Annals of Telecommunications
https://doi.org/10.1007/s12243-019-00719-5

"CFP: TECHNIQUES FOR SMART & SECURE 5G SOFTWARIZED NETWORKS"

Automotive virtual edge communicator (AVEC) with vehicular inter-agent service orchestration and resourcing (ViSOR)

Rebecca Copeland[1] · Michael Copeland[1] · Shohreh Ahvar[2] · Noel Crespi[2] · Oyunchimeg Shagdar[3] · Romain Durand[4]

Received: 2 June 2018 / Accepted: 7 June 2019

Abstract

At time of crisis, relief teams must have assured connectivity, not only just within the team but also across different service agencies in the area. Since emergency agencies and essential services always send service cars to affected zones, advanced technologies and computing resources aboard these vehicles can be pooled together to boost network capacity temporarily, just where it is crucially needed. These vehicles become automotive virtual edge communicators (AVECs). They are managed by a vehicular inter-agency service orchestration and resourcing (ViSOR) system that creates transient proximity-based "trust circles" to manage novel cooperative hosting, opportunistic virtualization, and "car sourcing" of crisis zone data. This study evaluates the feasibility for this challenging but highly rewarding concept and identifies gaps in emerging technologies.

Keywords MEC · NFV · PPDR · MCS · ITS · Blockchain

1 Introduction

The AVEC (automotive virtual edge communicator) as described in the conceptual study [1] is designed to support crisis situations, natural disasters, terrorist attacks, or urban unrest, when relief teams must cope with abnormal communication conditions, such as network downtime or crippling surges of traffic. The scheme is applicable not only in emergencies but also for scheduled uncommon situations, e.g., major network upgrade, mass crowding events, or green-site large construction projects, where multiple essential service agencies need to cooperate while network facilities are strained. In all these cases, boosting temporary connectivity is needed at a given spot for a finite duration.

The AVEC concept makes use of intelligence and computing power aboard service vehicles that rush to the affected areas. The vehicles may belong to emergency and essential service organizations, who must urgently overcome poor connectivity; hence, they would welcome bringing with them some network-boosting facilities.

The scheme is also useful to network providers, who can use their fleets of service cars to achieve cost-effective immediate network capacity increase, as and when needed, thus keeping infrastructure overhead costs much lower. Sharp spikes of demand are increasingly frequent since popular bandwidth services tend to create peaky traffic. In [2], analysis of average demand curves shows that traffic spikes rise exponentially while volume averages grow linearly, so the required infrastructure to support such occasional peaks becomes increasingly uneconomical. The AVEC scheme offers this sought-after network elasticity and cost-effective instant densification.

The AVEC concept provides more than a portable "hot spot" access—it assists in "healing" the network and propping up local connectivity by temporarily running hosted network functions, using pooled vehicular resources. This exploits emerging 5G technologies that integrate network resources from the smart edge: NFV (network function virtualization), MEC (mobile edge communications), converged multi-RAN (radio access network) access, network slicing for multi-SLA levels, and "connected cars" automation.

The proposed vehicular inter-agency service orchestration and resourcing (ViSOR) addresses orchestration and pooling of these self-selected nomadic resources from

✉ Rebecca Copeland
rebecca.copeland@coreviewpoint.com

[1] Core Viewpoint Ltd, Kenilworth, UK

[2] Institut Mines Telecom, Paris, France

[3] VeDeCom, Versailles, France

[4] Transatel, Paris, France

Published online: 19 June 2019

multiple agencies, supporting security and data privacy. The scheme creates proximity-based vehicular trust circles, enabling sharing vital local data securely between vetted teams in a defined zone.

This paper describes the vision and technology assessment that make the AVEC concept feasible. Section 2 is a survey of existing literature. Section 3 contains requirements by stakeholders. Section 4 explains the AVEC novel features. Section 5 describes the orchestrated services. Section 6 evaluates feasibility and technical gaps, followed by a summary.

