A Dynamic, Plug-and-Play and Efficient Video Surveillance Platform for Smart Cities

G. Baldoni*, M. Melita**, S. Micalizzi*, C. Rametta*, G. Schembra*, A. Vassallo*

* DIEEI – University of Catania, V.le Doria 6, Catania 95125, Italy (name.surname@dieei.unict.it)

** Strategy & Innovation, Joint Open Lab - WAVE, Telecom Italia, Italy (name.surname@telecomitalia.it)

***Abstract* — This work presents a video surveillance platform for smart cities designed to exploit the facilities offered by SDN/NFV networks to achieve gain in terms of scalability, flexibility, OpEx and CapEx reduction. The main elements of this platform are the Smart Access Nodes (SAN) and the Network Access Nodes (NAN). SAN devices are distributed on the territory to cover small/medium areas and provide connectivity to Data Flow Senders and Users. Data flow Senders may be IP cameras, sensors and camera-equipped drones. Thanks to the platform, they can be installed with no particular configuration setup.**

***Index Terms* — SDN; NFV; Fog/Edge Computing; Video Surveillance.**

I. Introduction

A Smart City is a city that leverages on new digital technologies to be efficient, environmentally friendly and socially inclusive for its citizens [1]. Following the traditional theories of urban growth and development, the Smart Cities project [2] identified six axes: smart economy, smart mobility, smart environment, smart people, smart living, and smart governance. In this scenario, there is a lot of interest to services like video crime monitoring, city's Eyes and Ears, smart meters for water and energy management, smart parking, intelligent traffic management, integrated multi-modal transport, tele-medicine & tele-education, emergency management during catastrophic events. A common elementary service needed to realize the above complex services is video surveillance. Many video surveillance platforms exist today, but all of them present severe problems of efficiency and scalability when the numbers of data flow senders and receivers increase.

With this in mind, the target of this work is to present a capillary video surveillance platform for smart cities. As described in the sequel, the main elements of the platform are some nodes that are compliant with the Software Defined Networks (SDN) [3] and Network Functions Virtualization (NFV) [4] paradigms, in order to be scalable and efficient even in presence of variable numbers of senders and receivers.

The power of SDN is based on its characteristic of decoupling control and data planes, moving the network intelligence to a centralized controller; on the other hand, NFV introduces an important change in the network service provisioning approach, leveraging standard IT virtualization technologies to realize network services. With the NFV paradigm, network functions and application services become software instances that can easily be deployed over the network and migrated according to specific policies aimed at optimizing energy efficiency, costs and performance.

Moving from this technical background, the video surveillance platform proposed here allows to easily deploying in the territory of a smart city a huge number of IP cameras and sensors, even installed on drones that rapidly may change their Internet access point. The platform allows to easily and dynamically associate the related video streams and data flows to interested users that may be local police, security forces, administrative entities and even simple citizens.

II. Platform Description

The target of the proposed platform is to provide a video surveillance service that presents the following main peculiarities: open to different video acquiring technologies, plug-and-play, flexible and scalable with the number of transmitting and receiving devices.

More specifically, as shown in Fig. 2, the service is realized with two different kinds of devices: the Smart Access Nodes (SAN) and the Network Access Nodes (NAN). The *SANs* are little boxes distributed on the territory of a smart city to cover small/medium areas (e.g. car park, square, school, roads, highways, and so on) and allowing Data Flow Senders (e.g. camera-equipped drones, video-surveillance cameras, and sensors) to access the platform through Wi-Fi or 4G technologies. *NANs* are the ingress nodes of the Telco Network.

SAN and NAN behave as Customer Premises Equipment (CPE) and Provider Equipment (PE), respectively. Thus, many SANs can be connected to the same NAN. Both SANs and NANs are realized according to the SDN/NFV standard paradigm by using general-purpose x86-based hardware equipped with a software SDN switch and a virtualization

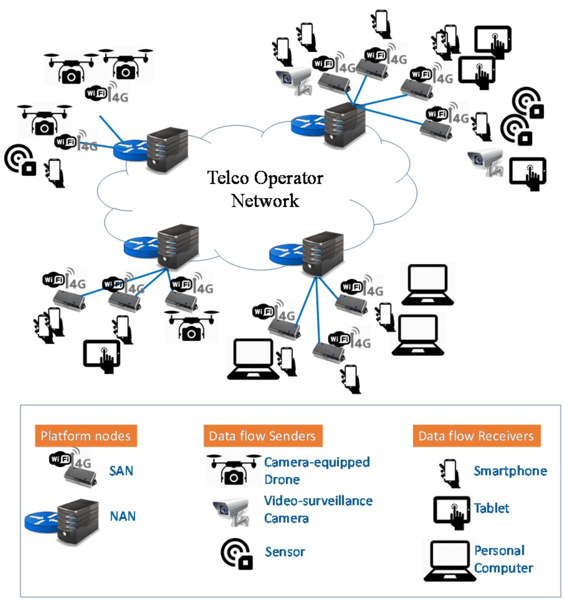

Figure 1. Platform Architecture

This work has been partially supported by the INPUT project funded by the EC (Call H2020-ICT-2014-1, Grant no. 644672).

environment [5-6]. The specific hardware that is used for these nodes depends on the amount of traffic they have to manage, and the complexity of the virtual network and application functions (VF) they have to run.

