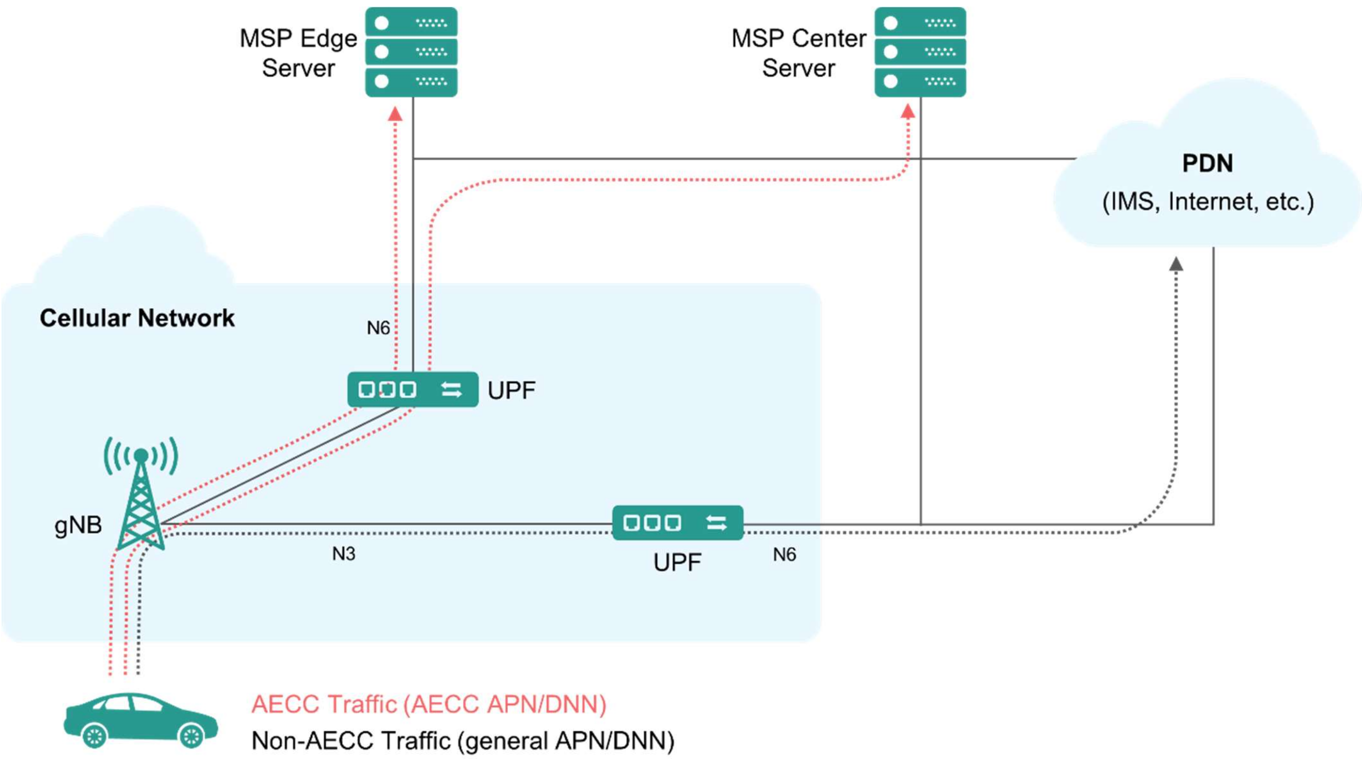

Figure 18. Data offload with Single PDU Session for AECC-related traffic (red) and other traffic (black) in 5GS.

3.1.2.6 Solution 5 – Data offload with Multiple PDU Sessions in 5GS

The UE creates multiple PDU Sessions using the same procedure as for the edge breakout with a Single PDU Session. While one PDU Session offloads traffic to edge UPFs, the other PDU Session uses a central UPF. For downlink traffic, the two external IP addresses of the respective PDU Sessions are used to select the corresponding UPF.

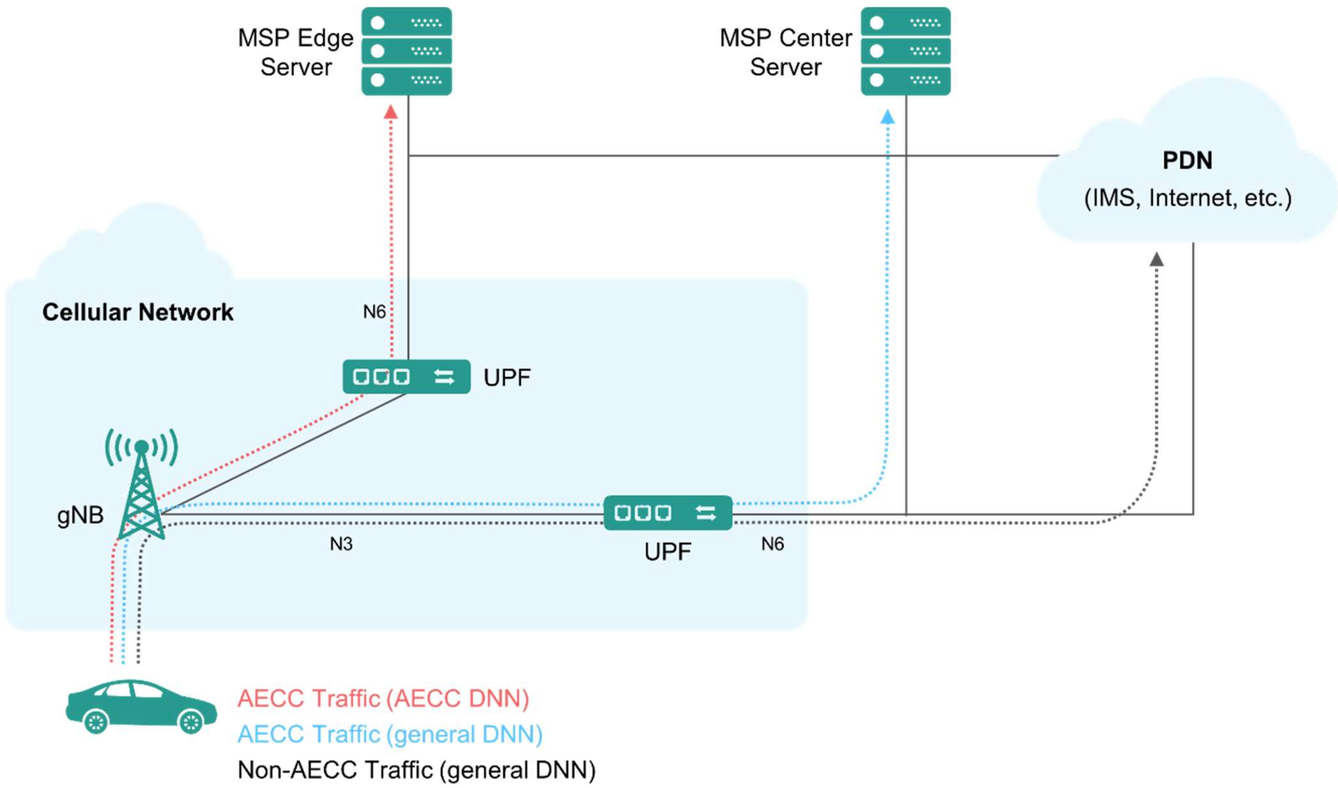

Figure 19. Data offload with Multiple PDU Sessions for AECC-related traffic (red & blue) and other traffic (black) in 5GS.

