Technology Assessment for Mission-Critical Services on Automotive Virtual Edge Communicator (AVEC)

Rebecca Copeland, Shohreh Ahvar, Noel Crespi
Institut Mines Telecom, France

Romain Durand
Transatel, Paris, France

Michael Copeland
Core Viewpoint Ltd, UK

Jean-Michel Duquerrois
Airbus DS SLC, France

Federica Paganelli, Federica Battisti, Alessandro Neri
National Inter-University Consortium for Telecommunications, Italy

Abstract—Mission critical services are beginning to migrate to broadband from the trusted-but-limited existing systems. They need assured availability and confidentiality for communication in areas affected by a disaster, flash crowding or any catastrophic network failure. This paper describes a vision for an automotive virtual edge Communication scheme that helps healing stricken networks, utilizing any available resources for hosting network functions on vehicles. Emergency and essential service organizations who rush to the area would 'bring their own network', i.e. computing capacity and connectivity tools, aboard their service vehicles. These vehicles form a dynamic community that shares resources, information and services, using the combined processing capacity via virtualized core functions. To realize such a scheme, innovative features are required, such as cooperative hosting, opportunistic vehicular resource virtualization, context-based edge SDN traffic prioritization, and ad-hoc vehicular community management, including multi-entity authentication.

Keywords— *PPDR, MCS, vehicular-MEC, vehicular-NFV, vehicular-SDN, NOS, BYON, PMR*

I. INTRODUCTION

The AVEC idea was conceived to support crisis situation – be it a natural disaster, a terrorist bomb or large public events – is a daunting task which unfortunately is called upon only too often. There can never be enough communication capacity for what is required within the affected area. Even advanced broadband networks are not likely to provide the needed headroom capacity everywhere, to match unpredictable peak congestion, especially when more demanding broadband services are relied upon. The network itself may suffer destruction of its own elements or crippling surges of traffic. Hence, what is needed is short term relief which can be achieved by transporting additional resources to the affected zone. We propose a scheme that supports an AVEC (Automotive Virtual Edge Communicator), which will use cars mounted servers to provide both computing capacity and additional local connectivity resources. The AVEC is more than a portable 'hot spot'. It is also an edge network server, or a MEC (Mobile Edge Computing) device.

Crisis support agencies - PPDRs (Public Protection and Disaster Relief), send relief teams to the location, so groups of emergency service cars reach the 'affected zone'. The PPDRs are highly motivated to enable communication between the team members and with the back office, so it is proposed that such vehicles will be equipped with AVEC units, which will provide not only internal services for the teams, but will also donate spare capacity to host core network functions that extend the network reach and its performance. As these AVECs will have varying capacity and compatibility, a process of resource coordination and allocation to local networks has to take place, using an 'AVEC scheme' on a Cloud-based community server. This scheme enables several AVEC cars from *different* car fleet owners to collaborate in supporting a failing network by letting it 'borrow' capacity temporarily. These AVEC units become an ad-hoc community in the crisis area, who can also share locally some essential services and information. This collaborative hosting facility, where the network customers offer the network providers hosting resources, can be regarded as a 'Bring Your Own Network' (BYON) facility.

The migration from PMR (Private Mobile Radio) to MCS (Mission Critical Services) requires moving from well protected services over traditional technologies (Tetra, Tetrapol), to richer broadband and multimedia services. Pressure to reduce public expenditure is driving PPDRs towards general purpose 5G infrastructure and generic platforms, instead of high-cost special equipment and dedicated network channels. Hence, PPDRs need to implement 3GPP-specified MCS (3GPP TS 23.179), for secure group conferencing (MCPTT), shared videos (MCVideo) and processing sensor input (MCData). The AVEC scheme supports the MCS migration by ensuring better resilience and QoS (Quality of Service) in crisis-affected zones.

The AVEC scheme is intended to support migrating PPDRs. Service vehicles are brought to a crisis zone by first responders primarily to help their own teams, but the AVEC scheme should support any relief team members, regardless of their affiliation. To ensure performance stability and efficient resource

utilization, the resources of AVECs belonging to any car fleet are pooled together, so the facility is shared across all eligible vehicles within the affected zone. In doing so, the AVEC scheme maintains knowledge of participating service vehicles, and can facilitate cross-organization local collaboration, which to-date is still very difficult to achieve. This ability to share relevant information across the ad-hoc vehicular community has a significant potential of enhancing efficiency of relief work.

ESOs (Essential Services Organizations) also bring vehicles to affected areas and will benefit from the AVEC scheme. ESOs are utilities (electricity and gas), road maintenance, automotive roadside support, car rescue, local council street services, or public transport. ESOs run 24/7 services, and often participate in the disaster relief efforts. Their scope is wider, since they get involved not only in disasters, but also as a result of unmanageable peak demand caused by flash crowding, which may be a scheduled event, e.g. Olympic games. ESOs can be both network providers and network consumers. For example, Smart Cities. More often than not, emergencies and flash crowding occur within urban areas, where Smart Cities provide local network (WLAN and other spectrum coverage) and consume resources for city services (e.g. street lighting services or transport systems). **Figure 1** shows the entities that could be involved in AVEC schemes.

