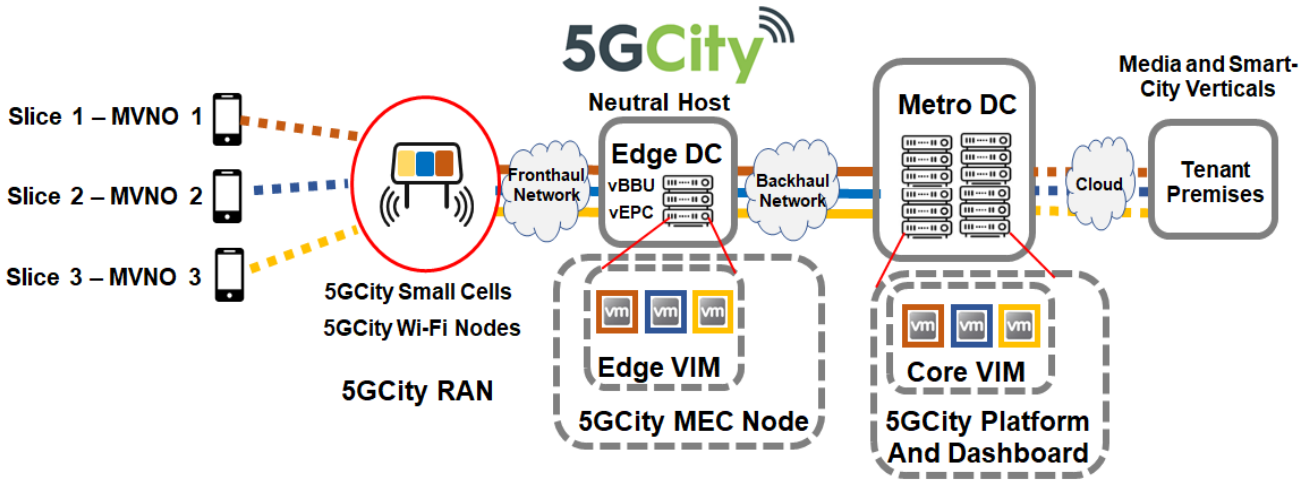
Virtualization at the edge

The virtualization enhancements developed within the 5GCity project have the goal to support the neutral host model for smart city deployments.

The envisioned virtualization technology demands high levels of security and performance with a unified view of sliceable and heterogeneous devices and radio technologies (e.g., LTE, 5G, and Wi-Fi) as well as analysis and design of the Multi-Points of Presence (Multi-PoP) orchestration.

In the **5GCity solution**, **security are enhanced by deploying a robust compute node authentication, monitoring, and geo-tagging.**

Further, wireless virtualization is provided via an innovative multiple RAN controller approach for the management and control of heterogeneous radio resources. In order to be validated, our proposed virtualization approach is being deployed and demonstrated in the cities of Bristol, Barcelona, and Lucca.

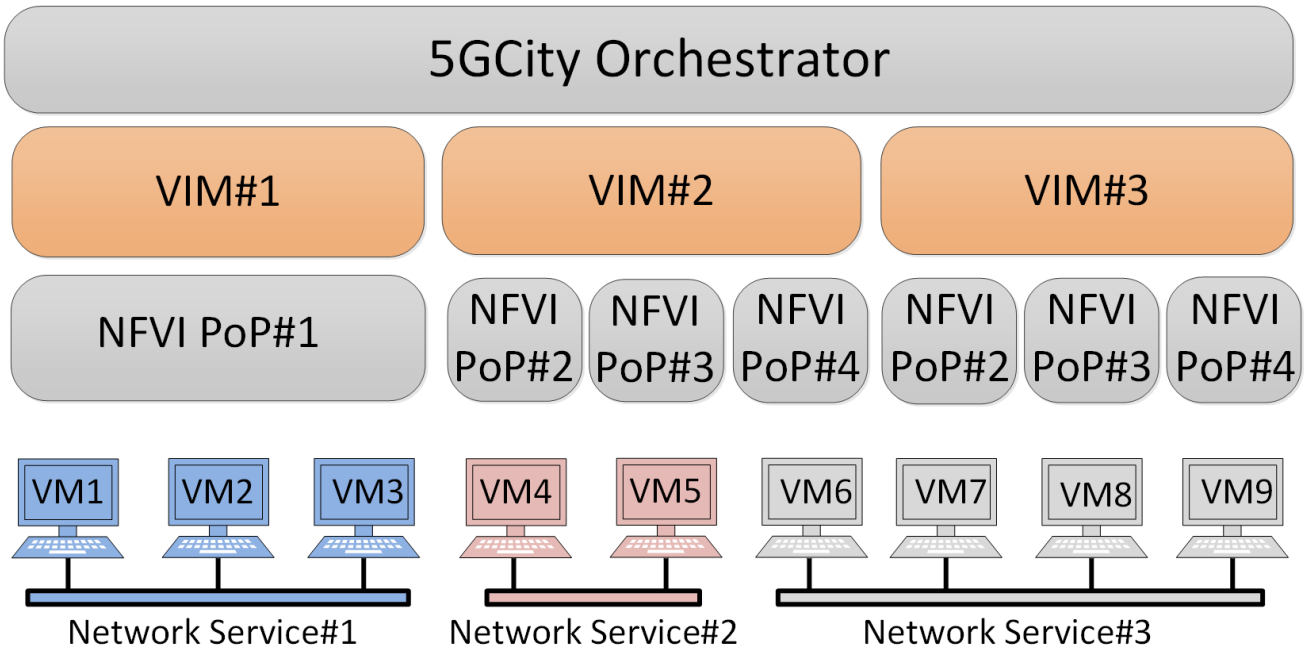


Multi-Points of Presence virtualization

Different scenarios of deployment are enforced by the Infrastructure heterogeneity, geographical constraints, traffic requirements etc where a set of network features will be enabled to support 5GCity architecture and its Use Cases.