3.1.2.7 Solution 6 – Uplink Classifier

In 5GS, an uplink classifier policy can be provisioned in UPF to offload the selected traffic to an Edge Server. The insertion and removal of an uplink classifier policy is controlled by the SMF. The SMF may include multiple UPFs with uplink classifier policies in the traffic data path and may modify this UPF chain dynamically. This solution is only supported in 5GS, and IP 5-tuples are used as traffic filters in the UPFs that, when matched, trigger local offload of the respective traffic.

In this approach, while there are multiple PDU Session anchors, there is only one IP anchor; that is, the IP address of the UE is assigned by only one UPF and preserved during the lifetime of the PDU Session. Even during mobility, the IP session is maintained, while traffic to the old uplink classifier UPF is tunneled. For downlink traffic, the Vehicle System is reachable using the same IP via all UPFs, which must be considered in the IP configuration of the MSP Servers and the corresponding IP network(s).

In order to forward data to the appropriate PDU Session anchors, uplink classifiers must be configured accordingly, based on information on IP subnets and location of MSP servers, in order to know which PDU Session anchor is most appropriate for the UE in a given cell, and the IP subnet with which it communicates. This information can be configured and updated manually, or it can be dynamically exposed to an MNO by an MSP. Typically, defining how such information is exchanged is part of an SLA.

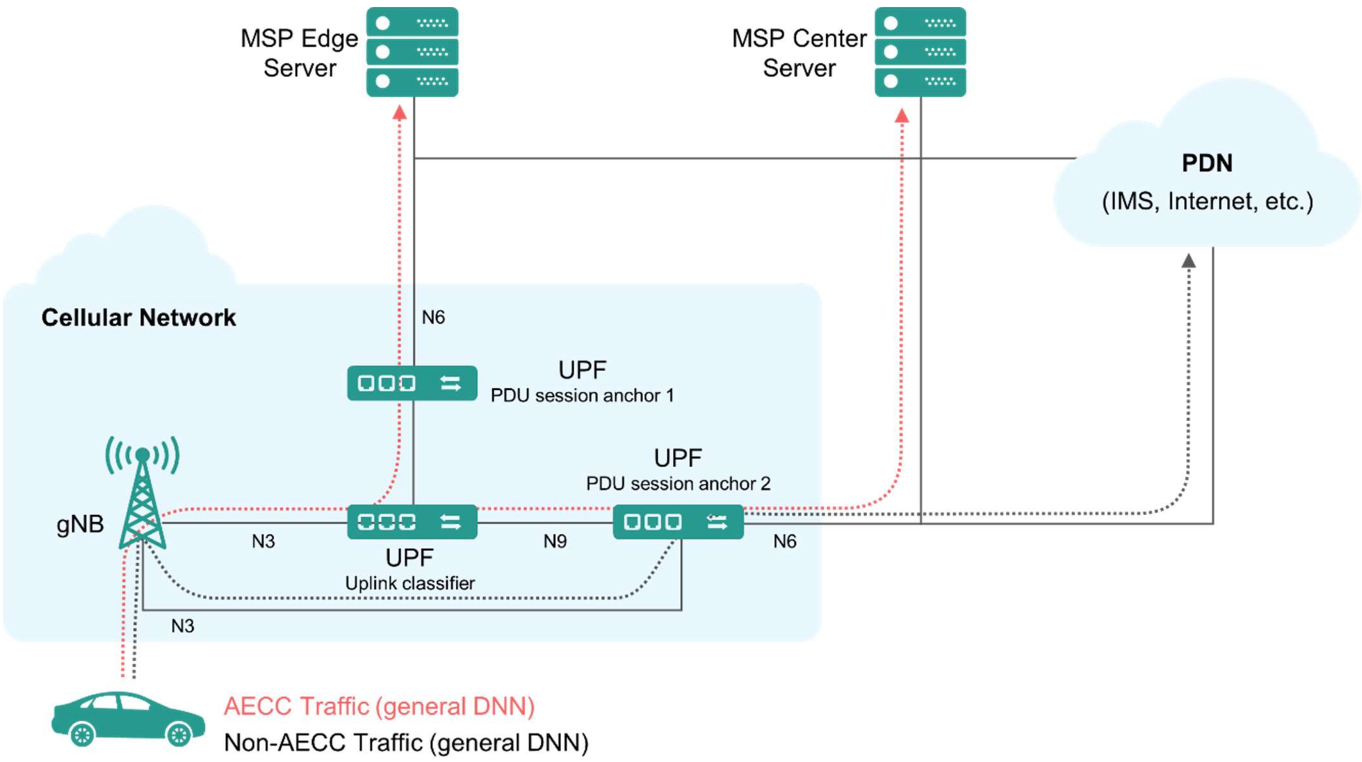

Figure 20. Data offload with Single PDU Session for AECC-related traffic (red) and other traffic (black) in 5GS, using uplink classifiers to selectively offload traffic based on traffic filters (usually IP 5-tuples).

3.1.2.8 Solution 7 – IPv6 Multi-homing

In 5GS, the PDU Session from a Vehicle System may be associated with multiple IPv6 prefixes. Selected traffic can be offloaded to the designated Edge Server as configured by the SMF, using a specific IPv6 prefix. In the traffic data path, the common UPF acts as a branching point, where the uplink traffic is split to different destinations and downlink traffic is merged to the Vehicle System. The UE selects the source IPv6 prefix according to rules pre-configured in the UE or received from the network.

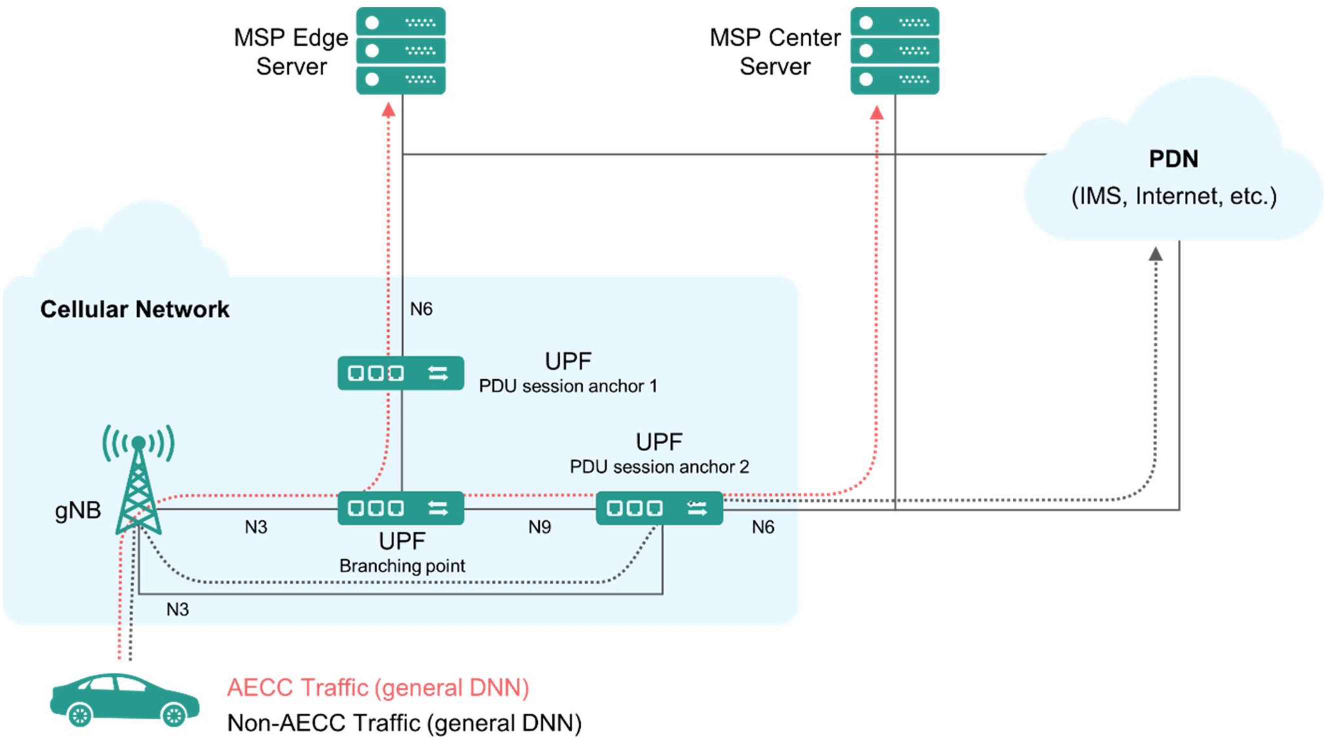

Figure 21. Data offload with Single PDU Session for AECC-related traffic (red) and other traffic (black) in 5GS, using different IPv6 prefixes to selectively offload traffic.