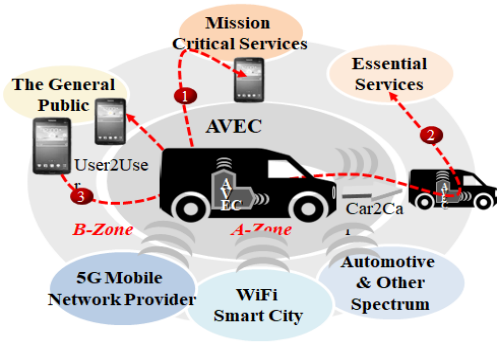

Fig. 1. The AVEC Parties

The general public also benefits from the AVEC scheme. With sufficient numbers of AVECs to enhance capacity, the public in the vicinity could also gain connectivity. Enabling personal communications at a critical moment is particularly appreciated by those who are caught in a disaster. Additionally, citizens' smartphones are a valuable source of information from stricken zones, as they can be used to send relevant images and videos to the relief teams, to the media and even to the PPDR/ESO call centers, to illustrate what is happening at ground zero. Hence, citizens communication in the affected zone should also be supported.

The business motivation for PPDRs and ESOs to adopt the AVEC scheme is to enhance their teams' efficiency while saving costs of dedicated equipment. They will demand resilience and high quality, which the AVEC shared resources will provide through reduced service degradation. Furthermore, cross entity communications will be much easier via the AVEC community services. These agencies will be empowered by the 'BYON' facility because they can ensure adequate connectivity for their teams exactly where and when they need it. Since they rely on connectivity, they are highly motivated to maintain the facility and remain compatible. AVEC resource donors gain the initiative for solving their own communication problems, and this increases their satisfaction and sense of control.

Mobile network providers are obliged by the AVEC scheme to support temporary changes to their resource map and topology, and allow for 'cooperative hosting' to take place, accepting third parties' devices as edge servers. However, this effort will pay dividends because they will increase their good reputation many fold - with better resilience and QoS for car fleets, allowing subscribers to connect when it really matters. In supporting AVEC, network operators are deemed responsive to the increasing pressure to share resources in a reciprocal manner. Network capacity will not only become 'elastic', but will be able to stretch to extreme conditions of unprecedented, unpredictable demand. Moreover, deploying AVECs provides coverage on lower budgets, since costs of configuring unnecessarily high network capacity for rare occasions are avoided.

Network infrastructure Developers will enrich their NFV/SDN portfolio that is now considered as strategic. The AVEC services help the migration to MCS services and provide a base for richer applications. The AVEC full functionality makes use of several emerging technologies that are used elsewhere, thus increasing the features portfolio and encouraging network softwarization. Creating AVEC communities provides opportunities for further collaborative services and enhances location-based mobile services, while delivering them under greater security policies.

II. Survey of Existing Literature

This paper provides a broad brush assessment of the emerging technologies that make the AVEC scheme possible. The solution presents particular challenges for network resource management, including Network Function Virtualization (NFV) [3], Software Defined Networking (SDN) [6,7], and Mobile Edge Computing (MEC) [10, 18]. The AVEC technical requirements will advance standardization in several fields: vehicular MEC binding, vehicular SDN, vehicular NFV, secure car verification, and more. AVEC requirements should be reflected in NOS (Network Operation System) standards, to support dynamicity and transience of resources.

Mission-Critical Communication Services are currently based on traditional 2G technologies (Tetra, Tetrapol), which are limited to low data rates, even for wideband TEDS. National PPDR networks are in most cases incompatible with each other, even if they are based on the same technologies, so migration to 3GPP 4G/5G and MCS, as developed by 3GPP SA6, would provide badly needed convergence [1]. 3GPP Rel. 14 (end of 2017) has implementable Technical Specifications (TS level) of MCS (MCPTT, MCData, MCVideo). It is planned to add more features in Rel. 15 by the end of 2018. Although MCS has been primarily designed for 4G LTE, it will accommodate 5G and beyond. FP7 HELP project proposed LTE based PPDR with network sharing and spectrum sharing [2]. The FP7 ISITEP project designed a framework for PPDR interoperability and international forces cooperation. Other projects proposed interoperability via Software Defined Radio (SDR) (ETSI TR 102 745). FP7 DITSEF proposed self-organizing ad-hoc networks with nodes located in critical infrastructures.

At present, separate reference architectures are proposed for MEC platforms and NFV-based systems, but a design of a common MEC and NFV management architecture [19, 20] is emerging, which will improve the relationship between the applications and the underlying network functions. The ETSI MEC Initiative is planning to release a specification of the MEC in an NFV-enabled environment. The 5G-MiEdge H2020 project is pursuing fusion of MEC with mmWave access to support applications requiring extreme high data rates, low latency end-to-end service provisioning, and full mobility support [29]. Edge computing challenges are also addressed by the OpenFog Consortium, in defining an open computation, control and data storage platform on top of distributed clouds. AVEC is a good example of the demand for such cross-layer resource orchestration architecture.

Optimization of virtualized resources and their orchestration is a popular topic [3], with many proposed methods for optimizing the locations of chained Virtualized Functions (VFs) [4, 5] according to resource characteristics. Some studies consider placement and routing optimization as a joint problem. The main aim is to minimize link utilization, or minimize E2E delay and bandwidth consumption by deploying chained VFs. Orchestration, cost evaluation and horizontal scaling are also often addressed. NFV energy efficiency models are particularly germane to AVEC that may operate where power supply is scarce. Schemes of distributing instances of the same VFs to micro-data centers at the network edge are essential to collaborative hosting. In [21], collaborative usage of resources in opportunistic networks formed by mobile users' devices is discussed, considering the service composition while taking into account users' mobility.