Each user registered to the platform, through a web site or a mobile app, has a map of the territory covered by the platform (i.e. the smart city), with all the active cameras and the sensors represented by a green circle. Association of one or more cameras to a registered user is done very easily by the same user by clicking on the map viewed on the screen, or through a QR-code that is present in proximity of cameras. The user can then customize the received video and the events associated to each camera, for example requesting to be alerted in case of a motion detection with a specific camera. Other tools are available like for example a mosaic view of flows coming from different cameras. Of course, more than one user can be "interested" to the same camera (for example people that have left their cars in the same parking area).

III. Benefits Achieved with this Technology

Taking into account the state of art of video-surveillance systems that are present on the market today, the proposed platform has the following peculiarities that, in the Authors' view, can stimulate the interest of the main system stakeholders, i.e. Telco Providers, Users and third-party video-surveillance service providers. In fact, thanks to the presence of the SDN/NFV technology used to realize the SANs and the NANs, the platform presents the following key advantages:

1) Reduction of network traffic, with consequent performance improvements. In fact, the data stream generated by each Data flow Sender is automatically rerouted only and directly to the "interested receivers" in a point-to-multipoint fashion, within the network, avoiding any need of over-the-top (OTT) servers, which cause flow replication even for users accessing the network through the same ingress node.

2) Scalability. As said in the previous point, network traffic does not increases when a user requesting a given data flow accesses the network from a NAN where at least one user is receiving the same flow. Moreover, network traffic increase is linear with the number of Data flow Senders.

3) Low end-to-end latency. This advantage derives from the application of the fog-computing paradigm, given that many VFs are provided to the users by their access nodes.

4) OpEx and CapEX reduction, since it is realized by software tools running on general-purpose hardware.

5) Plug-and-Play. Installation of new cameras or other Data flow Sources is trivial because they do not need to be configured: destinations of their video streams are automatically decided by the SDN/NFV Orchestrator.

6) Platform add-ons. Platform is able to support a large number of personalized services (e.g. video cryptography, area monitoring, area obscuring, target follower, mosaic) installed as plugins on some NANs according to the users' requirements. More in detail, according to the kinds of service requested by the end users, each data flow is routed through the set of required VFs organized in service chains; furthermore, the platform is able to easily integrate new plugins in order to integrate new capabilities and provide new functionalities.

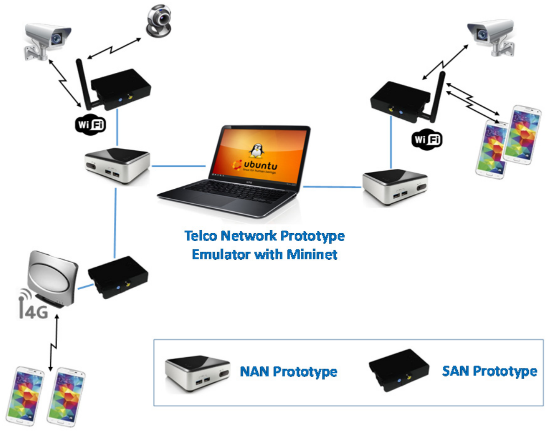

Figure 2. Prototype Description

IV. Prototype Description

The proposed demonstration is shown in Fig. 2. It consists of:

a. *1 PC with MiniNet PC emulator and OpenDaylight SDN Controller*; this PC hosts the network emulator, it is in charge of providing the network emulation and, by means of the OpenDaylight SDN controller, supports the centralized management of the network. At this scope, custom bundles have been developed in order to let the controller expose specific northbound API;
b. *2 Intel NUC Mini PC*, acting as NANs; they use the KVM hypervisor running in a Ubuntu 14.04 LTS environment;
c. *3 RaspberryPi devices*, acting as SAN. They are equipped with WiFi and 4G module to provide connectivity to the IP cameras and end-users requesting the service.
d. *3 wireless IP cameras*, behaving as Data flow Senders;
e. *5 4G smartphones*, running the Android mobile app to allow users to register to IP cameras and receive the relevant video flows;

V. Conclusions and Future Works

Design and deployment of the proposed platform involves and stimulate a multidisciplinary future work, since it involves expertizes in the fields of telecommunications network, computer science, computer programming, data center management, mobile 4G and 5G networks, video encoding, computer forensics, security, web and mobile app design.

References

[1] S. Zygiaris, "Smart City Reference Model: Assisting Planners to Conceptualize the Building of Smart City Innovation Ecosystems," Journal of the Knowledge Economy, Vol. 2, No. 2, 2011.

[2] European smart cities—project. http://www.smart-cities.eu/.

[3] White paper on "Software-Defined Networking: The New Norm for Networks", available at *https://www.opennetworking.org/*.

[4] A. Manzalini et al., "Software-Defined Networks for Future Networks and Services," White Paper based on the IEEE Workshop SDN4FNS.

[5] G. Faraci and G. Schembra, "An analytical model to design and manage a green SDN/NFV CPE node," IEEE Transactions on Network and Service Management, vol. 12, no. 3, pp. 435–450, Sept 2015.

[6] G. Faraci, A. Lombardo, G. Schembra, "A Processor-Sharing Scheduling Strategy for NFV Nodes," Journal of Electrical and Computer Engineering, Volume 2016.

This work has been partially supported by the INPUT project funded by the EC (Call H2020-ICT-2014-1, Grant no. 644672).