3.1.3 Conclusions

For 5GS, the recommended first choice of AECC is Solution 6 (Uplink Classifier). It leaves IP session termination during GW mobility to the applications, maintains IP connectivity via the central breakout point irrespective of the current edge breakout configuration, avoids complexity in the Vehicle System and allows for slim edge breakout dimensioning. On the other hand, as there is only a single IP anchor on the network side, IP-addressing has increased complexity and needs additional consideration for downlink traffic. This solution involves optional components (specifically Uplink Classifier functionality in UPFs deployed at the edge) of the 5G architecture, so it might not be deployed with global coverage.

As a fallback solution, Solution 4 (Data Offload with Single PDU Session) is recommended. This solution is based on distributed anchors for the AECC PDU session with re-anchoring as needed. Therefore, it consists only of mandatory 5GS features while limiting complexity in the Vehicle System. The feasibility of this solution depends on the mobile network deployment and the degree of cloud distribution. For a low degree of distribution, this solution may in fact be an excellent choice due to its low complexity. However, inefficiency for this solution rises with higher degrees of distribution combined with large data volumes to or from the MSP Center Server.

Solution 6 and Solution 4 require the same functionality in the Vehicle System, which is why no MNO-specific functionality needs to be applied. One difference in behavior is that Solution 4, in the most basic configuration (SSC mode 1), forcefully terminates PDU Sessions during mobility, while Solution 6 keeps PDU Sessions up even during handover.

Finally, as Vehicle System capabilities evolve, Solution 5 (Data Offload with Multiple PDU Sessions) is more feasible and can then be applied as a complement to Solution 4 or Solution 6.

For EPS, the AECC recommendation is Solution 1 (SIPTO with Single PDN Connection) as the first choice for keeping Vehicle System complexity low. Furthermore, SIPTO ensures connectivity to the most appropriate offloading point, even during mobility. However, as the PDN Connection is terminated and re-established during mobility, all IP connectivity (including connectivity to the MSP Center Server) is unavailable for a short time.

Solution 2 (SIPTO with Multiple PDN Connection) is a possible enhancement for reducing the load on the edge breakouts and maintaining connectivity to the MSP Center Server at all times while the Vehicle System is in coverage. However, the Vehicle System needs to manage two separate PDN Connections with different APNs in this case, as opposed to Solution 1.

3.2 MSP Server Selection

3.2.1 Key Issue

The AECC system enables data communication between Vehicle Systems and MSP Servers. In the case where there are multiple concurrent services in use within a Vehicle System, the Vehicle System may connect to multiple MSP Servers as shown in Figure 22. For example, in this figure, Vehicle System A connects with MSP Center Server, MSP Edge Server 1 or MSP Edge Server 2A. Vehicle System B connects with MSP Edge Server 2B in addition to the MSP Servers connecting Vehicle System A.

Each service scenario may require the Vehicle System to connect to a certain MSP Server that is hosting dedicated applications for respective services. The objective of the MSP Server selection will vary, depending on each service scenario. For each objective, information such as vehicle geolocation, access network topology, server load, network performance and policy may be consumed for the selection process. A mechanism to collect, distribute and process the information to enable selection of the appropriate MSP Edge Server needs to be selected.

Furthermore, an AECC System may have a highly dynamic network topology. For this reason, restrictions affect endpoints using IP addressing. An addressing scheme is necessary for the MSP Server selection process and must be established for subsequent use of the system. Part of the selection process is to ensure a dynamic addressing of the MSP Edge Server, the MSP Center Server and the Vehicle Systems.

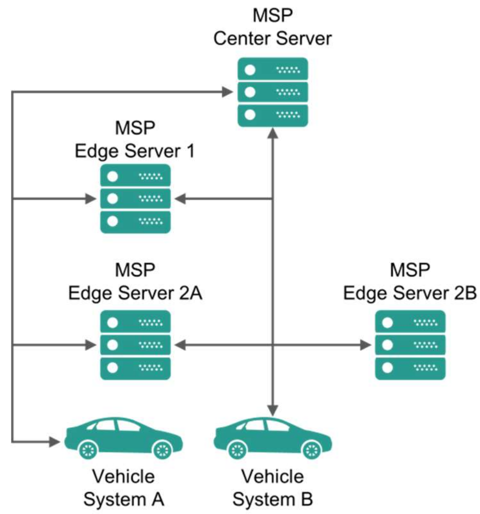

Figure 22. Topology of hierarchical distributed computing, with the lines and arrows showing the message bus and possible data exchange path between all entities.

3.2.2 Potential Solutions

3.2.2.1 Solution 1 – Access Network-based MSP Server Assignment

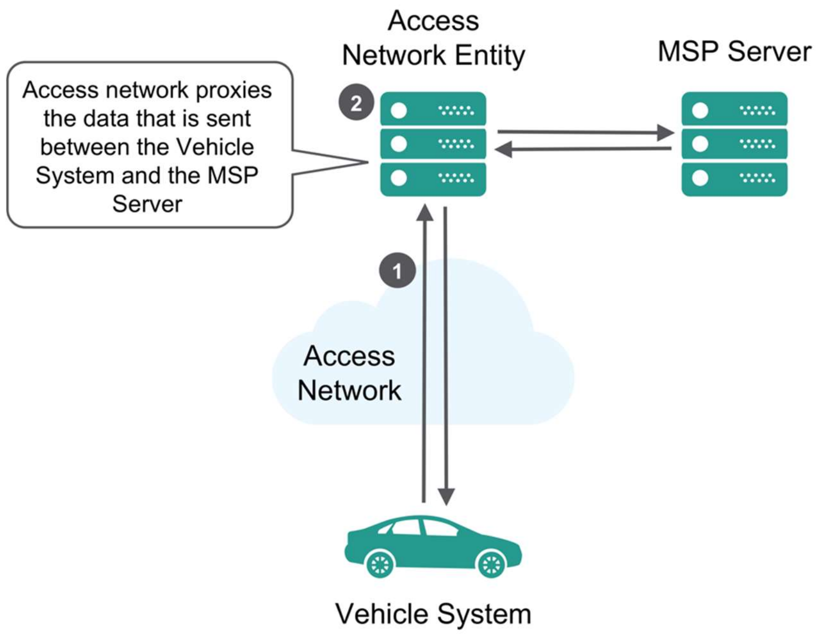

Figure 23. Access Network-based MSP Server Assignment.

In this approach, the Cellular Network entity becomes a proxy and a control agent for communication between the Vehicle System and the MSP Server; this makes the Vehicle System agnostic regarding the MSP Server Assignment procedure. The approach assumes that the Cellular Network operator and the MSP have mutual agreement on how the assignment should occur.

