Softwarization and Virtualization in 5G Networks for Smart Cities *

Massimo Condoluci[†], Fragkiskos Sardis[‡], and Toktam Mahmoodi[‡]

[†] Mediterranean University of Reggio Calabria, Italy
[‡] Department of Informatics, King's College London, UK

Abstract. Smart cities are one of the foreseeable mission-critical hybrid networks connecting machines and humans to provide various public services through highly reliable, ultra-low latency and broadband communications. It is known that the next generation mobile networks, a.k.a 5G networks, should address requirements of of such hybrid network inherently. Among the main features of 5G networks, therefore, are cognition and programmability that allow for addressing different needs. These features are so far discussed with the introduction of softwarization and virtualization technologies. In this paper, we briefly discuss how the two technologies enable use of 5G in the smart cities and allow for multiple tenants to share a common physical infrastructure. We further describe an example use case through which such multiple tenant environment can be designed.

1 5G in Smart cities

Faced with an ever larger portfolio of applications to serve, it is now commonly recognized that future networks will have to consider requirements by different vertical sectors. Despite earlier network generations that have been designed as general purpose connectivity platforms with limited differentiation capabilities across use cases and application environments [1], 5G needs to consider different sectors inherently in its design. Such design requirement is not only to consider very high bandwidth usage, but also for range of targeted applications such as mission-critical applications. The 5G mission-critical networks are hybrid networks that connect machines and humans to provide future services through highly reliable, ultra-low latency and broadband services. A good example of such hybrid network are the smart cities. Smart cities bring together mix traffic of machines and humans generated by various city-wide infrastructures and introduce plethora of opportunities as well as challenges.

Two of the main features of 5G design are cognition and programmability through softwarization and virtualization of the end-to-end chain of the radio, networks, applications and services. The two promising and well-developed

* This work has been supported in part by the 5GPP VirtuWind (Virtual and programmable industrial network prototype deployed in operational Wind park) Project.

technologies in this path are Software-defined networking (SDN) and Network Function Virtualization (NFV). Among other functionalities, SDN &NFV enable multiple tenants to share a common physical infrastructure. Comprising of various inter-related infrastructure, smart cities scenarios can benefit significantly from multi-tenant design.

To this end, we depict the vision of 5G in smart cities and briefly discuss role of SDN and NFV technologies in developing smart city networks in Sections 2 and 3. Afterwards, through a specific use case instance of emergency and transport services, we demonstrate how different actors can interconnect and how a multiple tenants can co-exist and co-operate (in Section 4). Finally, some concluding remarks are summarized in Section 5.

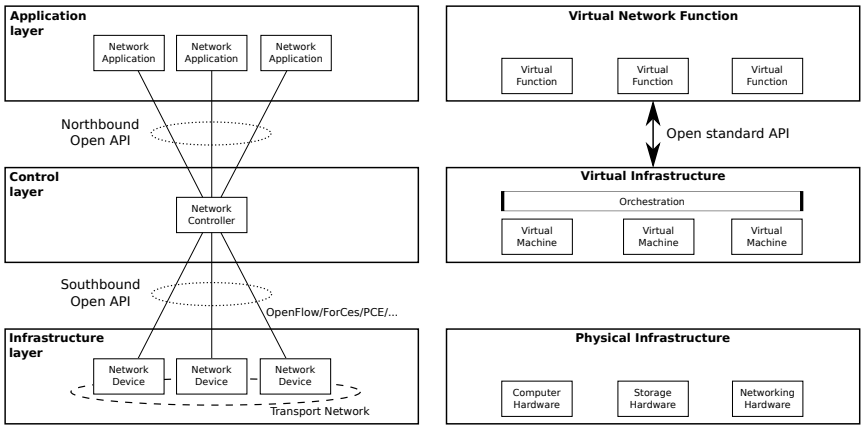
2 Softwarization and Virtualization in 5G

The introduction of cognition and programmability is considered as one of the main challenges to be handled in the mobile 5G with the aim to manage the increasing volume of traffic with different Quality of Service (QoS) requirements generated by huge load of heterogeneous devices. both cognition and programmability are needed to guarantee flexibility, reliability and auto-reconfiguration to 5G systems to always exploit the optimal network configuration according to the current state of the network. Different paradigms are currently investigated as enablers of such cognition and programmability in 5G. Among those, as for instance stated by [2], *softwarization* and *virtualization* are expected to have a significant impact on forthcoming 5G deployment trends as they guarantee to speed up the innovation of network architectures. Furthermore, softwarization and virtualization play a key role in *multi-tenancy* environments, where a single instance of a software application may serve multiple network operators. Furthermore, multi-tenancy allows for multiple users and organizations to share a common infrastructure by virtualizing hardware and sharing resources without private data and network traffic being exposed outside of their virtual boundaries. In the following, we will consider in detail these two enablers paradigms.