SDN literature addresses flow scheduling and rerouting technique to manage the 'elephant' flows by rerouting over less utilized links [6]. SDN at the edge is proposed for improving efficiency and reliability in home networks, by making use of redundant links. SDN is also considered to enhance mobile LTE performance [7]. The use of the SDN paradigm in the vehicular framework is attracting more research, as evident in recent works [22,23,24]. Traffic prioritization by vehicular context-based policy is discussed in [8]. Dynamically configurable SDN for emergency traffic is proposed in [25], based on specific frequencies, but also on current traffic conditions and application requirements. In [26], the SDN concept is applied to mobile wireless and demonstrated by a Software-Defined VANET (Vehicular Applications and Inter-Networking Technologies), for ad-hoc grouping of vehicles in car-to-car communication. More vehicular MEC studies are now appearing, e.g. MEC for local micro cloud (cloudlet) on base stations to compute resources for offloading and Device-to-Device [9], or to leverage under-utilized resources from nearby mobile devices [10]. In [11], multiple network operators share a base station while adopting different management policies.

Power Management and Spectrum Optimization is required to conserve car battery when operating virtualized functions on AVECs and selecting the best access network where the infrastructure is damaged. Vehicular energy management has been investigated for electric cars, but not for optimizing VFs and spectrum selection. A study of task allocation on mobile ad-hoc grids [12] has utilized user mobility pattern and distance from the node, to reduce communication costs. Energy efficient resource allocation is sought in several studies of battery-operated sensors and CPU-intensive processing on mobile devices. AVEC solutions extend these methods to spectrum selection and virtualization decisions at a vehicular edge.

Authentication of external servers that are adopted by the network as transportable access points require particularly strong verification process, while still allowing for fast binding of servers. Identification of vehicles by their SIM cards is now routine. In [15], embedded SIM is compared with exchangeable SIM, which is flexible but more vulnerable. In [27], firmware and secure connectivity are combined to support vehicular virtualization. H2020 project reTHINK yielded an IETF draft [28] that investigates identity privacy issues in peer-to-peer communications.

III. THE AVEC REQUIREMENTS AND DESIGN

A. *The AVEC Scheme Requirements*

The AVEC idea places a MEC, which has been conceived as a wired stationary edge server, on board of vehicles, so that they can be driven to affected areas, in order to provide transient densification, when and where needed. The AVEC scheme enhances network elasticity and resilience by allowing dynamic augmentation of network capacity to be made to the network topology. This is achieved by virtualizing functionality of the core (VoLTE elements and EPC) on car-mounted edge server, and by providing additional access points that are used by local devices and sensors. Hence, AVEC increases connectivity as well as computing capacity and recovers network operations at various failure points, as shown in **Figure 2**, where network functions can be virtualized.

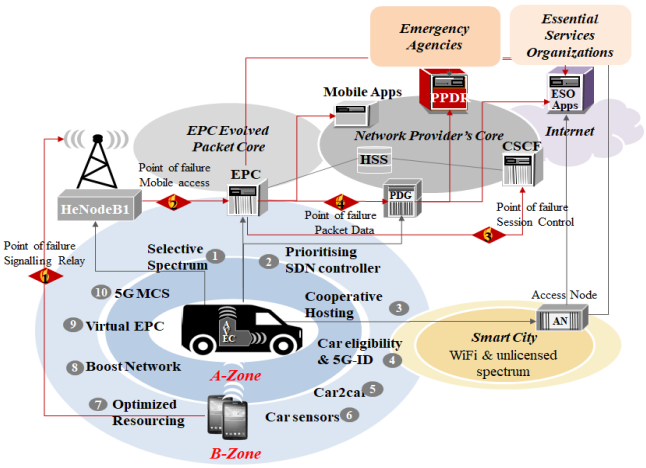

Fig. 2. Network Failure points and AVEC zones

The solution requires setting up defined Affected Zone (A-Zone) that has poor connectivity, and the surrounding Base Zone (B-Zone), which is the proximity area. A-Zones must be defined for the AVEC scheme from various reports from the field. The B-Zone should be determined by a given, updatable coefficient, to allow for preemptive AVEC preparation before entering the stricken area. Cloud downloads of necessary procedures may rely on local WiFi, such as Smart City connections, and other

spectrum made available for vehicular communication. Community base services include car eligibility and authentication, MEC compatibility, and downloading the necessary clients. Hence the process of vehicle registration into the AVEC 'community' takes place in the B-Zone and the coordination of AVECs contributions begins there. Further cross-entity effort coordination within each disaster zone can be supported by more community services, perhaps monitored by nominated zone coordinators in each case.

The AVEC car unit should firstly support the owning agency's internal services that the PPDR/ESOs run routinely, such as activity reporting and location-based services. However, as a pre-requisite, the car unit should have spare capacity to host virtualized network functions. The AVEC server requires additional intelligence to link to more networks in its role as a universal MEC server. The AVEC should be equipped with multi-spectrum converged access point. It should also be possible, though not essential, to support a team of associated devices and provide device-to-device local communications. The allocation and release of resources will be orchestrated by a central module of the scheme in the Cloud, that will optimize the assignment of AVECs to particular networks and particular VFs. The orchestration uses information from the vehicles' internal resourcing function, which notifies the scheme of vehicle's capabilities, and matches that with network's self-healing information, to identify requirements for boosting resources. The orchestrator monitors vehicles' status until they leave the zone and their resources are no longer available.