1) The Vehicle System sends data through the access network.
2) The Cellular Network entity chooses the most suitable MSP Server based on the agreement with the MSP Server and other criteria such as current server load.
3) Data is routed toward the target MSP Server.
4) Response from the MSP Server is then routed back to the Vehicle System through the Cellular Network.

3.2.2.2 Solution 2 – IP Network-based MSP Server Assignment

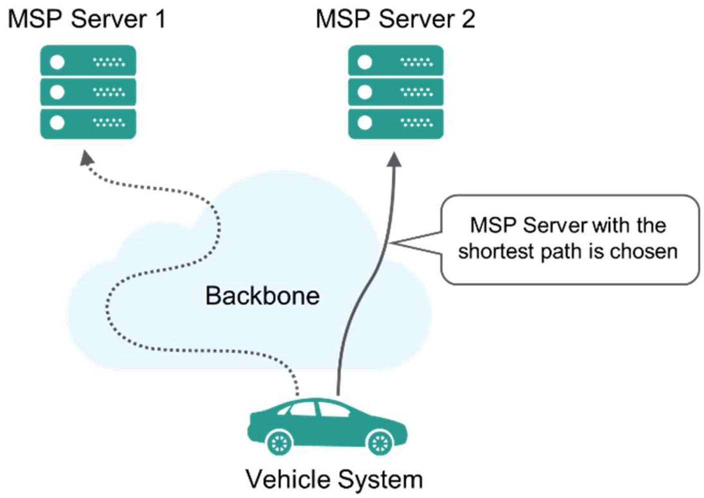

Figure 24. IP Network-based MSP Server Assignment.

In this approach, both the MSP Server and the Vehicle System do not have any logic to decide the appropriate MSP Server. The routing scheme may leverage IP anycast, so that traffic from the Vehicle System will be forwarded by routers within the IP network to the MSP Server with the shortest path. In this approach, all required information is located in the application layer, thus making it agnostic regarding the access network.

3.2.2.3 Solution 3 – MSP Server Assignment by a Selection Function

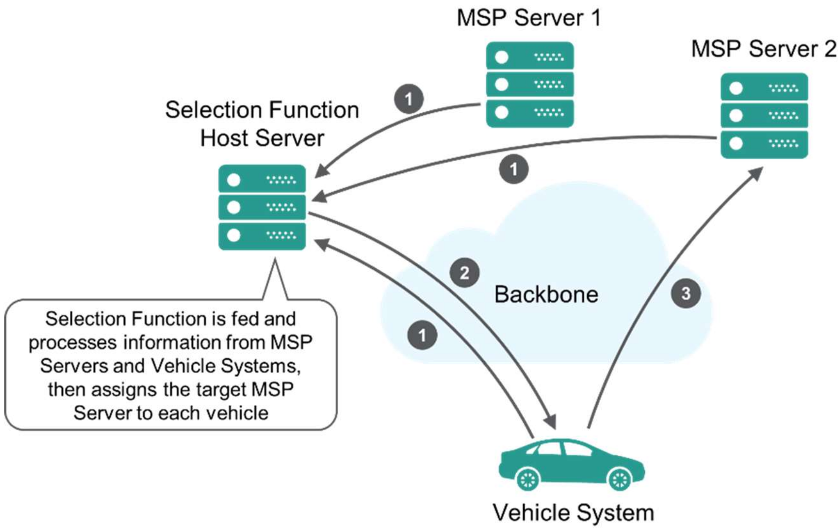

Figure 25. Selection Function-based MSP Server Assignment.

In this approach, a Selection Function receives information from MSP Servers and the Vehicle System. The Selection Function then processes the information and informs the Vehicle System, allowing the Vehicle System to initiate a session with the selected MSP Server. For example, implementation of the Selection Function can be a DNS Server, although implementation is possible independent of the DNS system. Specific configuration of the Selection Function may allow processing of information shared by Vehicle Systems and MSP Servers, including but not limited to geolocation and/or server health check. This approach is agnostic regarding the access network.

1) The Selection Function accepts information from MSP Servers and Vehicle Systems.
2) The Selection Function assigns the target MSP Server.
3) The Vehicle System connects to the target MSP Server assigned to provide it with connectivity.

Figure 26 shows an example of implementing Edge Server Assignment by a Selection Function using DNS:

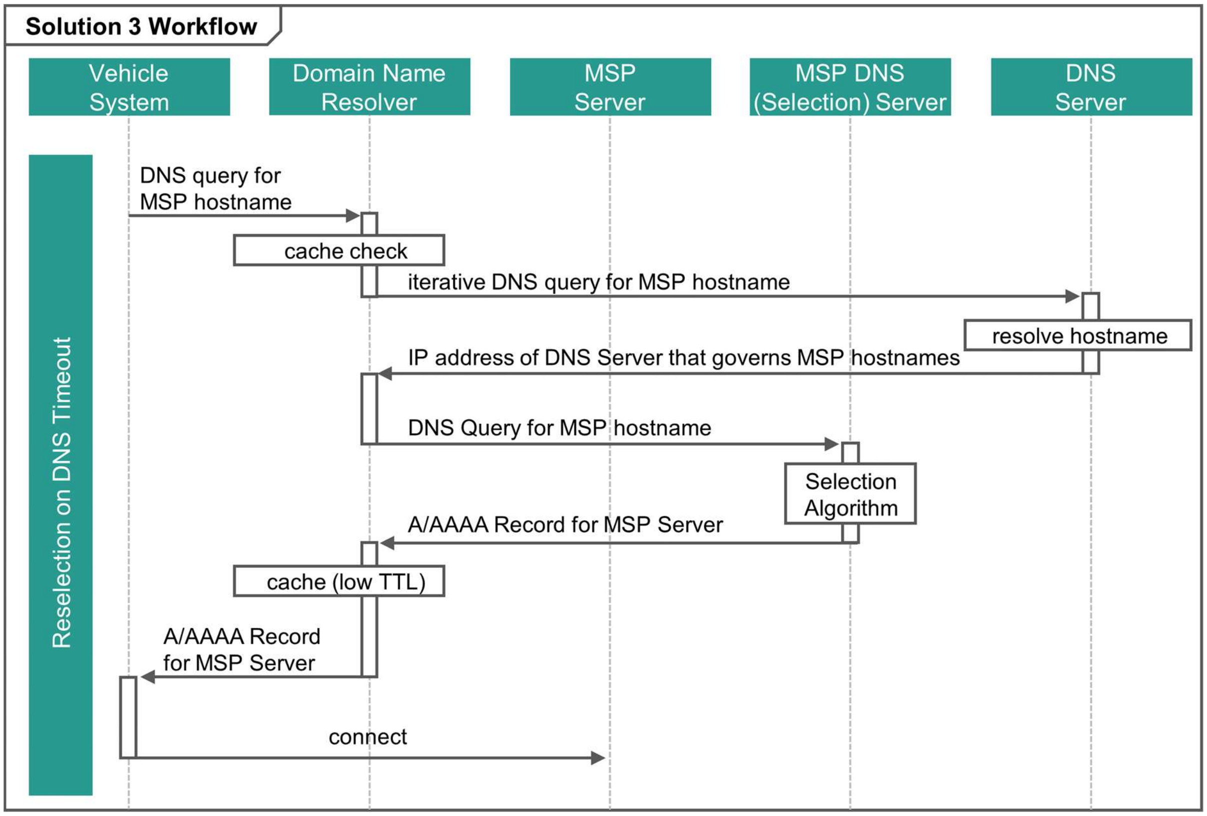

Figure 26. Example implementation of Solution 3.