- Single domain OpenStack deployment with single controller node collocated with the compute nodes – used in Lab deployments and early stages of demos.

- Single domain Open-Stack deployment with single controller Node and compute nodes at data center and at edge level – Layer 3 (L3) Traffic routing, Neutron DVR and distributed L3 agents.
- Multi-domain OpenStack deployment - Layer 2 (L2) cross-domain networking automation, Tricircle.



EdgeVIM and EdgeNFVI

The 5GCity Edge VIM and Edge NFVI provide a virtualization-based security and trust infrastructure for Arm-based edge devices that enable enhanced security, authenticated devices, geo/asset tagging and secure storage. This infrastructure includes VNF, NFVI and VIM-extensions, setting the ground of security and trust features at the lower level of the software architecture.

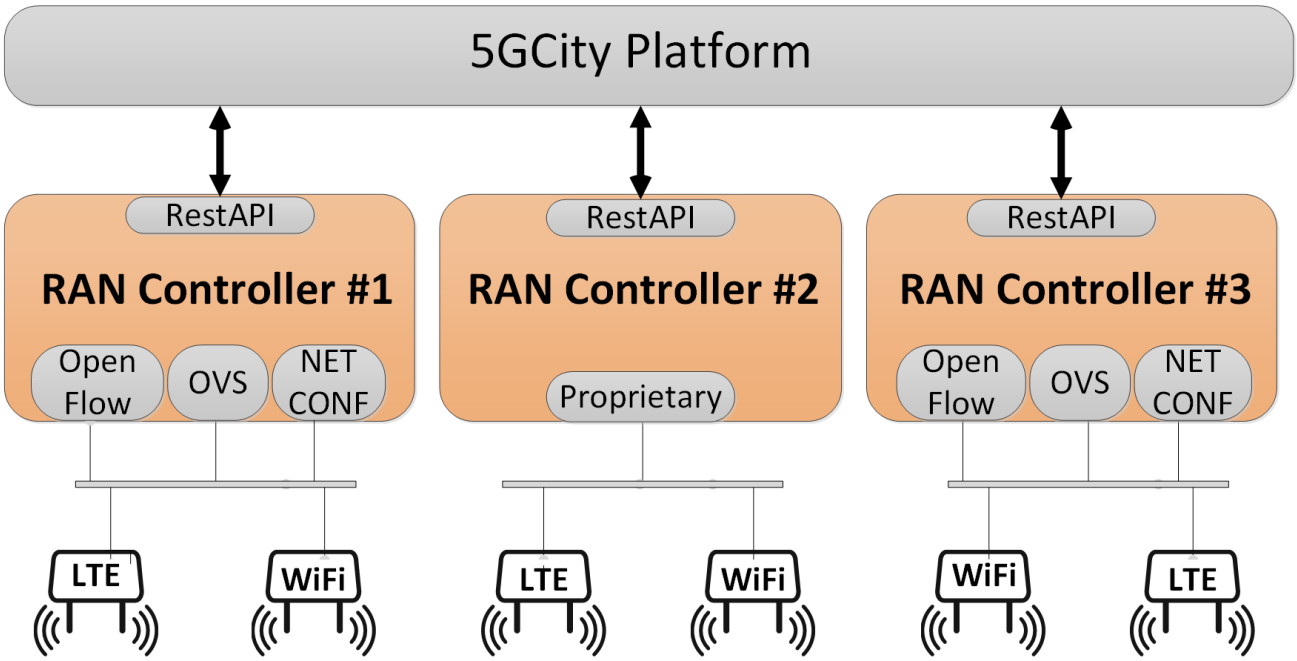
The computational overhead of the added security is measured in an experiment comparing it with a vanilla OpenStack deployment showing a ~2% increase of the average VM creation time, an acceptable result that can be further improved in future implementations.

RAN Virtualization

Why? RAN elements need to be virtualized to allow the instantiation of multiple virtual networks over a single, shared physical infrastructure.

How? Sharing a physical wireless interface among a set of tenants or services and defining a configuration and management plane between the physical devices and the 5GCity platform. In LTE, for each tenant a Public Land Mobile Network (PLMN) ID can be instantiated on the same carrier to differentiate between the tenants, each PLMN ID associated toa different service. In Wi-Fi, this corresponds to instantiating virtual access points on top of physical access points and attaching them to services hosted in the 5GCity infrastructure.

Infrastructure abstraction enables the support of different RAN controllers by 5GCity platform and the integration of the underlying RAN technologies.



The results of this work are published in a WP3 joint paper presented at the 5G World Forum (5GWF'19) in Dresden, October 2019.

Title: Computer and network virtualization at the edge for 5G smart cities neutral host infrastructures

Authors: Michele Paolino, Gino Carrozzo, August Betzler, Carlos Colman-Meixner, Hamzeh Khalili ,Shuaib Siddiqui , Teodora Sechkova, Dimitra Simeonidou, Virtual Open Systems, Nextworks, University of Bristol, i2CAT Foundation, Barcelona, Spain