The requirements for Mission Critical Services, as specified by 3GPP (MCPTT, MCData, MCVideo), are mainly to achieve compatibility with the underlying network, since MCSs are network agnostic, but they require adequate bandwidth to run without service degradation. An AVEC may be required to play a role of a device that MCS will address directly, or as an edge server that connects several MCS handsets. Mission Critical services necessitate requirements for high communication security and QoS and confidentiality, to replace the safety of the previous isolated secure channels of traditional emergency communications. The ESOs also require a certain level of security and reliability, but perhaps not as high and not as costly as critical emergencies. ESOs could use not only mobile networks for MCS, but also take advantage of unlicensed wireless spectrum and new spectrum ranges.

There is also a requirement to support members of the public that happened to be in the zone. Such services can be accessed via mobile networks or WLAN (e.g. Smart City), and provide access to the Internet. These services require only normal level of security, and would be provided at lower priority. As shown in **Figure 3**, multiple levels of security are required:

Security Level 1 is for PPDRs who need the highest security and priority for critical communication. They may rely on mobile network 'slicing' to create secure virtual channels. *Security Level 2* is for Essential Services who require protection, but not as time-critical. While essential communications could also be channeled in the same way as PPDRs, they may also run services that will be transported over less well equipped networks, and possibly route web services via '*fortified*' Internet servers and special security filtering gateways (TURN servers), as described in [16]. *Security Level 3* is normal service level for the general public, with 'best-effort' quality of service. Establishing these communication levels entails prioritizing connection sessions per user as well as per application.

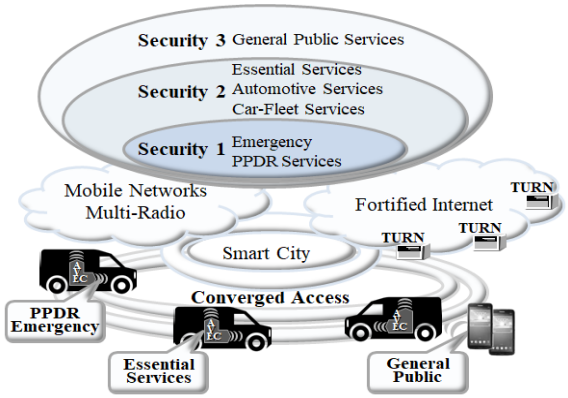

Fig. 3. Service Security Levels

The AVEC scheme must include a system for managing the community of vehicles, which is dynamically created within each crisis zone. AVECs must be securely identified by the scheme, to avoid abuse and intrusion, so incorruptible, with tamper-proof identification and eligibility per disaster zone. The scheme must detect vehicles entering the affected zone, identify their owning agency and verify their hosting capability. Eligibility may involve checking on online rosters of service vehicles in the area and association of drivers and vehicles.

B. AVEC Components Design

The AVEC architecture follows the ETSI MEC reference architecture [18], but requires the standard network interfaces (Mm2, Mm3, Mm4) to be open. As shown in **Figure 4**, the AVEC system comprises of three main components**:** The Vehicular Resource Manager, the Network Integration Module and the AVEC Community Centre.

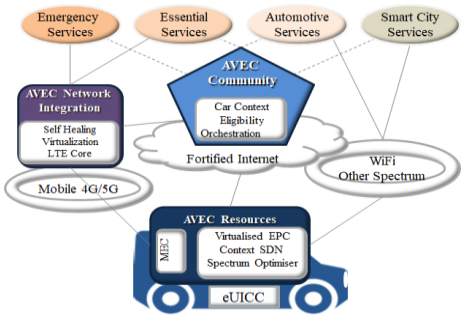

Fig. 4. Service Delivery Architecture

1) Vehicular Resource Manager

The AVEC car-mounted unit serves several purposes: it is an in-car endpoint device and is used for drivers' communications, but it is also a local access point for several more nearby devices and handsets. It is used as a powerful server for locally run applications for the organization internal use. Now it is proposed that it will also provide virtualization capacity for hosting core network functions. As an edge device, it must be modelled on

the evolving standards for MEC. As shown in **Figure 5**, the MEC server interfaces to the car internal intelligence, which provides car authentication and car sensor data collection. Due to the AVEC mobility, it has to refresh its position within the network topology via the network-side integration module. This mobility defines the car context (movement, speed and direction) and ascertains the expectations from the AVEC when it is approaching or leaving the affected zone. The AVEC context is monitored via the interface to the central AVEC Community facility, which assigns NFV tasks. Optionally, AVEC features are deeply integrated within the car intelligence, or remain car agnostic, depending on the application. Similarly, AVEC connectivity may utilize the car internal communication stack, an on-board microcell/base-station to enhance local connectivity, or operate as a client of the mobile network.