Notes on the implementation:

- To enable responsive Edge Selection, due to mobility of the Vehicle System, appropriate DNS cache timeouts should be selected.
- To accommodate applications that require server clustering based on geolocation, the Selection Function will need the vehicle's geolocation information, for which granularity may differ between services with the DNS query.
- The selection sequence takes into account that the resolved IP address may be an address of a load-balancer, thus triggering Solution 5. When using 5GS, additional functions may be needed to enable the correct Edge Selection when coupled with the offloading function discussed in the previous key issue, Edge Data Offloading.

3.2.2.4 Solution 4 – Vehicle System-based MSP Server Assignment

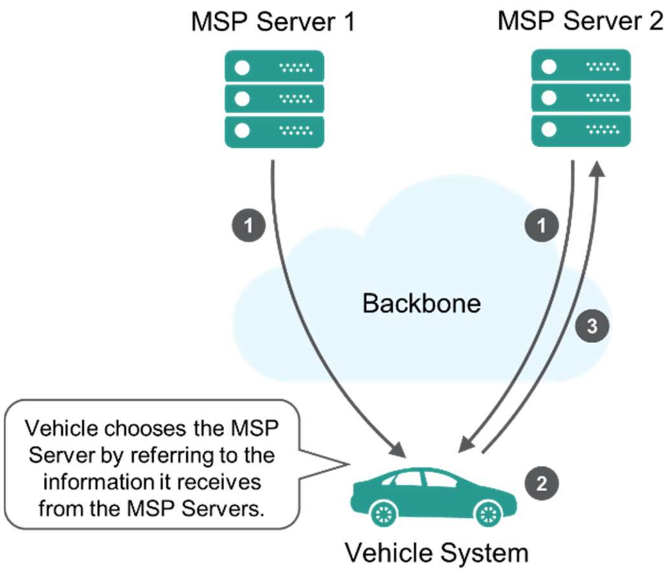

Figure 27. Vehicle System-based MSP Server Selection.

This solution can be combined with the Selection Function solution, allowing MSP Server assignment without the Vehicle System having to share sensitive information. In this approach, the Vehicle System will choose its MSP Server. The Vehicle System may select the appropriate MSP Server based on in-vehicle information such as physical vehicle location, and/or additional information collected from potential MSP Servers. This approach is agnostic regarding the access network.

1) The Vehicle System collects information from MSP Servers.
2) Based on the information received by the Vehicle System, the Vehicle System selects an MSP Server.
3) The Vehicle System connects to the target MSP Server.

Figure 28 shows an example of implementing the combination of a Selection Function and Vehicle-based assignment:

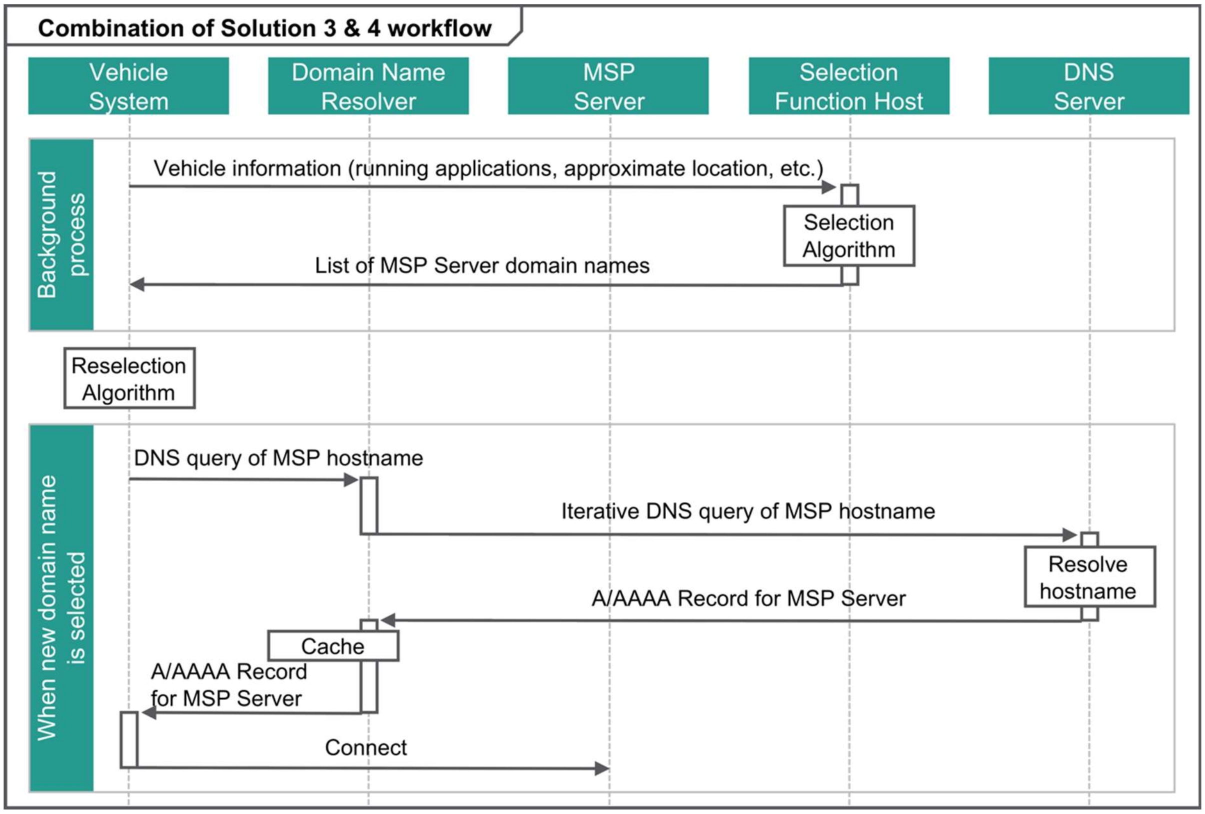

Figure 28. Example implementation of the combination of Solution 3 and Solution 4.

3.2.2.5 Solution 5 – Combination with load-balancer for MSP Server Selection

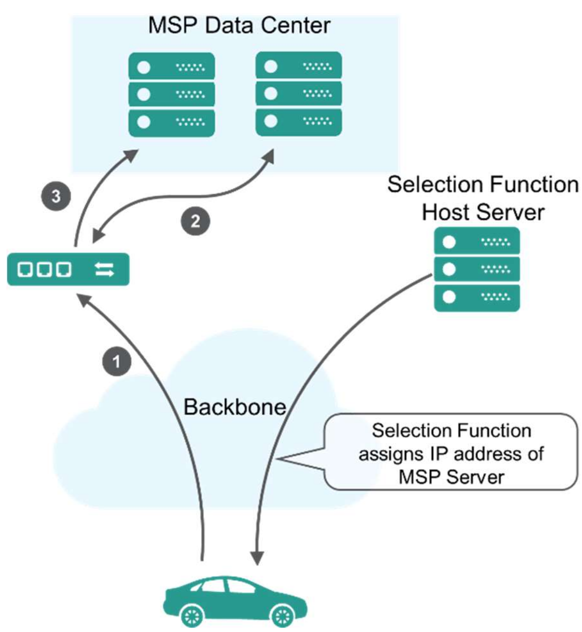

Figure 29. Example illustrating a load-balancer coupled with selection on a server.

This method combines one of the selection methods with an application-aware load balancer in order to determine which application instance should be used by the Vehicle System. One must be aware that the MSP Edge Server is not a single server but rather a set of cloudified servers in one or more data centers composed of the necessary functionality to support the various service scenarios.