2 Current status and existing literature

Collaborative network of vehicles We first proposed the concept for a vehicular network hub to support MCS (Mission Critical Services) in 2016, under the name "VV-MEC." Since then, a system of stand-alone hubs that contains a small cell and full 5G core on-board vehicles has attracted attention. Such a network-in-a-box creates an "island" of team connectivity but does not provide network healing or inter-team secure data sharing. It does not utilize built-in vehicular capabilities, thus increasing the unit costs considerably. By contrast, the collaborative AVEC and ViSOR solution is intended to mesh-in connected car technologies and computing power as cost-effective, targeted network resources.

Non-native CPE as infrastructure add-ons AVECs join the network as CPEs (customer premises equipment). In an ETSI paper (pages 5, 6) [3], distributed EPS (evolved packet system) functions on fixed enterprise-based CPEs are proposed. Although this is feasible, it is not underpinned by business rationale and cannot achieve instant coverage at the critical spot. By contrast, vehicular CPEs are sent to the affected zone anyway, and their owners are highly motivated to use their resources to ensure connectivity.

For CPEs to be accepted as non-native network resources, they must have stronger verification than any native server. Unlike stand-alone portable boxes, the vehicular CPEs can utilize further means of car authentication: in [4], car-embedded SIM is compared with exchangeable SIM, which is flexible but more vulnerable; in [5], combined firmware and high security measures are involved in vehicular validation; in [6], owners may confirm car assignments and attributes to cement proximity-based collaboration.

Automotive services The AVEC concept relies on utilizing built-in car sensors and communications. Car connectivity includes not only cellular but also various wireless LAN, Bluetooth, DSRC 5.9 GHz (dedicated short-range communications), and LiFi (light fidelity) technologies. Cars are equipped with short-range and long-range radars, multiple cameras, lidars (light detection and ranging), inertial measurement units, and GNSS (global navigation satellite system) receivers. The AVEC scheme will support car fleet service development that utilizes these capabilities in automotive service types, like those defined by ITS (intelligent transportation services): decentralized environmental notification message (DENM) [7] to alert for extreme weather condition, slippery road, or accidents; cooperative awareness message (CAM) [8] to announce vehicle presence; or collective perception message (CPM) to share sensor information.

MEC/NFV optimization The AVEC utilizes MEC standards [9], where vehicle-mounted hubs provide converged access plus virtualization. The NFV and MEC environments have been integrated in the MEC/NFV reference architecture [10]. The optimization of generic NFV is a popular topic [11], with many proposed methods for chaining virtualized functions (VFs) [12]. They focus on different goals, e.g., minimizing links, reducing delays, or conserving bandwidth, but the AVEC system must optimize according to mobility and dynamicity. This also involves managing VF instances as multi-party "micro-data centers"; chaining VFs where one resource donor is unknown [13]; and as optimized dynamic resource in opportunistic mobile phone networks [14].

Support for public protection and disaster relief Emergency communication services can use MCS as specified in 3GPP TS 23.179 over public mobile networks but only if they can be assured of reliable and secure connections, which the AVEC scheme reinforces. AVECs will also facilitate inter-agency collaboration that overcomes the lack of compatibility between national public protection and disaster relief (PPDRs) [15]. The guaranteed level of security in the public mobile network is provided by each operator running network slicing [16], through segregation of channels for assigned QoS and security levels. Different network slices can be assigned to different trust levels, distinguishing service-level agreements (SLAs) for different stakeholders or public services.

Sharing infrastructure Network operators have tried to share expensive infrastructure upgrades between them [17] with little success, due to inherent inter-competition barriers. Several European Mission Critical projects proposed solutions: in FP7 HELP, LTE-based PPDR with network and spectrum sharing was proposed [18]; in ISITEP, a framework for PPDR interoperability was designed; in DITSEF, self-organizing ad hoc networks were prototyped with nodes located in critical infrastructures. The issue with the proposed fixed infrastructure sharing is the required prior arrangement and achieving full coverage. By contrast, AVECs are available on-demand, already on-site when needed, available regardless of who the owners are, and require no long-term commitment between donors and consumers.

Zoning and car context Zoning means defining the area of interest, depending on purpose and activity. The physical zone is governed by spatial-temporal factors [19] and by vehicular accessibility. The networking zone may be based on 3GPP defined mobile management areas for coverage and handover. For AVEC, the synchronized physical zoning and network zoning constitute the operational area. For AVEC collaborative NFV, there is also the dimension of car mobility and context, i.e., movement/direction and presence patterns. Defining car mobility context [20] is a growing topic, especially for 5G-ITS services [21]. Zoning by mobility context is also studied on ad hoc grids in [22], aiming to reduce communication costs by utilizing user mobility patterns.