2.1 Software Defined Networking (SDN)

Softwarization is considered a key enhancement in the network design of next-to-come 5G systems, as for instance stated by [2] and [3]. In this direction, software-defined networking (SDN) is a promising architecture which aims to introduce meaningful benefits through *isolation of control plane* and the use of a *centralized network controller* handling control plane functionalities, such as the allocation of traffic to network elements. Network intelligence is centrally managed by the network controller and, thus, the network controller can output the best fine granular flow routing control rules to the heterogeneous network devices.

The network controller interacts with other network entities/layers through two interfaces, as considered in detail by [3] and depicted in Fig. 1(a). The



(a) Overview of SDN concept. (b) Overview of the NFV concept.

Fig. 1. SDN & NFV Illustration.

controller exploits the *northbound interface* with the aim to be as a single, logical switch to the upper layer network applications: this provides an overall overview of the whole network status (overloading, congestion, and so on) to network applications. The main benefit is in the deployment time of novel network functions/applications. The *southbound interface* is defined between the network controller and the network devices. Being widely supported by various device manufacturers, service providers, and operators, *OpenFlow* (defined by the Open Networking Foundation, ONF) is broadly considered as the dominating solution for implementing the southbound interface; more details on OpenFlow are given by [4]. Further solutions, such as ForCES and PCE, defined by the Internet Engineering Task Force (IETF) [5, 6], are available as southbound interfaces.

2.2 Network Function Virtualization (NFV)

The Network Function Virtualization (NFV) can provide the infrastructure on which SDN can run. Indeed, as discussed by [2, 7], NFV is a complementary technology of SDN which allows *(i)* to build a virtual-based end-to-end network infrastructure and *(ii)* to enable the consolidation of many heterogeneous network devices onto industry standard high-volume servers, switches, and storage.

The key characteristic of NFV paradigm is that network functions of a network device are implemented in a *software package(s)* and *virtual machine(s)* are used to run such packages. Therefore, NFV introduces flexibility in the network deployment as it the introduction/test of novel network functionalities becomes easier: only installation/upgrading of software package(s) is needed, without the need of hardware upgrade to network entities which obviously introduces higher delays. As a consequence, NFV reduces the time to market of novel network

functionalities with thus money saving. In addition, NFV allows network operators to build and operate a network with reduced equipment costs, as generic hardware can be used and properly tuned via software according to the need of the operator. More details on NFV technology are given by [8].

The architecture of NFV, described in Fig. 1(b), has the following characteristics:

- *Virtual infrastructure*: virtual machines run on generic high-volume hardware servers, equipped by storage devices and connected by network switches.
- *Software separation*: generic hardware is used by the software that defines the network functions for network devices, i.e., the hardware is not designed for specific task(s).
- *Automated orchestration*: the orchestration automates installation and management of the virtualized network functions on the generic hardware.

3 SDN & NFV in Smart Cities

The smart city scenario poses several challenges in the management of network resources. Indeed, a smart city environment is expected to be a heterogeneous scenario where different types of devices (e.g., smartphones, sensors, actuators) co-exist in heterogeneous deployments (e.g., macro, pico, femto-cells) and have heterogeneous traffic patterns (e.g., machine-type communications require high-reliability and low-latency to reduce the energy consumption while human-oriented traffic has less stringent requirements in terms of energy consumption).

This intrinsic heterogeneity in smart city environments requires quick reconfiguration of network parameters/deployment according to the current state of the network: this clearly shows the inefficiency in the current deployment strategies adopted by network operators, mainly based on pre-configured network parametrization and ad-hoc network devices with pre-defined tasks. In 5G systems, network has to be configured according to the use case but also the information such as traffic, mobility levels, interference levels, QoS requirements, overloading of radio/core segments and so on. Such information is obviously time-varying, and this consequently dictates for novel solutions allowing low-latency network reconfiguration. The above discussed softwarization and virtualization paradigms are useful to achieve the flexibility that smart city environments pose on 5G systems. Examples of the enhancements introduced by the exploitation of SDN/NFV are provided by [2] and are summarized here:

- dynamic cell configuration, traffic balance and resource management;
- spectrum and transmission powers to be assigned to involved cells;
- best interconnections between network devices;
- best connections between transceivers and physical elements;
- activation of the appropriate transceivers that will be involved in the handling of a particular situation.