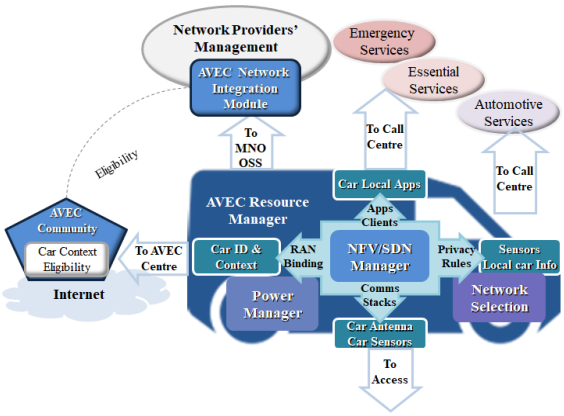

Fig. 5. The AVEC Resource Manager

As a smart vehicular resource manager, the on-board AVEC configures the vehicular resources for both local functionality and for hosting virtualized core functions (such as P-CSCF or EPC). It may restrict non-critical applications when more processing power is required for network functions. It collaborates with the Network Integration Module to establish the hosting relationship, but needs the AVEC Community Center to coordinate the virtualization across the whole group of AVECs. The resource manager assesses the on-board capability and informs the coordination function at the center of any changes. Optimal network selection by endpoints is traditionally dependent on signal strength, but the AVEC optimizer will also consider the state of the car battery and the impact of the predicted energy consumption of different spectrum frequencies and virtualized functions.

The AVEC car unit performs a number of other tasks: It initiates and supports the preemptive downloading of procedures and clients, when needed. It must comply with strict hosting rules that ensure secure multi-tenanting processing and secure data storage that will guarantee full confidentiality. It must also protect the vehicle native intelligence from network based tampering, and facilitate authentication that involves firmware embedded data. To support varying requirements and priorities, the AVEC car unit also acts as an edge SDN controller that priorities critical, essential and ordinary network traffic in separate streams, with different levels of security and QoS. Once established as an SDN controller via the Network Integration Module, it interfaces to the network directly, managing traffic to and from the AVEC endpoints.

2) AVEC Community Center

The Community Center provides common services to the transient population of service vehicles in the zone. It determines the coordinates of the affected zone from reports received by the relevant agencies. It detects and identifies AVEC cars to be considered for virtualization, and initiates eligibility verification processes, considering the current car context. Eligible AVECs will be able to communicate between them, thus it provides the all-important cross-entity communication, since it will have verified identities of all AVECs within the zone. In addition, a common service can collect and aggregate relevant sensor data to help all the first-responders who require real-time processing of wearable sensors, car environmental sensors and the installed base of sensors in the vicinity.

The AVEC community function ascertains a profile for each AVEC for vehicle/driver verification, vehicle location (within the zone, approaching or leaving), and available capacity and connectivity, to optimize distribution across the vehicular community. The organizations' priority and security requirements are also taken into account. It coordinates the dynamically formed and constantly changing population of vehicles and their contributions. It matches capabilities and compatibilities and allocates AVECs to participating networks. This process involves monitoring car location and persistence in the zone, gauging AVEC capacity changes, and assigning AVECs according to information supplied by the AVEC unit. The NFV assignments are constantly monitored, to respond to the overall group make-up, changes in AVECs locations and the depletion of resources, including power and storage. Where possible, more than one network can be assisted at the same time, given appropriate population of AVECs.

3) The Network Integration Module

The Network Integration Module is network-side component that is responsible for the AVEC integration as NFV resource, edge SDN controller, and a MEC with end clients. It will be activated in a predictive mode in the B-Zone, before reaching the A-Zone, to allow for assessment of candidates for AVEC operations before the network connectivity deteriorates. It links to the network's management system and allows customization to achieve compatibility. It should support the emerging Network Operating System standards to interface with actual and virtual resource management. This Module obtains information about each network's virtualization requirement, to pinpoint network failures that need recovery assistance. The final decision to deploy AVEC virtualization is based on the whole group of AVECs acting as a collaborative platform, as viewed by the AVEC Community Center.

IV. THE AVEC MAIN FEATURES

A. Portable Converged Mobile Access Node

The remarkable advantage of vehicular MECs is their timely physical portability, bringing needed resources to exactly where they are needed. The difficulty for the AVEC as a MEC access node is that its movements are governed by the priorities of the

relief teams, therefore sustainability and stability of the MEC service can become an issue when sharing with other teams.

The AVEC MEC will be a converged access node, which could utilize several frequencies that are available on board. It could optimize the choice of network to attach to according to the type of signaling, not only the strength. Additionally, the groups of MECs in the zone can be used to implement alternative connectivity. For example, they may be used as a network of TURN servers in the vicinity that transports traffic only on these secure servers, until it reaches the safety of a wired network.

B. Cooperative Hosting

Today's XaaS services are competent in multi-tenanting, but mobile networks are not used to hosting their own functions on their customers' computing platforms. This cooperative but temporary hosting requires some changes in OSS. To achieve multi-AVEC cooperative hosting requires on-the-fly binding of discovered resources, hence the recipient networks must have a compatible module and standard interfaces to their NFV management and resource orchestration functions. The AVEC would make dynamic changes to network topology which are transient and reversible, requiring considerable OSS agility. The emerging NOS standards will simplify this requirement greatly by facilitating plug-n-play. However, to integrate external servers on-the-fly business and administrative issues must be settled between the participating parties, so cooperative hosting needs an agreed framework that sets up the relationships.

C. Optimising Group Resourcing

While self-healing networks and virtualization are well researched, the optimization of the sources that provide resources gets less attention. In particular, it is challenging when the group of sources is dynamically changing. Using vehicles as transient network nodes requires NFV optimization that copes with the dynamicity and mobility and is fast to implement. In addition, the optimization needs to consider each source of resources, i.e. each AVEC, so the dynamic mapping of resources is performed continuously, considering vehicles capability (processing power, memory, CPU, connectivity spectrum) and availability (movement/speed, predictive duration).