3 Stakeholders requirements and benefits

3.1 The stakeholders

The requirements for the proposed system flow from both donors and recipients of spare resources. Figure 1 shows the involved entities and the range of services they wish to access:

- Emergency agencies (PPDRs), using secure MCS
- Essential Services, using mobile/cloud support services
- Network providers using 5G/4G, smart city, V2V/V2X
- The general public, using "best-effort" communications

Emergency agencies are the first responders who rush to a crisis zone. They rely heavily on secure communication, so they would be willing to equip vehicles with AVEC units to ensure connection availability. PPDRs are already migrating to 3GPP-defined MCS services on non-dedicated mobile networks, which are deemed more cost-effective than private networks, but this is conditional on having appropriate security and resilience, which the AVEC will support. Collaborating with other emergency forces significantly enhances their efficiency; if system incompatibilities can be overcome, so proximity-dependent time-limited data sharing between trusted circles may provide a practical solution.

Essential services agencies also send service vehicles to affected areas. They are utilities (electricity, gas), road maintenance, car rescue/roadside repair, city street services, or public transport. Their scope is not only just emergency relief but also scheduled operations, large projects, and public events; hence, they represent a substantial market for AVECs. They still need resilient connectivity at trouble spots and would favor bringing their own assured connectivity to the site.

Network Providers 'consume' AVEC resources, whether they are their own resources or resources that are offered by third parties. Their own vehicles act as native edge resources that boost network capacity temporarily to satisfy unusually high demand and save costs of over-provisioned infrastructure that may be needed for rare communication spikes. Native AVECs do not need elaborate verification but still need resource discovery and integration. They may not reach the scene as fast as emergency vehicles, so despite initial reticence, network providers are likely to accept donated resources. Unlike cross-operator infrastructure sharing, using customer equipment is not competitive, and such cooperation may even lead to better relationships with numerous car fleet owners.

The general public benefits from the AVEC scheme by gaining precious connectivity in time of crisis. This enhances

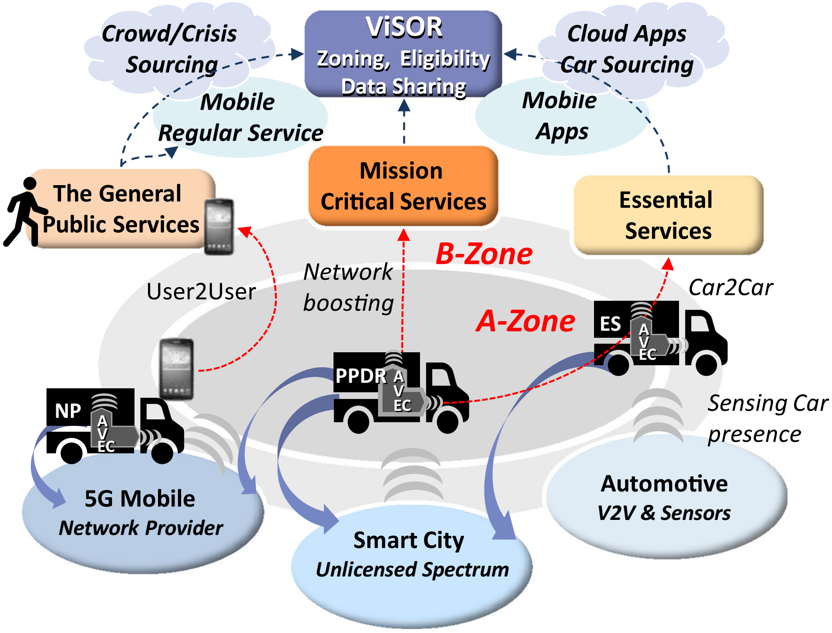

Fig. 1 The AVEC ViSOR stakeholders and services

the network provider's reputation, since such occasions are especially memorable. Additionally, this will facilitate citizens' crisis-time crowdsourcing, which often provides valuable information from the crisis zone.