Nevertheless, to reach these goals, several issues are to be taken into account. A first aspect is the need of dynamically redirecting user traffic when scaling offered services: this becomes challenging as is still not clear how existing SDN controllers perform in the wide area of 5G cellular systems. When considering the huge load relevant to smart cities, where enormous and unpredictable number of devices are expected to be simultaneously connected in a limited coverage area, *scalability* becomes the major concern to avoid network overloading and congestion. In addition, when focusing on applications where sensors and actuators need to communicate under strict latency requirements, overloading may involve unacceptable delays which may cause instabilities in some segments of the smart city.

Another interesting challenge is in the overhead reduction in applications like machine-type and the IoT, which are considered as primary services for smart cities. Communications inherent to such applications deal with the transmission of very limited traffic (few bytes) whose management in the current 3GPP standard involve high consuming of bearer resources in the core network. The overhead reduction needs a novel design for the protocol interfaces in the SDN/NFV 5G architecture to guarantee benefits for low-cost sensor devices (i.e., energy savings as lower number of control bits are needed for each data bit to be transmitted) and in the radio/core networks (i.e., lower amount of data/control resources are needed for data/control bearers).

Finally, a concern of notable importance is in terms of *security*. Indeed, in a NFV network, virtual applications run in data centers which may not be owned by network operators directly, i.e., virtualization may even be outsourced to third parties as considered by [9]. In addition, the introduction of orchestrators may generate additional security vulnerabilities with thus higher loads (and consequent higher delays) to the systems/functionalities of intrusion detection. Finally, security threats are also due to the use of shared networking and storage, i.e., when virtual machines share the physical resources with other network appliances or when software-based components are offered by different vendors; these scenarios may potentially create security holes due to integration complexity. As a consequence, operators need to make sure that the security features of their network will not be affected by above considered issues and this dictates to rethink security issues when designing/building 5G NFV systems.

4 Case of Multi-Tenancy in Smart City

This section illustrates an example use case in smart cities that is built on SDN & NFV -based 5G network, and explains a multi-tenancy design. We investigates how transport and emergency services in smart cities can make use of a shared network infrastructure to drive down their running costs, integrate more efficiently and automate certain aspects of their operations. According to a recent report by the UK metropolitan police, they receive more than five million calls per year on their emergency numbers and public increasingly want more flexible ways on interacting with the police [10]. Hence, automation in emergency

services can potentially have significant social impact. To study the interaction between emergency and transport services, we consider the use-case of an emergency incident occurring on the transport network and explore how the two services may communicate between them and with external actors in order to respond to the event.

4.1 Modelling Transport and Emergency Services

Transport and emergency services are composed of actors that report information, process data, make decisions and execute operations. The first actor involved in the use-case is the *emergency services* that receive incident reports from patrol units, civilians or roadside devices. The main task of this actor is to process such reports and determine how emergency services should respond in terms of units needed (police, ambulance, fire brigade), and what is the urgency level. It is therefore an actor focused on processing information and issuing instructions. Location of the incident, availability of emergency teams nearby and the traffic conditions on the roads are among the information that should be known to the actor. The second actor is the *transport services* with its main role in this use-case being, keeping track of the transport network's condition, the locations of emergency units, issuing traffic updates to the public and making traffic control adjustments when necessary. The third actor is the *roadside equipments and the officers*, that are the patrol units, roadside sensors, smart cars and civilians. This set of actors gives input to the emergency service by reporting incidents.

Finally, the fourth actor is the *traffic control* such as traffic lights, traffic sensors, electronic road signs and transport service officers. They are primarily tasked with informing civilians (or smart devices) of incidents and shaping the traffic in the transport network. Actors in this group also send periodic traffic updates to the transport services in order to maintain an overview of the congestion in the transport network. Fig. 2 presents the main components of the framework and the flow of information between them. It also includes input from policies that affect the behaviour of the system in terms of responding to events and handling traffic. The components of the framework are as follows:

- Emergency Service Policy: is responsible for controlling how the emergency systems respond to events.
- Event Response: receives information from *incident reporting actors* and the *location tracking*, utilizes the *emergency service policy*, and issues instructions to response units that can reach the location of the incident in the most optimal form.
- Location Tracking: tracks the location of incidents via input from the *incident reporting actors* via periodic updates from the units.
- Traffic Monitoring & Control: that is the main part of the transport network and receives input from the *transport service policy* and *roadside equipment and officers*.

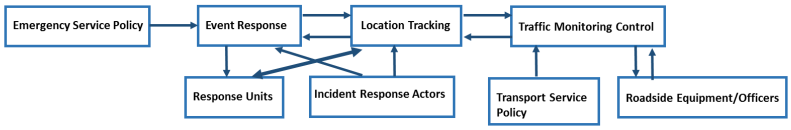


Fig. 2. Actors' communication in Transport & Emergency service model.