1) The Vehicle System initiates a connection toward the load balancer.
2) The load balancer determines which MSP Server to use.
3) The load balancer will manage the session on behalf of the Vehicle System toward the selected application instance within the MSP Data Center.

3.2.3 Parameters for MSP Server Assignment

The following parameters may be used for MSP Server Assignment.

- IP Ping **Round Trip Time (RTT) –** The RTT between the Vehicle System and reachable MSP Servers.
- **Completion Rate –** The quality of this parameter is inversely proportional to the number of packet losses and timeouts between the Vehicle System and the MSP Server.
- **Hops –** Number of hops needed to route the data between the Vehicle System and the MSP Server.
- **Vehicle System Physical Location –** To address localized contents/process, vehicle physical location is needed.
- **Request SLA –** By identifying the dataflow, the system is able to know the SLA of the request, including the required time needed to finish a particular data flow.
- **Server Turnaround Time –** The time needed for an application in the MSP Server to complete a process queried by the Vehicle System.
- **Server Load –** The load of an MSP Server, which might include the CPU and memory usage ratio.
- **Application State**[2] **–** The current application state, which indicates when reselection of MSP Edge Server can be done without interrupting the application.

3.2.4 Considerations Across Key Issues

In current deployments of LTE and WLAN networks, the network typically provisions the IP address of a DNS server to a user located in the user's subnet – thus close to the user's point of presence. It could also be an anycast address, such as "8.8.8.8". In other words, it is a DNS server that is close to the Network Edge. In 5G, an MNO DNS Server may serve clients from multiple anchor points.

Consider now the combination of a DNS-based solution with an uplink classifier-based solution, which is the preferred Edge Data Offloading solution for 5GS. As the user has multiple possible anchor points of presence that can be used based on IP header filtering (typically destination IP address), an extra piece of functionality is needed. In this

[2] Note: The current version of this Technical Report does not consider MSP Server Selection for stateful applications. That part will be further studied in the Key Issue "Service Continuity" as a future work item.

case, the cellular network must ensure that a DNS query is sent to a Domain Name Resolver at a point of presence that is deemed feasible for the corresponding FQDN and UE location in the network.

As a solution, the mobile network operator operating the respective cellular network should provide a central DNS stub resolver that, when receiving a DNS query, forwards this query to an appropriate Domain Name Resolver. This action is based on the tracking area (looked up using standard 5G core functionality) of the UE, and potentially additional knowledge related to the FQDN such as rules about feasibility of different breakouts for specific domain names. Furthermore, the DNS stub resolver may aggregate multiple records in the reply.

3.2.5 Conclusions

Recommendations on the technologies to be used for MSP Server Selection are as follows:

- Solution 3 is preferable for deployments in the near future. This solution is transparent for the Vehicle System. Furthermore, it minimizes the customization effort for the access network. Dedicated DNS Servers (MSP DNS Servers) are recommended to be deployed for MSP Server Selection, which are authoritative for the corresponding DNS zone(s), to enable seamless integration with existing deployed systems, due to their wide adoption rate in the internet, in access networks and on existing clients.
- Solution 4 or the combination of Solution 4 and Solution 3 allows the Vehicle System to select MSP Servers without the Vehicle System having to share sensitive information. This option is also transparent to the access network. A specific selection module must be implemented within each Vehicle System.
- Solution 1 allows a deployment that is transparent to the Vehicle System and MSP Servers when a cellular network is used as the access network. Although this solution will be most advantageous with respect to privacy and security, integration of Wi-Fi to a cellular network is needed to allow heterogeneous access.
- In conclusion, Solution 3 is recommended as a baseline solution, preferably reusing existing DNS functionality and infrastructure, while both Solutions 1 and 4 are feasible to offer enhanced functionality for the MSP Server selection process.

3.3 Vehicle System Reachability

3.3.1 Key Issue

In the AECC distributed computing architecture, MSP Servers – Center or Edge – are required in many use cases to send data to the Vehicle System. However, it is challenging for the MSP Servers to effectively reach the Vehicle System due to mobility of the Vehicle System and network functions such as NAT/NAPT and firewalls. For example, Figure 30 shows several reasons that make Vehicle System reachability a key issue.

1) IP anchor point changes due to a change of MSP Edge Server.
2) Network functions such as NAT/NAPT have timers that can be expired.
3) Service outage occurs when the Vehicle System moves into an area without network coverage.
4) Handover between different access networks.

All these issues can cause a Vehicle System IP address change that results in MSP servers not being able to reach the Vehicle System. Therefore, the AECC System needs to deploy a specific mechanism to ensure the reachability of a Vehicle System according to service requirements.

Note 1: Depending on the service requirements, the Vehicle System reachability issue could be handled differently by the application layer or by both the application and network layer.

Note 2: Both IP and non-IP based solutions shall be considered for this key issue.

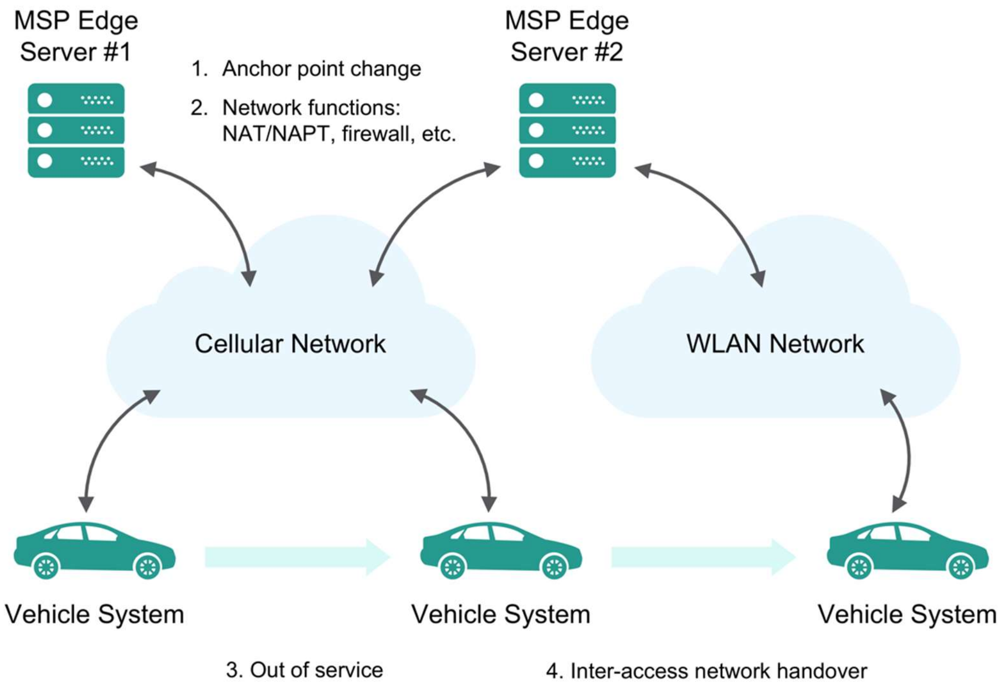

Figure 30. Typical causes of the Vehicle System reachability issue.

3.3.2 Potential Solutions

There are two solutions commonly seen in the mobile industry that enable the MSP server to reach the Vehicle System at any time via a push server and allow the MSP server to receive reachable address updates from the corresponding Vehicle System.