3.2 Service guarantees and security levels

Different stakeholders demand varying degrees of quality and security which can be achieved by mobile network slicing. As shown in Fig. 2, three levels can be identified.

Level 1 is for PPDRs who need the highest security and critical communication prioritization. Level 2 is for essential services who require protection and high availability but lower priority. Level 3 is the general public service with "best-effort."

Vehicular authentication as well as NFV eligibility validation must be carried out, to reassure recipient networks that AVECs are tamper-proof and capable of hosting core network functions for the required duration. A secure connection over IP Mobile and private data networks is necessary for security levels 1 and 2. On-board TURN servers [23, 24] were previously thought to fortify Internet security, but returning traffic does not follow the same routes; hence, level 3 can only promise "best-effort" for Internet connection.

4 The AVEC concepts

4.1 Vehicular MEC

While fixed mobile edge functions are now well understood, portable MECs still need exploring. Fixed MECs allow for static distribution of functionality to servers at the edge, e.g., on packet data gateways, while vehicular MECs achieve more pinpointed densification. Portable hubs can be brought by cars to the required spot and plugged in as fixed MECs for a short duration, but such self-sufficient portable servers do not use car intelligence. The AVEC is a vehicular MEC that utilizes the integral car communication and sensing capabilities. It needs to connect to local RANs and backhaul or relay signaling, hop-by-hop via other AVECs, to reach a terrestrial network presence point. Signaling can also be enabled by V2V (vehicle-to-vehicle) spectrum and V2X (vehicle to anything) methods, as specified in 3GPP TR 23.786.

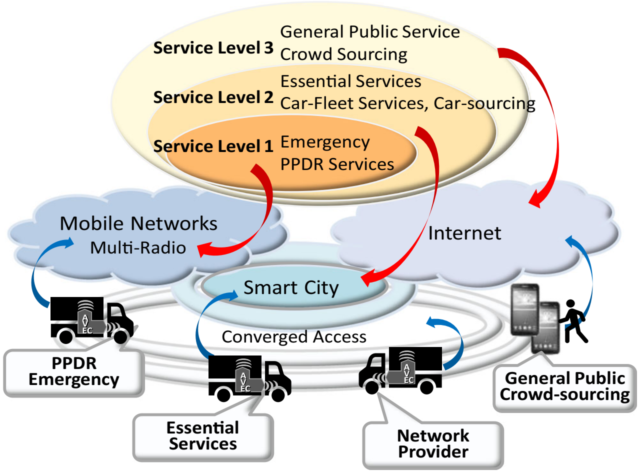

Fig. 2 Service security levels (source [1])

4.2 Vehicular virtualization with network slicing

The AVEC scheme makes it possible for vehicles in the vicinity to host virtualized EPS functions (3GPP TS 22.278), by pooling together their resources. Applications using 3GPP MCS need to operate securely; therefore, service guarantees will be assured by applying network slicing across the participating AVECs and the end-to-end channels. Note that hosting choices, VF placement, and network slicing are all under the control of each recipient network.

4.3 Non-native CPEs

The AVEC approach is to harness vehicles' computing capacity and connectivity capacity that do not necessarily belong to the native network, thus introducing non-native hosting contributors. Autonomous car services explore network interactions, but it is quite a leap to consider vehicles providers of network resources, instead of consuming them. This constitutes a reversal of roles, when network functions are hosted on customer equipment, rather than customer services hosted on the network infrastructure.

The main advantage of non-native CPEs is the collaboration of donors and recipients and the efficient resource usage. However, the availability of non-native CPEs is driven by their owners' schedules, not by the network NFV requirements. AVECs are withdrawn from the resource pool when the vehicles exit the zone or have overriding priorities under their own tasking. Hence, VFs must be carefully allocated across native and non-native AVECs and, when needed, transferred to other AVECs.

4.4 Managing CPEs hosting by blockchain

The cooperative hosting must be supported by a suitable cross-entity business framework. Hosting on mixed native and non-native nodes requires appropriate administration and auditing that manages on-the-fly dynamic provisioning of the multiple heterogeneous access nodes with assured transparency.