D. Edge-Based Traffic Streaming By Service Requests

The advantages of vehicular SDN are evident: it is able to effectively support the required dynamicity of the vehicular environment and the varying demands for resource-hungry applications, while reducing the computational complexity. SDN brings low delays and can support frequent handovers, thus it is highly suitable for AVEC services. However, there are still many implementation challenges, e.g. in concentration and automation of complex network functions and distinguishing traffic requirements. It is paramount for the AVEC scheme to reserve connectivity resources for emergency, but let the general public connect when there is enough capacity, so the streaming of traffic by level of service is granted by the type of service request, under application control. The AVEC SDN controller should determine its own rules for its 'sector', rather than receive instructions from the network. The AVEC 'sector' is the group of devices hanging off the temporary circles of communal AVECs access nodes. The Edge SDN should be able to segregate traffic to streams of varying QoS and security levels, and enforce the rules upstream, through the connecting networks. This will enable intelligence from local applications that are external to the network to define SDN rule for critical/ essential /normal traffic slicing. Such applications could be at the layer of MCS services or the AVEC community Center.

E. Vehicular Composite Identity Management

There are many schemes of identity authentication, but more rigorous verification of eligibility is required for AVECs. Beyond multi-factor authentication of associated car SIM and driver's phone, it should be possible to include other attributes that are verified by the car fleet owners via linked web services. The procedure shown in **Figure 6** considers dynamic association of verifying 'attributes', including driver ID, vehicle car fleet ID by the owner, car SIM, and Community eligibility. Light-touch processes of the driver's self-provisioning and the organizational ratification are both required. Network providers will be able to obtain direct verifications from the sources through their membership in the AVEC community.

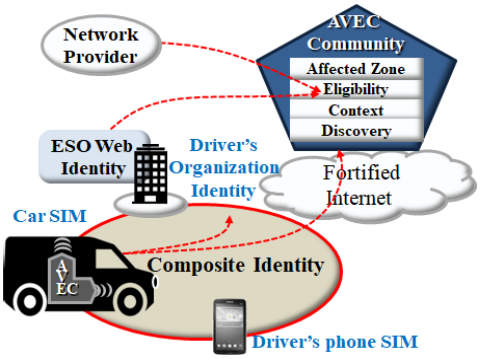

Fig. 6. AVEC Composite Identity

F. Vehicular Mobility Context

The dynamic nature of AVECs positioning is a particular challenge. Since the AVECs deliver scarce computing power and connectivity exactly where it is needed, matching supply and demand of resources is a continuous process. Both supply and demand are determined by the participation of network providers and PPDR/ESO agencies. Network providers join the community when their network is within the A-Zone, and they require assistance. PPDRs and ESOs join each community only when their vehicles are present in the A-Zone (Affected) or B-Zone (Base service area). AVECs need to be recognized (affiliated to a relevant agency/authority), registered (logged on to a dynamically formulated AVEC Community) and assessed (measured for capacity, compatibility and capability).

The assignments of AVECs to network functions must consider vehicular current position, speed and direction of movement, as well as predicted 'persistence' in the zone. As AVECs vehicles have variable in-zone stay periods, it is necessary to ascertain when and for how long AVECs can be used for NFV to provide operational stability and consistence. The AVEC status as the vehicle arrives at the scene, leaves it, or is stationary must be considered as indicators of 'persistence'. Additionally, potential persistence within the zone may be

predicted according to historical average stay duration, modelled for each type of first responders (e.g. fire, police, road maintenance) by previous patterns of presence.

G. Proximity Based Ad-Hoc Community

There must be trust relationship between the various organizations and the network providers to support cooperative hosting. These ad-hoc communities are regional and local, and by the nature of the task, have common interests and a strong need to share information. Specific small circles of relief workers will be defined by the proximity of the AVEC vehicles. The AVEC Community Center will foster community shared services by identifying and verifying the members. This can facilitate inter-communication across agency, as well as connectivity back to base. They could also make use of common services, such as cross-agency situation reports, coordination of traffic and parking, and providing important local information (e.g. detailed local maps and building plans, location of water hydrants and power supply etc.). Community calling between vehicles could use VANET techniques with the help of the common AVEC center, or support of MCS based applications.

V. EVALUATION

A. Feasibility and Adoption Challenges

This AVEC scheme is unquestionably challenging, but the rewards to society and stakeholders are immense. The compatibility of AVECs with network providers' systems needs to be confirmed, perhaps by certifying MEC platforms, to ensure that they cannot disrupt normal network operations. The cooperative hosting business relationships between network providers and their customers need to be resolved for on-the-fly integration of AVECs. Pipe-line technologies and upcoming standards will make AVEC schemes feasible, but several features are still missing and the technologies need extending.

Early implementations with specific network compatibility will be the first step. Adoption by PPDR and ESO depends on achieving simplicity and low cost, and the timing is linked to their migration to Broadband MCS. Their security concerns should be alleviated by implementing the proposed vehicles verification that empowers car fleet managers to control the dynamic community. Smart Cities are likely to be early adopters and heavy users of AVEC, since cities are where many emergency incidents occur. However, wide adoption may be hampered by network providers who resist involving third parties in boosting their network performance. This may be lessened by greater AVEC security and the lower cost of temporary infrastructure instead of under-used permanent fixtures. Operators AVECs on their own service cars (which are pre-authorized to act as MECs) could bring quick value and enhance reputation. PPDR/ESOs may hesitate before letting network providers use their vehicular spare capacity, but the rewards of improved services are concrete and immediate.