Solution 1 – SMS Push

SMS Push is an SMS “call-in” trigger message in current Over the Air (OTA) software delivery systems. The trigger message is sent to the target Vehicle System by a campaign manager application. The application maintains links to a database operated by the OEM that contains the IMEI number of each Vehicle System within the fleet. Database fields enable the OEM to identify subsections of the vehicle fleet based on parameters such as vehicle type, country and so on. When the SMS trigger message is received, the Vehicle System initiates the appropriate application. The application will then establish a connection to the OTA delivery system and initiate the download. Once a vehicle system connects, it is marked as having received the message and taken the action. This allows the OTA system to identify those vehicles that have not yet connected.

Since the application in the vehicle system initiates the connection into the OTA delivery system, the IPv4/IPv6 address of the Vehicle System is not initially known by the MSP Server, and the MSP Server will discover the address upon connection by the Vehicle System to the MSP Server. It is possible that the vehicle system's unique Vehicle Identity Number (VIN) may be exchanged with the OTA delivery system application to identify the vehicle.

Solution 2 – Push notifications

Push notifications are a common method for maintaining connectivity with highly mobile end-user devices, such as smartphone applications.

A push notification is a message that is "pushed" automatically from a backend server or application to remote clients. These notifications are sent from the application to a remote server, which acts as an intermediary. Each client application needs to be registered with the remote server using a unique key or UUID. The remote server then sends the message against the unique key and delivers the message to the client application via an agreed client/server protocol such as HTTP or XMPP.

The Vehicle System's IPv4/IPv6 address is not required since the backend server or application communicates with the remote server, and the client-side application in the Vehicle System registers with the remote server. It is possible that the Vehicle Identity Number (VIN) of the Vehicle System may be exchanged with the registration of a key or UUID in the remote server to identify the vehicle.

Solution 3 – Vehicle System triggering via Network Exposure Function

Network Exposure Functions, such as SCEF defined in 3GPP TS 23.682 and NEF defined in 3GPP TS 29.522, specify various Network APIs for third parties. The Vehicle System could be triggered via these exposure functions to report its IP address to the MSP servers.

One solution example uses the oneM2M framework [6].

The oneM2M framework defines four types of network nodes -- Infrastructure Node (IN), Middle Node (MN), Application Service Node (ASN), and Application Dedicated Node (ADN) -- and specifies two types of entities -- Application Entity (AE) and Common Services Entity (CSE). AE is an entity that implements an M2M application and CSE is an entity that provides common service functions for AEs. Examples of service functions offered by the CSE include: Application and Service Layer Management, Data Management, Device Management, M2M Service Subscription Management and Location Services. The CSE entity can be deployed at ASN, MN or IN. ADN is a node that contains at least one AE and does not contain a CSE. Thus, each entity is represented as "[Node Type]-[Entity Type]".

The oneM2M framework could potentially be leveraged to solve the vehicle system reachability issue through a network exposure API. As shown in Figure 31, the IN-CSE can dynamically update the current IP address of the ASN-

CSE in a Vehicle System via SCEF/NEF triggering. The MSP application only needs to know the ID of the ASN in the Vehicle System; the IN-CSE in the MSP Server will maintain an ID-IP binding.

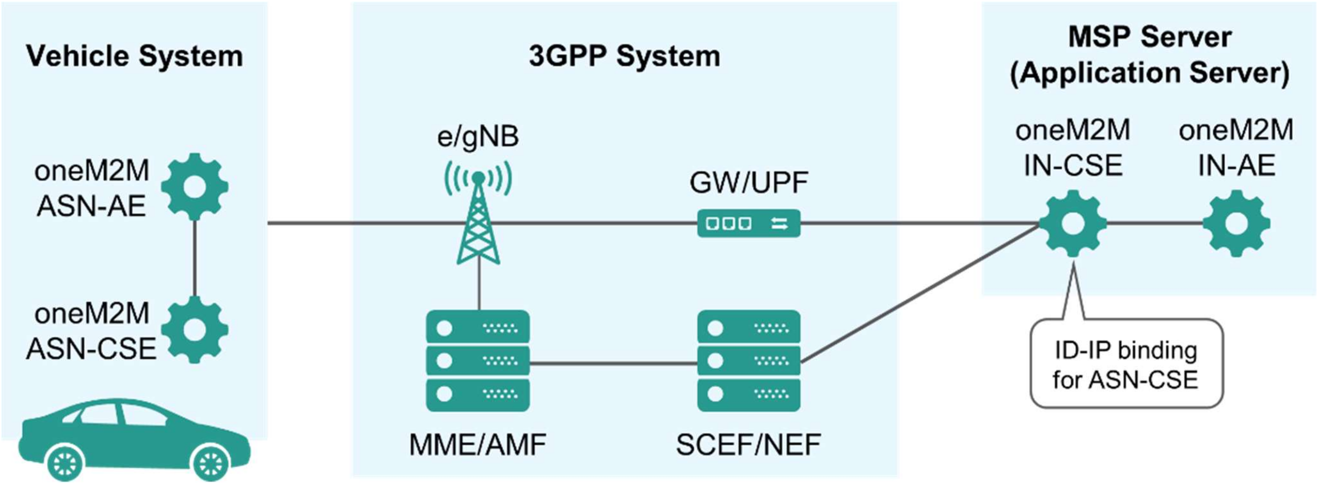

Figure 31. Example of Network Exposure Functions.

3.3.3 Conclusions

Recommendations on the technologies to be used for Vehicle System Reachability are as follows:

- Solution 2 is preferable for supporting both Cellular Network and WLAN access types, which is an architectural requirement in the AECC system.
- Solution 1 could be a fallback solution when the Cellular Network is the only access to be used for push services, since solution 1 already has good adoption in many existing industry sectors, such as automotive and other IoT systems.
- Solution 3 would be promising to replace Solution 1 in Cellular Networks that support SCEF/NEF due to the advantage of less Vehicle System complexity and better extensibility compared to Solution 1.

Further study on the solutions for Vehicle System Reachability will be conducted, your comments and recommendations are welcome.

4 A Path Forward for New Solutions

The three key issues and their solutions presented by the AECC in this paper offer a path detailing how to drive data to the edge from a networking and distributed computing perspective. The AECC believes this proposal should play a significant role in supporting new automotive service scenarios.

In the future, the AECC will consider the distributed computing architecture and connectivity solutions that will be required to meet the growing data volumes of the automotive industry. Five important issues are planned for further study by the AECC in order to develop potential solutions:

4.1 Opportunistic Data Transfer

Network capacity planning has become a major challenge, especially for MNOs, due to soaring costs associated with the exponential increase of mobile data traffic. Meanwhile, new vertical markets such as Connected Vehicles will further drive the mobile traffic growth to a new level that will cause a critical issue for MNOs and MSPs: how to provide sufficient capacity for new and growing services for Connected Vehicles.

In many cases, data traffic such as vehicle telemetry collection from Connected Vehicle services has a relaxed latency requirement. This could be leveraged by MNOs and/or MSPs for more efficient use of existing network resources with minimal cost and interference to existing services. The transfer of such data should be opportunistic, with the potential for such data to be delivered in the background from the point of view of normal data traffic.

4.2 Access Network Selection

The AECC system architecture assumes multiple access networks could be used by the Vehicle System. When multiple access networks are available, it is preferable for the Vehicle System to make full use of all access networks, such as Cellular Networks and WLANs, to meet the AECC service requirements as shown in Figure 32. A mechanism is needed for the AECC system to select and manage one or more access networks according to the MSP policies, service requirements, network connectivity, vehicle mobility and so on.