A flexible approach would be to use blockchain. With blockchains, AVEC nodes automatically negotiate short-term smart digital contracts with network providers. Each AVEC agrees on best-fit "contract" according to owners' preferences and requested service guarantee levels. Since each trust circle has a limited number of actors (i.e., it is limited in scale), private blockchain systems are perfectly suitable. Usage of donated resources is logged in auditable transactions that both donors and consumers can see, thereby enhancing transparency and trust.

4.5 Harnessing vehicular sensors

AVEC functionality is enriched by the growing power and sophistication of vehicular sensors. This includes on-board licensed and unlicensed radio technologies, environmental and motion metering, and extensive visual sensors. Vehicular sensors contribute to many upcoming services, e.g., detect road obstacles, ground-level conditions, proximity and congestion, but more importantly here, they are used by the AVEC scheme:

- Car proximity sensorial detection can be used to confirm circle members for data sharing;
- VF allocation may consider car metering, such as battery and power consumption of radio technologies;
- Car location sensors and visual recording can determine affected zone perimeters more accurately than traditional satellite navigation, e.g., by using urban roadside sensors, car landmark detection and car dynamic maps.

5 ViSOR orchestration and management

5.1 Dynamic trust circles

Deployment of AVECs requires an orchestration system—vehicular inter-agency service orchestration and resourcing (ViSOR), as in Fig. 3. ViSOR creates a temporary community, or a circle of trust, for collaborating network-native and non-native service vehicles within an affected zone.

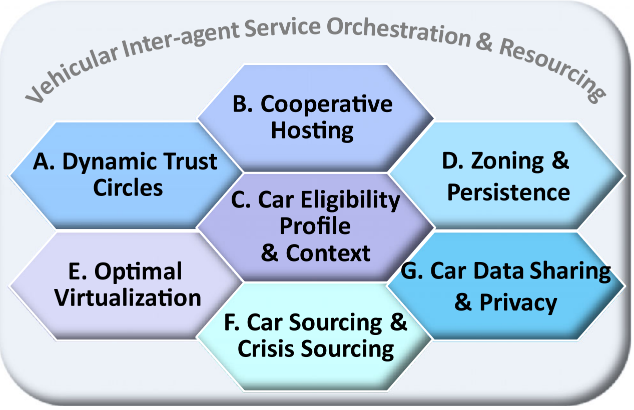
Vehicular Inter-agent Service Orchestration & Resourcing
A. Dynamic Trust Circles
B. Cooperative Hosting
C. Car Eligibility Profile & Context
D. Zoning & Persistence
E. Optimal Virtualization
F. Car Sourcing & Crisis Sourcing
G. Car Data Sharing & Privacy

Fig. 3 ViSOR functions

Vehicles join the trust circle when they respond to a beacon from roadside units or an invitation through proximity recognition. AVECs participate in the trust circle while they are within the zone perimeter and can share vital local data even if they do not contribute to the virtualization effort. The circles are dismantled when all the cars have left the zone.

Network providers join a circle when their network overlaps the affected zone, and they wish to support their network performance. ViSOR functions interact with the local networks via APIs that assist joining an active circle and allow requesting specific resources.

5.2 Cooperative hosting

The management of native and non-native resources in cooperative hosting requires a network-independent service that orchestrates participation and performance for the zone. As mentioned above, it is proposed to use blockchain for smart contracting on-the-fly and transparent transaction recording to manage the negotiation between the donors and recipient networks for each VF placement. ViSOR enables AVECs to assign spare capacity to be donated and the recipient network to decide on attaching VFs to available AVECs. Virtualization may create multiple instances of the same function on different vehicles or multiple AVECs for a single function.

The running of NFV must not interfere with the execution of car internal computing, so the VFs are performed in sandboxes or clearlinux containers that isolate the executed software from the car's internal processes.

5.3 Eligibility and authentication

AVECs need permission to join particular trust circles; network admission as non-native CPE by each recipient network; and acceptance for virtualization of core functions. ViSOR aids these processes with its eligibility procedures: The ID eligibility maintains an AVEC profile, linking car details, driver's details, and car fleet owner; the dynamic eligibility determines proximity and mobility, to verify car positioning within affected zones and car mobility status (approaching or leaving direction); the virtualization eligibility supports VF placement, matching specific network requests with the AVECs' resource details, release compatibility, currently available computing capacity, power status, and predicted duration.

