5GASP: Security and trust in NetApp deployment and Operation

Jorge Gallego-Madrid, Ana Hermosilla, Antonio F. Skarmeta
Department of Research and Innovation
Odin Solutions
Murcia, Spain
{jgallego, ahermosilla, skarmeta}@odins.es

***Abstract*—The adoption of 5G solutions in the industry vertical passes through the empowering of 5G-based Network Applications (NetApps) in the SMEs. This will unleash their potential with respect to the use of 5G technologies, while preparing them for beyond 5G. H2020-5GASP project aims to create an open, and inter-domain 5G NFV-based reference ecosystem of 5G European experimental facilities for SMEs, fully automated and self-service, in order to foster rapid development and testing of new and innovative NetApps, which will be built using the proposed 5G reference architecture. Furthermore, it will provide security and trust of 3rd party IPR running in the deployed testbed.**

Keywords—5GASP; NetApps; H2020;

I. EXTENDED ABSTRACT

As 5G approaches a very high maturity level, the testing and validation of the innovations achieved in 5G by integrators and verticals service providers has become of utmost importance. Verticals have very different needs, such as the case of the Automotive industry and Public Protection and Disaster Relief (PPDR). Thus, they will require different levels of support evolving their applications from ideas to prototypes and finally to products.

In this way, the objective of 5GASP is to shorten the idea-to-market process through the creation of a European testbed for SMEs that is fully automated and has self-service provisioning. With this idea, the development and testing of new and innovative NetApps can be fostered by using the newly proposed 5G Network Function Virtualization (NFV) based reference architecture. Building on top of already existing 5G physical infrastructures, 5GASP intends to focus on innovations related to the operation of experiments and tests across multiple domains, providing software support tools for Continuous Integration and Deployment (CI/CD) of VNFs, in a secure and trusted environment for European SMEs capitalizing in the 5G market.

5GASP aims to create a Virtual Network Function (VNF) marketplace with an Open Source Software (OSS) repository targeting SMEs with building blocks and VNF OSS examples. Besides, it targets the incubation of a community of NetApp developers assisted with a series of tools and services that can be used to validate and certify the formulated products and services for 5G. The project is focused on inter-domain use cases, development of operational tools and procedures and security and trust of 3rd party IPR running in the multiple testbeds.

Accordingly, the main technical objective of 5GASP is to build and operate an Open, and Inter-Domain 5G NFV-based Reference (Open5G-NFV) ecosystem of Experimental Facilities. This ecosystem shall not only integrate existing facilities already proven in previous ICT projects but shall also lay down the foundations for instantiating fully softwarized architectures of vertical industries. Further on, it shall provide facilities to test and validate NetApps taking into consideration vertical-specific requirements. 5GASP will demonstrate its Open5G-NFV ecosystem for the specific verticals deployed across state-of-the-art 5G infrastructures: Automotive and Public Protection and Disaster Relief (PPDR); however, it will also be as generic as possible in order to deploy, validate and certify NetApps stemming from other verticals.

5GASP also aims to provide a set of exemplary use cases to be used first as showcases to prove the functioning of the platform and to collect principles, lessons learnt, good practices in the process of onboarding, developing, testing, validation and certification of NetApps that will help future developers to accelerate the design, development and deployment of NetApps. The initial set of NetApps covers an extensive range of use cases in the Automotive and PPDR ecosystems, such as a virtual On-Board Unit (vOBU), a virtual RoadSide Unit (RSU), a ITS station, Multi-domain Migration, Vehicle-to-Cloud (V2C) Real-Time Communication, Remote Human Driving, Efficient MEC Handover, Privacy Analysis, 5G Isolated Operation for Public Safety, or Vehicle Route Optimization.