B. Technology Gaps

Optimizing Opportunistic NFV: The process of selecting VFs should consider the dynamicity and mobility of the resources in the effort to provide processing stability and 'headroom' for continuity. Optimizing opportunistic NFV is made more complex where decisions are made for vehicles while they are in the B-Zone, during the eligibility checking process, so the probability ratio for zone persistence is particular useful. This involves assessment of vehicular mobility context together with predicted persistence within the A-Zone, based on staying patterns per PPDR/ESO. Opportunistic NFV should consider the collaborative effect in terms of the total communal capacity available per particular function, so the Virtualized Functions are prioritized accordingly. The selection of VFs must also consider other conditions, e.g. battery/mains power affected by VF processing rate of consumption and the spectrum frequencies that are associated with it. The impact of restored VFs on the rest of the communal hosting is also a factor.

Network slicing enablers: Ensuring privacy and enhanced quality for critical communication means segregation of communication streams. Emerging techniques of network slicing into channels with different levels of QoS and security will do just that. With differentiation of connectivity requests, different network slices can be assigned to the three levels: services for critical emergencies, essential services, and the general public. Network slicing, as described in [13,14], requires the same features as for AVEC: Slice Selection (zone identification); Mobility (vehicular context); Network authorization (AVEC binding); Subscriber Identity (Vehicle/ user composite ID); Integration to 3rd party systems (collaborative hosting); Exposure to 3rd party management (Smart City AVEC access); Dynamic management (AVEC ad-hoc MEC binding); Multi-access network support and convergence. Slice segregation is performed by a) applications and/or b) class of users (e.g. emergency authorities), which relies on subscription authentication.

Edge controlled SDN: For AVEC scenarios, applications could be given priority levels, so that MCS traffic is distinguished from other video streaming, for example. However, beyond prioritization by the application type, SDN decisions should also depend on the vehicle positioning (e.g. A-Zone), and even the type of user, which is recognized by the application. Hence, the recipient network needs to accept rules that are imposed by a *customized edge* SDN controller on board the AVEC, in a reversal of the normal responsibilities.

Support for collaborative hosting: Collaborative hosting by third parties requires further attention to the multi-entity and communal aspects, including standards that streamline cross-entity administration. This also requires interfaces to be defined at lower layers of the network, such as considered in the concept of the NOS. The ability to temporarily bind an AVEC to a sector of the network requires both the vehicular units and the participating network to follow new standard NOS procedures.

Verifiable Identity and Vehicular Context: AVECs will exploit car-embedded SIMs in their eUICC (Embedded Universal Integrated Circuit Card) that are carrier-agnostic, which are now common practice as a result of a GSMA initiative. These SIMs offer secure private execution environment and mobility between carriers. They provide the 'root of trust' mechanism for secure authentication, but further verification and eligibility procedures are still required for AVEC eligibility. AVEC verification will confirm that this vehicle has been sent to the area by a specific PPDR/ESO

through a process that protects the information and merely sends verification tokens. Eligibility confirmation will be conveyed to the network to which the AVECs are to be attached. This must be a confidential process that will take place in the B-Zone, and will confirm eligibility of each vehicle according to the organization's daily roster for dispatching service cars, while the full list of the vehicles is never divulged. This can be achieved by extending the technique in [17] from a personal service to a cross-entity function that uses webID 'attributes' (i.e. eligibility) to verify the current car status in the AVEC community.

VI. SUMMARY

This study describes a vision for automotive virtual edge communicator that provides transient connectivity in times of network failure. The scheme allows PPDRs/ESO to bring their own network resources on-board service vehicles to affected areas, and heal stricken networks. This challenging concept highlights a wide tapestry of issues, for which we provide innovative solutions based on emerging technologies. The AVEC scheme relies on new features in opportunistic virtualization, edge SDN, external MECs, cross-entity communication, and multi-source eligibility verification. Implementation of a single-network solution is entirely feasible with upcoming technologies, but the full societal benefits will only be realized by collaboration of network providers with ad-hoc communities of service vehicles in crisis affected zones.

REFERENCES

[1] C. Becchetti, F. Frosali and E. Lezaack, "Transnational Interoperability: A System Framework for Public Protection and Disaster Relief," IEEE Vehicular Technology Magazine, vol. 8, issue 2, pp. 46-54, June 2013.

[2] R. Fantacci, F. Gei, D. Marabissi and L. Micciullo, "Public safety networks evolution toward broadband: sharing infrastructures and spectrum with commercial systems," IEEE Communications Magazine, vol. 54/4, pp. 24-30, April 2016.

[3] J. Gil Herrera and J. F. Botero, "Resource Allocation in NFV: A Comprehensive Survey," in IEEE Transactions on Network and Service Management, vol. 13, no. 3, pp. 518-532, September 2016.

[4] A. M. Medhat, G. Carella, C. Lück, M. I. Corici and T. Magedanz, "Near optimal service function path instantiation in a multi-datacenter environment," Network and Service Management (CNSM), Barcelona, 2015, pp. 336-341.

[5] S. Mehraghdam, M. Keller, and K. Holger, "Specifying and placing chains of virtual network functions," IEEE 3rd International Conference on Cloud Networking (CloudNet), Luxembourg, 2014, pp. 7-13..