The ViSOR authentication procedures address cars as servers, not as individual devices, and links to car fleets and drivers. This robust authentication utilizes several data items: vehicular embedded SIM that is used for car communications; car registration; driver's personal mobile phone; and driver's validation by the owning car fleet. To achieve even greater trust, car assignment, and routing can be dynamically confirmed by the owning agency, e.g., the vehicle dispatching to the relevant zone. To preserve confidentiality, individual confirmations can be automatically sent from each car owner to the target network directly, as described in [6], while the full list of dispatched vehicles remains confidential.

5.4 Zoning and zone persistence

ViSOR determines zone perimeters for each trust circle. Initiated by a disaster alert or a calendar event, the physical zone perimeter is assumed, given the type of activities or circumstances, e.g., crowded football match, smart city road maintenance, massive road accident, earthquake, or flooding areas. The physical perimeter should be defined widely enough, e.g., to incorporate the root cause location and vehicular physical access roads. The exact perimeters may be aided by AVEC visual reporting via car sourcing on the site.

The network zone depends on recipient networks that determine where connectivity boosting is needed. The definition must consider end-to-end signaling and local backhaul. The resulting network zone combines the requirements of the participating networks and is correlated with the physical zone.

ViSOR zoning determines AVEC eligibility to participate in specific trust circle. AVEC selection for VFs depends on their zone persistence, i.e., the vehicle's predicted stable duration within the zone. Persistence forecast is assessed by historical average stay duration, modeled by previous patterns per car fleet. AVECs with predicted short zone persistence can still be useful for short-duration VFs, such as one-off repair procedures. On the other hand, long-stay AVECs will be allocated to continuous communication, e.g., continuous video streaming.

AVECs chosen by operators for NFV must still be "discovered" and incorporated into their network resource map. Since network connectivity may be diminished or severed, the binding to the network must be performed before reaching the affected zone, i.e., in the buffer zone (B-Zone) outside the perimeter of the affected zone (A-Zone). This buffer zone must be large enough to engage AVECs with a network before connectivity is impaired, allowing time for administrative processes and API downloading. An AVEC may be moving between A-Zone and B-Zone, but once it leaves the area altogether, its resources are withdrawn from the resource pool and the network binding is disengaged.

5.5 Optimal Virtualization

ViSOR collaborates with the network NFV managers to attach VFs to eligible AVEC resources, considering their nomadicity and dynamicity and the VFs' execution demands. Matching them is based on several factors, including the VF process longevity and their repetitiousness and the AVECs' predicted persistence and capacity. ViSOR will notify participating networks when long-stay native AVECs are needed for some long VFs, so more native AVECs may be sent in. Other factors include preferred radio type, strength of signaling in the zone, and spectrum energy efficiency (if using car battery where power supply is scarce).

5.6 Crisis sourcing and car sourcing

ViSOR will support collecting visual evidence captured by end user devices as well as visual recording by the cars. This crisis sourcing system formalizes "crowdsourcing" in affected zones. It means opening scarce connectivity resources to the public standard mobile service so that citizens will post essential local data on a secure portal, which will provide vital information to the relief teams without delay.

Furthermore, vehicular sensors and cameras can contribute car sourcing data—by automatically posting streamed sensor output that provides crucial details of ground-zero status. This will deliver useful information in a more timely fashion without human intervention and will assist in mapping out affected zone perimeters.

5.7 Car data sharing and privacy

ViSOR will provide data sharing in affected zones between relief teams and local agencies, which is highly sought after. Inter/intra-agency information may consist of situation reports, coordination of traffic, detailed large-scale maps, building plans, water hydrants locations, or power supply. Data sharing also includes car sourcing (captured sensor data) from the site. This information may be sensitive, requiring filtering and restricting the distribution. Details caught on camera may inadvertently reveal personal details as well as pinpointed locations, which are subject to privacy regulations, e.g., General Data Protection Regulation (GDPR) in Europe. Commercial confidentiality is also an issue, as many organizations are reluctant to divulge car deployment details. Hence, the AVECs must be equipped with automated filtering and data sanitization. Since it is proposed to share data only within the trust circles for the duration of the stay, the distribution is restricted, and data is only available to members who have been meticulously vetted.