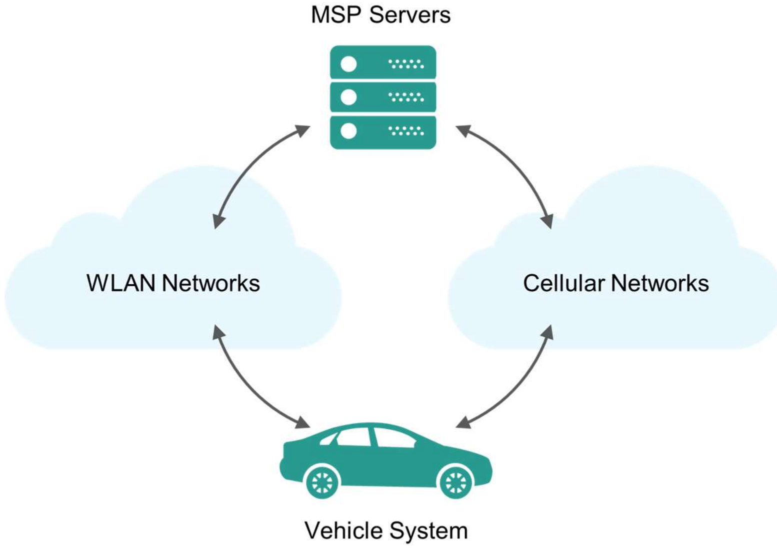

Figure 32. Access Network Selection.

4.3 Distributed Application Layer Architecture

As stated in [3], the AECC system envisions the use of hierarchically distributed computing to reduce the concentration of computation and reduce the processing time needed to conclude a transaction. To describe how the AECC use cases will be realized, parts of the distributed application layer architecture and its interfaces of interest will be defined in more detail.

4.4 Provisioning and Configuration Update

The AECC system embraces high-volume data of different varieties. Also, the AECC system will need to interact with Center/Edge MSP Servers, Cellular/WLAN networks and Vehicle Systems. Configuration provisioning and update must be supported in order to prepare the servers, Cellular/WLAN networks and the Vehicle Systems to meet AECC requirements in a dynamic environment. As the vehicle moves, the location, environment and network availability change dramatically. The AECC system should be aware of these changes based on either access network or Vehicle System reports and adjust policies and configurations accordingly. It is therefore important to consider how configuration provisioning and update can be performed.

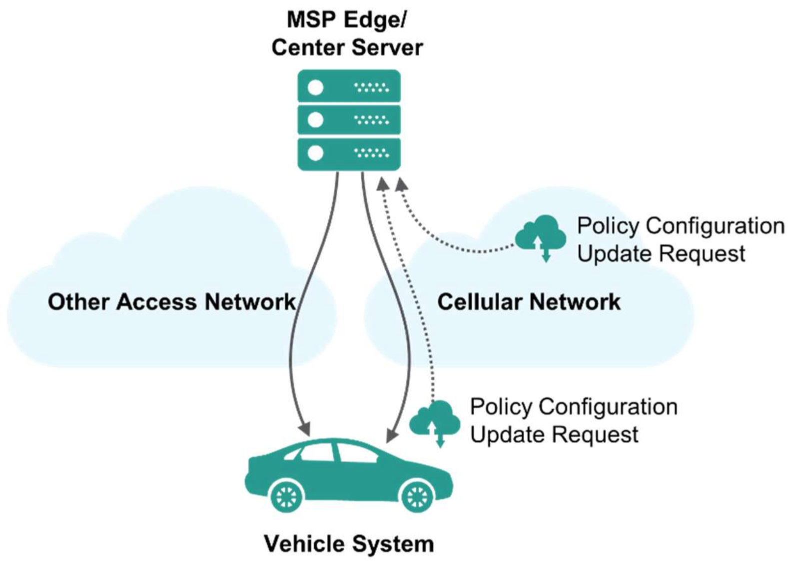

Figure 33. Provisioning for AECC.

4.5 Service Continuity

In the AECC distributed computing architecture, a Vehicle System may be served from different MSP Servers and IP anchor points. Handovers between MSP Servers and/or communication anchor points may be triggered by movement of the Vehicle System.

The AECC system should be defined such that adequate service continuity can be preserved during handovers. Service continuity is affected by different forms of state associated with the communication session or application. To preserve service continuity certain states should either be avoided, migrated or reproduced during handovers between base stations, anchor points and MSP servers.

References

[1] GSMA, Connected Car Forecast: Global Connected Car Market to Grow Threefold Within Five Years. February 2013.

https://www.gsma.com/IoT/wp-content/uploads/2013/06/cl_ma_forecast_06_13.pdf

[2] Cisco, Cisco Visual Networking Index: Forecast and Trends, 2017–2022.

https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[3] Automotive Edge Computing Consortium, White Paper, General Principle and Vision, Version 2.1.0, Dec. 2018.

https://aecc.org/wp-content/uploads/2018/02/AECC_White_Paper.pdf

[4] 3GPP, Technical Specification 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, Version 16.3.0, Jun. 2019.

http://www.3gpp.org/ftp//Specs/archive/23_series/23.401/23401-g30.zip

[5] 3GPP Technical Specification 23.501: System Architecture for the 5G System, Version 16.1.0, Jun. 2019.

http://www.3gpp.org/ftp//Specs/archive/23_series/23.501/23501-g10.zip

[6] oneM2M, Technical Specification 0001: Functional Architecture, Version 4.1.0, Jun. 2019.

http://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30069

[7] Ericsson Mobility Report, June 2019 edition.

https://www.ericsson.com/49d1d9/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf

[8] Ericsson Mobility Visualizer, June 2019.

https://www.ericsson.com/en/mobility-report/mobility-visualizer?f=14&ft=2&r=1&t=21,22,23&s=14&u=1&y=2018,2024&c=1s

Acknowledgements

This document is provided by the Automotive Edge Computing Consortium (AECC) Technical Solution Working Group (WG2). The following people have provided valuable contributions to this document:

ORGANIZERS

Leifeng Ruan (WG Chair)

Mikael Klein (WG Vice-Chair)

Lei Zhong (Chief Editor)

CONTRIBUTORS

Bastian Cellarius, Brian Keller

Clara Li

George Ericson

Hirochika Asai

Joel Obstfeld

Koya Mori

Lidwina Andarini

Ryokichi Onishi, Ryo Tamura

Seiichi Koizui

Takuya Miyasaka, Thorsten Lohmar, Tomoyuki Kurobe, Toru Furusawa

Wenlei Wu

Xiaopeng Tong

Zongrui Ding

Feedback to AECC Technical Report

This version of technical report is the first step in AECC's technical solution progress. AECC looks forward to your feedback and recommendations.

Additionally, we appreciate a few minutes of your time to provide us feedback or ask questions. Please scan the QR code below or directly go to https://aecc.org/technical-report-input-form-questions/ to provide your comments, feedback and recommendations.

SCAN ME

About the Automotive Edge Computing Consortium (AECC)

The AECC is a consortium of leaders across industries focused on driving the evolution of edge network architectures and computing infrastructures to support high volume data services in a smarter, more efficient connected-vehicle future. AECC members are key players in the automotive, high-speed mobile network, edge computing, wireless technology, distributed computing, and artificial intelligence markets.

Our mission is to develop an open, technology agnostic framework to support the transfer of data and communications between the vehicle and local networks near the source of the data, and then to a centralized cloud in a seamless, safe, reliable and optimized manner. Our members collaborate on the development of use cases, technical reports and reference architectures.

- **Use Cases** – Create use cases and requirements in networking and computing for connected services in cars.
- **Technical Reports** – Inform standards and open source communities on best practices for deploying distributed and layered computing architecture for connected cars.
- **Reference Architectures** – Develop for next-generation mobile networks and cloud that are suitable for automotive use cases.

We invite you to join AECC and add your insights and influence. Visit https://aecc.org/ to learn more.