[6] V.G. Vassilakis, I.D. Moscholios, B.A. Alzahrani and M.D. Logothetis, "A Software-Defined Architecture for Next-Generation Cellular Networks" IEEE International Conference on Communications (ICC), Kuala Lumpur, 2016, pp. 1-6.

[7] C. S. Hong, S. M. A. Kazmi, S. Moon, N. V. Mui, V. H. Duy, T. Trong Dao, I. Zelinka, H. Choi and C. Mohammed, "SDN Based Wireless Heterogeneous Network Management," AETA 2015: Recent Advances in Electrical Engineering and Related Sciences, Springer International Publishing.

[8] R. Copeland, "Automotive Context-Aware Policy System for Car Connectivity Requests," IEEE 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, 2015, pp. 128-135..

[9] L. Pu, X. Chen, J. Xu and X. Fu, "D2D Fogging: An Energy-efficient and Incentive-aware Task Offloading Framework via Network-assisted D2D Collaboration," IEEE Journal on Selected Areas in Communications (JSAC), Series on Green Communications and Networking, 2016.

[10] A. Ahmed and E. Ahmed ,"A Survey on Mobile Edge Computing," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016, pp. 1-8.

[11] S. Sardellitti, G. Scutari and S. Barbarossa, "Joint optimization of radio and computational resources for multicell mobile-edge computing," IEEE Transactions on Signal and Information Processing over Networks, vol.1, pages 89-103, 2015.

[12] S.C. Shah, Q.U.A. Nizamani, S. H. Chaudhdary and M.S. Park, "An Effective and Robust Two-phase Resource Allocation Scheme for Interdependent Tasks," Mobile Ad Hoc Computational Grids, Journal of Parallel and Distributed Computing, 2012.

[13] A. Corston-Petrie, "Network Slicing," Virtual Networks SIG, https://www.cambridgewireless.co.uk/media/uploads/resources/Virtual%20Networks%20Group/08.02.17/VirtualNetworks-08.02.17-BT-Andy_Corston-Petrie.pdf, February 2017.

[14] 5G Americas, "Network Slicing for 5G Networks and Services," https://www.ericsson.com/en/networks/topics/network-slicing November 2016.

[15] UL Transaction Security, "The Future of SIM," https://library.ul.com/wp-content/uploads/sites/40/2015/05/The-future-of-SIM.pdf, 2015.

[16] E. Janczukowicz, A. Braud, S. Tuffin, G. Fromentoux A. Bouabdallah and J.M. Bonnin, "Specialized network services for WebRTC TURN-based architecture proposal," ACM 978-1-4503-3477-8/15/04, 2015.

[17] R. Copeland and M. Copeland, "Independently Verifiable Identity Scheme (IVIS)," *2017 20th Conference on Innovations in Clouds, Internet and Networks* (ICIN), Paris, 2017, pp. 196-198..

[18] Mobile Edge Computing (MEC) Framework and Reference Architecture ETSI GS MEC 003 V1.1.1 (2016-03).

[19] V. Sciancalepore, F. Giust, K. Samdanis and Z. Yousaf, "A double-tier MEC-NFV architecture: Design and optimisation," 2016 IEEE Conference on Standards for Communications and Networking (CSCN), Berlin, 2016, pp. 1-6.

[20] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1657-1681, 2017.

[21] U. Sadiq, M. Kumar, A. Passarella and M. Conti, "Service Composition in Opportunistic Networks: A Load and Mobility Aware Solution," in IEEE Transactions on Computers, vol. 64, no. 8, pp. 2308-2322, August. 1 2015.

[22] X. Ge, Z. Li and S. Li, "5G Software Defined Vehicular Networks," in IEEE Communications Magazine, vol. 55, no. 7, pp. 87-93, 2017. doi: 10.1109/MCOM.2017.1601144.

[23] M. Jutila, "An Adaptive Edge Router Enabling Internet of Things," IEEE Internet of Things J., vol. 3, no. 6, pp. 1061–69, December 2016.

[24] K. Liu et al., "Cooperative Data Scheduling in Hybrid Vehicular Ad Hoc Networks: VANET as A Software Defined Network," IEEE/ACM Trans. Net., vol. 24, no. 3, pp. 1759–73, June 2016.

[25] M. Manic, D. Wijayasekara1, K. Amarasinghe, J. Hewlett, K. Handy, C. Becker, B. Patterson and R. Peterson3, "Next Generation Emergency Communication Systems via Software Defined Networks," Research and Educational Experiment Workshop (GREE), 2014.

[26] I. Ku, Y. Lu, M. Gerla, R. L. Gomes, F. Ongaro and E. Cerqueira, "Towards Software-Defined VANET: Architecture and Services," Ad Hoc Networking Workshop (MED-HOC-NET), 2014 .

[27] Transatel "Security For The IoT," http://www.transatel.com/wp-content/uploads/2017/03/Security-for-the-IoT_Feb_2017_high-res-1.pdf

[28] R. Copeland, K. Corre, I. Friese and S. El Jaouhari, " Requirements for Trust and Privacy in WebRTC Peer-to-peer Authentication," IETF draft September, 2016

[29] [mie] V. Frascolla et al., "5G-MiEdge: Design, standardization and deployment of 5G phase II technologies: MEC and mmWaves joint development for Tokyo 2020 Olympic games," 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, 2017, pp. 54-59. doi: 10.1109/CSCN.2017.8088598.