6 Evaluation

6.1 Feasibility and adoption

The AVEC scheme is unquestionably challenging, but the rewards to stakeholders are immense. The cooperative hosting concept is yet to be accepted by established network providers, and the inter-agency business framework needs to be formalized to operate on-the-fly. However, early implementations can succeed with simple use cases, implemented in local pockets of trusted regional participants. It needs relatively little outlay of investment, and it brings benefits even in small deployments.

Adoption by emergency and essential services depends on achieving management simplicity and low cost, while assisting the migration to broadband MCS. Network security concerns can be alleviated by the proposed extensive vehicular verification and narrowly selected trust circles.

Smart cities have the greatest motivation to become early adopters, since they run their own fleets of service cars, support city WLAN, and experience most of the emergency incidents that frequently occur in urban areas. They would appreciate the system even without NFV, simply for hot spot densification, secure connectivity, and trusted shared data.

Most of all, adoption depends on developers of ViSOR systems, who would launch them as independent cloud-based services for local subscribing networks and service agencies. These hosting service providers will appreciate the spontaneous creation of trust circles per crisis zone that supports a non-geographical approach that crosses telecom borders, while the small-scale circles (only few network providers and agencies in each locality) ensure manageability.

6.2 Research Opportunities

The AVEC concept raises several areas for research:

1. Opportunistic collaborative NFV: AVEC optimization algorithms need to remap VF topography to volatile resources. VF selection must consider network priorities, available computing capacity, and vehicular power consumption. Additionally, dynamicity (in-out of zones), mobility direction (towards-away), and predicted stability (modeled persistence) are important factors. Spatial-temporal algorithm, such as time-based Voronoi diagrams [25], may be used, with an added dimension for the AVEC mobility context.
2. Vehicular eligibility verification: Executing composite ID authentication for user-associated objects and with multi-party attribute verification that preserves privacy requires a procedure that needs ruggedization, security protection, and performance assurance and would benefit from standardization.
3. Car data privacy: Rules should be defined for car data privacy as a special case for GDPR, since unintended disclosure can occur through divulging location with driver association. Extensions to GDPR rules will protect commercial car owners as well as drivers in person and cover mobility privacy aspects.
4. Transient trust circles with blockchain auditing: Providing ad hoc secure services for dynamically formed interest groups requires web-like agility in telecom management systems. This may be achieved by private blockchain and smart contracting, with suitable security. Adaptation is needed for multi-party transactions and contracting terms.
5. Car sourcing: Although crowd sourcing is already a research topic [26], automated car sourcing is yet to be explored. It is much more efficient in obtaining vital data in a timely manner, but it needs aggregation of captured vehicular sensor data with suitable analytics and confidentiality procedures.

7 Summary

This study describes the vision and rationale for automotive virtual edge communicators that provide transient connectivity in times of crisis and network failure. The scheme allows emergency and essential services to pool together resources on-board service vehicles and to provide temporary access nodes and virtualization capacity. This challenging concept is based on strong stakeholders' motivation, but there are many issues in cross-party vehicular resource orchestration, VF optimization, and zoning. While the scheme is feasible using emerging 5G NFV, MEC, network slicing, and automotive technologies, the study highlights technology gaps to be studied further.

References

1. Copeland R, Ahvar S, Crespi N, Copeland M, Durand R, Duquerrois J-M, Paganelli F, Battisti F, Neri A (2018) Technology assessment for mission-critical services on automotive virtual edge communicator (AVEC). Conference on innovations in clouds, Internet and networks
2. Wood R (2013) Fixed internet traffic worldwide: forecasts and analysis 2013–2018. Analysys Mason Ltd, London
3. MEC deployment of mobile edge computing in an NFV environment. ETSI GR MEC 017 V1.1.1 (2018–02), pp 6,7
4. UL Transaction Security (2015) The future of SIM. https://library.ul.com/wp-content/uploads/sites/40/2015/05/The-future-of-SIM.pdf. Accessed 12 June 2019
5. Transatel (2017) Security for the IoT. http://www.transatel.com/wp-content/uploads/2017/03/Security-for-the-IoT_Feb_2017_high-res-1.pdf. Accessed 12 June 2019
6. Copeland R, Copeland M (2017) Independently verifiable identity scheme (IVIS). Conference on Innovations in Clouds, Internet and Networks, pp 196–198
7. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of decentralized environmental notification basic service (2010) ETSI TS 102 637–3, V.1.1.1
8. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of cooperative awareness basic service (2011) ETSI TS 102 637–2, V.1.2.1