- Roadside Equipment & Officers: includes devices such as traffic lights and electronic road signs that may be remotely programmed, sensors for traffic measurements, and human officers.
- Incident Reporting Actors: include roadside sensors, embedded devices in smart cars, officers on patrol and civilians. When an incident is reported, the location of the incident is also submitted to the *location tracking*.
- Response Units: are the officers and fleet of vehicles of emergency services. They receive dispatch instructions from the *event response*. They also report periodically their status and location to the *location tracking*.

4.2 Illustration of the Example Use case

Using the above framework and actors, we can now envision a scenario where an emergency event has occurred in the city. Let's assume that the incident is reported by a smart car via the Internet. The *event response* will process the location of the incident as well as the vehicle involved and request the location of Response Units nearby. Upon determining the severity of the incident, it will dispatch the required units to the location. At the same time, it will send a request to the *traffic monitoring & control*, to prioritize traffic on the route of the emergency services; for example to update the timing on traffic lights.

4.3 Multi-Tenancy Network Considerations using SDN

After considering the example above, we can begin to examine the various communication methods and networking technologies required for this system to operate. We can identify four distinct infrastructures that are involved in achieving communication between the actors. The first one is the public network where all information gathering points, either machines or humans, are connected to. The second and third are the emergency services and the transport networks virtual infrastructure which are also connected to the public networks for data communications. Finally, the fourth infrastructure is the shared physical infrastructure that hosts the virtual infrastructures for emergency and transport services. This infrastructure physically peers with other public or private networks.

Communication between these infrastructure entities needs to adhere to QoS parameters in order to facilitate the communication between components in a reliable and timely fashion. Because the physical infrastructure is shared between

the two services, multi-tenancy and scalability issues have to be addressed in order to guarantee an optimal distribution of resources. Furthermore, depending on the type of communication and the volume of information, additional communication channels between the two virtual infrastructures may be created or removed. This will allow the physical infrastructure to provide additional resources when required or switch off physical interfaces to reduce power consumption when they are not needed.

5 Concluding Remarks

In this paper, we depict the vision of 5G in smart cities and briefly discuss role of SDN and NFV technologies in developing smart city networks. Through a specific use case instance of emergency and transport services, we demonstrate how multiple tenants can co-exist and co-operate. While complying with the traditional definition of multi-tenancy requires tenants to be restricted to control only their virtual space and not the physical infrastructure, our detailed use case here needs more stringent control. In this case, either of the emergency and transport services should have some control over the physical infrastructure so that they can program the SDN controller according to their needs. This requirement is mainly due to the sensitivity and critically of the emergency and transport services, and the fact that functionality of the physical layer plays an important role in the response time and the reliable operation of these services.

References

1. G. Araniti, M. De Sanctis, S. C. Spinella, M. Monti, E. Cianca, A. Molinaro, A. Iera, and M. Ruggieri, "Hybrid system HAP-WiFi for Incident Area Network," in *2nd International ICST Conference on Personal Satellite Services (PSATS)*, pp. 436–450, February 2010.
2. P. Demestichas, A. Georgakopoulos, D. Karvounas, K. Tsagkaris, V. Stavroulaki, J. Lu, C. Xiong, and J. Yao, "5G on the Horizon: Key Challenges for the Radio-Access Network," *VT Magz, IEEE*, vol. 8, pp. 47–53, Sept 2013.
3. D. Kreutz, F. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, vol. 103, pp. 14–76, Jan 2015.
4. A. Lara, A. Kolasani, and B. Ramamurthy, "Network innovation using openflow: A survey," *Commun. Surveys & Tutorials, IEEE*, vol. 16, pp. 493–512, First 2014.
5. "Forwarding and Control Element Separation (ForCES)." IETF RFC 5810, 2009.
6. "Path Computation Element (PCE) Communication Protocol (PCEP)." IETF RFC 5440, 2009.
7. T. Wood, K. Ramakrishnan, J. Hwang, G. Liu, and W. Zhang, "Toward a Software-based Network: Integrating Software-defined Networking and Network Function Virtualization," *Network, IEEE*, vol. 29, pp. 36–41, May 2015.
8. B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network Function Virtualization: Challenges and Opportunities for Innovations," *Commun. Magz, IEEE*, vol. 53, pp. 90–97, Feb 2015.
9. J. Sherry, S. Hasan, C. Scott, A. Krishnamurthy, S. Ratnasamy, and V. Sekar, "Making middleboxes someone else's problem: network processing as a cloud service," in *ACM SIGCOMM CCR*, pp. 13–24, 2012.

10. “One Met Total Technology 2014 - 2017.” Metropolitan Police, 2014.