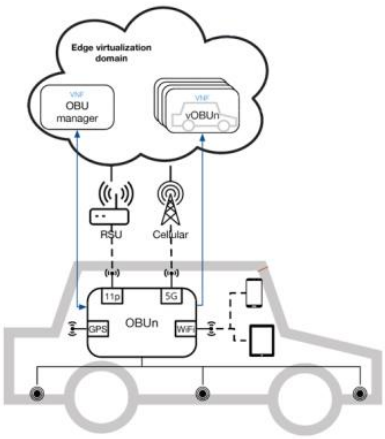

Fig. 1. *vOBU NetApp*

The vOBU NetApp (Fig.1) can perfectly illustrate the usefulness of the Open5G-NFV ecosystem that 5GASP is aiming to create. In this case, from the point of view of the Automotive vertical and including data access management control, access mechanisms, and privacy management. One of the founding pillars of 5G ecosystem is the softwarization [1] and virtualization of computing and network resources, in the form of Software Defined Networks (SDNs) and NFV. These advances have enabled the possibility to easily design and implement the offloading of tasks performed by mobile devices and ensure low latency responses due to the proximity of the computing facilities to the point of attachment. This is called Multi-access Edge Computing (MEC). In this way, the novel idea of instantiating virtual substitutes for the OBUs that are physically located into the vehicles has been proved to be beneficial in terms of device access delay, reliability against wireless disconnections or data cache. This has been demonstrated in the SURROGATES [2] proposal in the context of 5GinFIRE project [3]. This solution, introduced as a NetApp, provides the necessary vOBUs that are instantiated at the edge of the access network with the purpose of offloading high computational cost tasks to the network following the MEC approach. Thus, the NetApp can be used to gather logging information about the status of the vehicle and delegate the costly analytic processes to the virtual surrogate, which could also act as a proxy for external requests, avoiding them reaching the OBU, which should be focused in higher priority tasks.

In this way, besides the usefulness of the virtualization of the 5G ecosystem concerning the design and deployment of NetApps, another advantage is the menu of possibilities that appears for privacy management. These NetApps can be orchestrated in conjunction to provide a service of vOBUs, which will be deployed in a virtualized infrastructure. Therefore, the data flows exchanged between the physical OBU and the virtual surrogate, and between the latter and the application servers, can be continuously analyzed. Thus, multiple privacy enhancements can be adopted by the NetApp.

In the context of these kind of automotive scenarios, privacy enables the user to control which information is sent by the vehicle and how much time that data lasts. The content of these messages varies depending on the employed OBU, but it usually contains time, position, motion state, activated systems, dimensions, vehicle type, and role. The aim of these messages is to inform continuously other stations or applications about road safety related status and presence information. Anonymity is a common method to protect an individual´s privacy, and a digital pseudonym is a unique identifier used to authenticate the sent messages. To make it works, it must not contain any personal information linkable to the real identity of the holder.

In a similar way, the vOBU must also include access control mechanisms that manage the access to the data that it processes. Besides, this can be also enhanced due to one of the big advantages that provide the softwarization of the 5G infrastructure, that is the isolation of network resources among them by using Network Slicing [4]. In the Open5G-NFV proposed by 5GASP, the NetApps will be deployed on their own Network Slices, and, consequently, the traffic flows of the network will be effectively separated from each other. By doing so, the access control capabilities are greatly increased, as the network isolation eases the management of who can access a certain segment of the network.

5GASP vision is to introduce a well-defined approach to empower the use of NetApps in SMEs. To do so, it will implement a methodology to enable the automated and reproducible validation of NetApps across multiple 5G infrastructure sites. Thus, becoming a widely deployed and operational platform with strong industrial backup with the aim and potential to become a reference for validation and deployment of 5G experiments.

ACKNOWLEDGMENT

This work has been supported by Fundación Séneca — Agencia de Ciencia y Tecnología de la Región de Murcia — under the FPI Grant 21429/FPI/20, and co-funded by Odin Solutions S.L., Región de Murcia (Spain); by the Spanish Ministry of Science and Innovation through the Industrial PhD grant DIN2019-010827; and by the European Commission, under the 5GASP (Grant No. 101016448) H2020 project.

REFERENCES

[1] D. Lake, N. Wang, R. Tafazolli and L. Samuel, "Softwarization of 5G Networks – Implications to Open Platforms and Standardizations," in IEEE Access, doi: 10.1109/ACCESS.2021.3071649.

[2] https://5ginfire.eu/surrogate

[3] Aloizio P Silva, et al, 5GinFIRE: An end-to-end open5G vertical network function ecosystem," Elsevier Journal Ad Hoc Networks, 2019.

[4] R. Wen et al., "On Robustness of Network Slicing for Next-Generation Mobile Networks," in IEEE Transactions on Communications, vol. 67, no. 1, pp. 430-444, Jan. 2019, doi: 10.1109/TCOMM.2018.2868652.