9. Mobile edge computing (MEC) framework and reference architecture (2016) ETSI GS MEC 003 V1.1.1
10. Sciancalepore V, Giust F, Samdanis K, Yousaf Z (2016) A double-tier MEC-NFV architecture: design and optimisation. IEEE Conference on Standards for Communications and Networking (CSCN), pp 1–6
11. Gil Herrera J, Botero JF (2016) Resource allocation in NFV: a comprehensive survey. IEEE Trans Netw Serv Manag 13(3):518–532
12. Mehraghdam S, Keller M, Holger K (2014) Specifying and placing chains of virtual network functions. IEEE 3rd International Conference on Cloud Networking (CloudNet), Luxembourg, pp 7–13
13. Dieye M, Ahvar S, Sahoo J, Ahvar E, Glitho R, Elbiaze H, Crespi N (2018) CPVNF: cost-efficient proactive VNF placement and chaining for value-added services in content delivery networks. IEEE Trans Netw Serv Manag 15:774–786
14. Sadiq U, Kumar M, Passarella A, Conti M (2015) Service composition in opportunistic networks: a load and mobility aware solution. IEEE Trans Comput 64(8):2308–2322
15. Becchetti C, Frosali F, Lezaack E (2013) Transnational interoperability: a system framework for public protection and disaster relief. IEEE Veh Technol Mag 8(2):46–54
16. 5G Americas (2016) Network slicing for 5G networks and services. https://www.ericsson.com/en/networks/topics/network-slicing. Accessed 12 June 2019
17. Li T, Bai L (2011) Model of wireless telecommunications network infrastructure sharing & benefit-cost analysis. International conference on information management, innovation management and industrial engineering, Shenzhen, pp 102–105
18. Fantacci R, Gei F, Marabissi D, Micciullo L (2016) Public safety networks evolution toward broadband: sharing infrastructures and spectrum with commercial systems. IEEE Commun Mag 54(4):24–30
19. Meireles R, Steenkiste P, Barros J, Moura DC (2016) LASP: lookahead spatial protocol for vehicular multi-hop communication. IEEE Vehicular Networking Conference (VNC), Columbus, OH, pp 1–8
20. Copeland R (2015) Automotive context-aware policy system for car connectivity requests. IEEE International conference on intelligence in next generation networks, pp 128–135
21. Qiu H, Chen J, Jain S, Jiang Y, McCartney M, Kar G, Bai F, Grimm DK, Gruteser M, Govindan R (2018) Towards robust vehicular context sensing. IEEE Trans Veh Technol 67(3):1909–1922
22. Shah SC, Nizamani QUA, Chaudhdary SH, Park MS (2012) An effective and robust two-phase resource allocation scheme for interdependent tasks. Mobile ad hoc computational grids, Journal of Parallel and Distributed Computing 72(12): pp 1664–1679, December 2012
23. Janczukowicz E, Braud A, Tuffin S, Fromentoux G, Bouabdallah A, Bonnin JM (2015) Specialized network services for WebRTC TURN-based architecture proposal. ACM 978-1-4503-3477-8/15/04
24. Punnoose RJ, Tseng RS, Wang S, Nikitin PV, Schlesinger TE, Stancil DD (2001) Communications resources management for advanced telematics applications. IEEE Intelligent Transportation Systems. Proceedings (Cat. No.01TH8585), Oakland, CA, pp 1056–1060
25. Das GK, Das S, Nandy SC, Sinha BP (2006) Efficient algorithm for placing a given number of base stations to cover a convex region. J Parallel Distrib Comput 66:1353–1358
26. Kobayashi K, Shishido H, Kameda Y, Kitahara I (2017) Method to generate disaster-damage map using 3D photometry and crowd sourcing. IEEE international conference on big data

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.