CHARISMA

Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access

Eduard Escalona
Fundació i2CAT

EuCNC 2015

Project Participants

- Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access

- Consortium members:
  1. *FUNDACIO PRIVADA I2CAT*
  2. *FRAUNHOFER HHI*
  3. *NATIONAL CENTER FOR SCIENTIFIC RESEARCH*
  4. *APFUTURA*
  5. *INNOROUTE*
  6. *INCITES CONSULTING SARL*
  7. *JCP-CONSULT*
  8. *UNIVERSITY OF ESSEX*
  9. *COSMOTE KINITES TILEPIKOINONIES AE*
  10. *INTRACOM SA TELECOM SOLUTIONS*
  11. *TELEKOM SLOVENIJE DD*
  12. *PT INOVACAO E SISTEMAS SA*
  13. *ETHERNITY NETWORKS LTD*

Project Outline

- Start date: July 2015
- Length: 30 months
- Combination of SDN implementations with autonomic **management of resources**.
- **Network security** across multiple virtualised or SDN domains:
  - Definition of threat models and authentication mechanisms across multiple domains
  - Intelligence driven security and data analytics

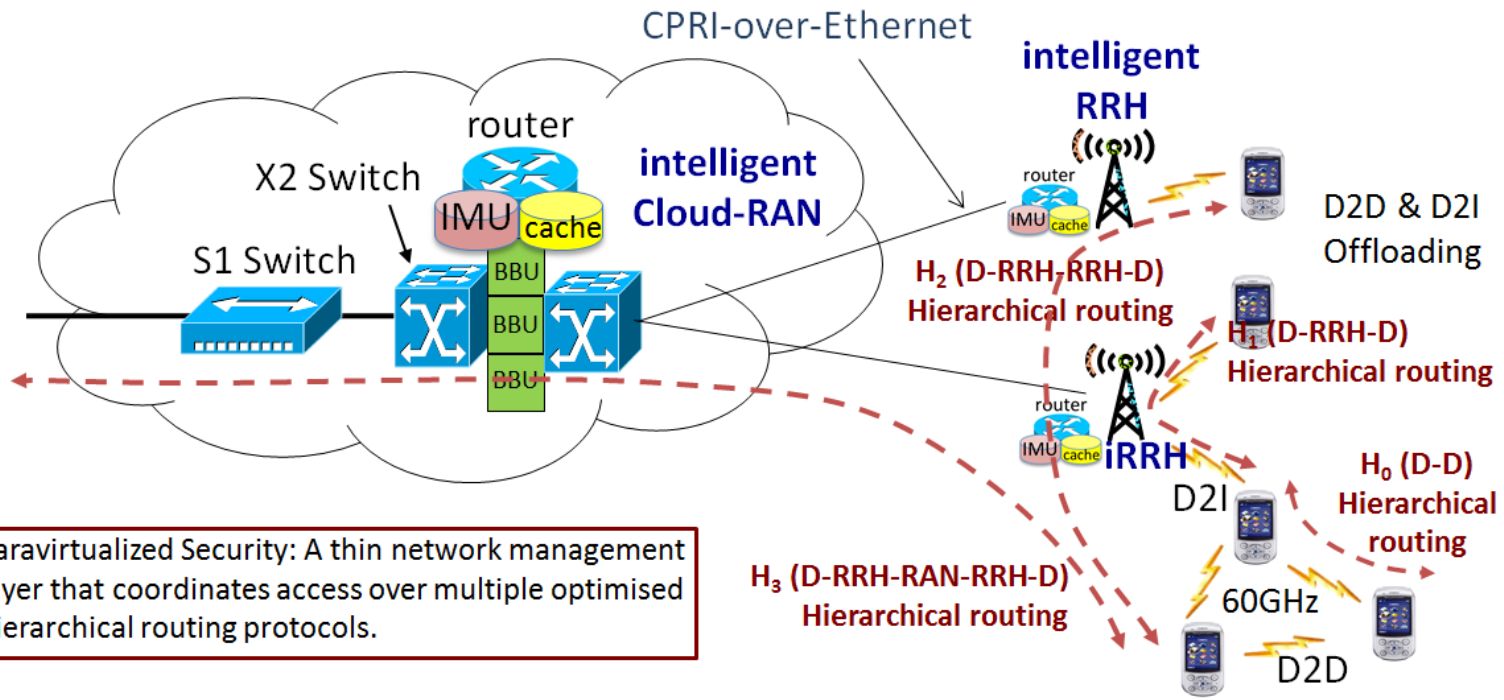
Project Objectives

- CHARISMA proposes an intelligent hierarchical routing architecture that unites two important concepts:
  - devolved offload with shortest path nearest to end-users
  - end-to-end security service chain via virtualized open access physical layer security (PLS).
- CHARISMA architecture aims for future converged wireless and wireline advanced 5G networking.
- Cloud infrastructure platform with increased spectral and energy efficiency and enhanced performance targeting the identified needs for:
  - 1000-fold increased mobile data volume
  - 10-100 times higher data rates
  - 10-100 times more connected devices
  - 5x reduced latency
- Cost savings enabled by SDN

Hierarchical Routing

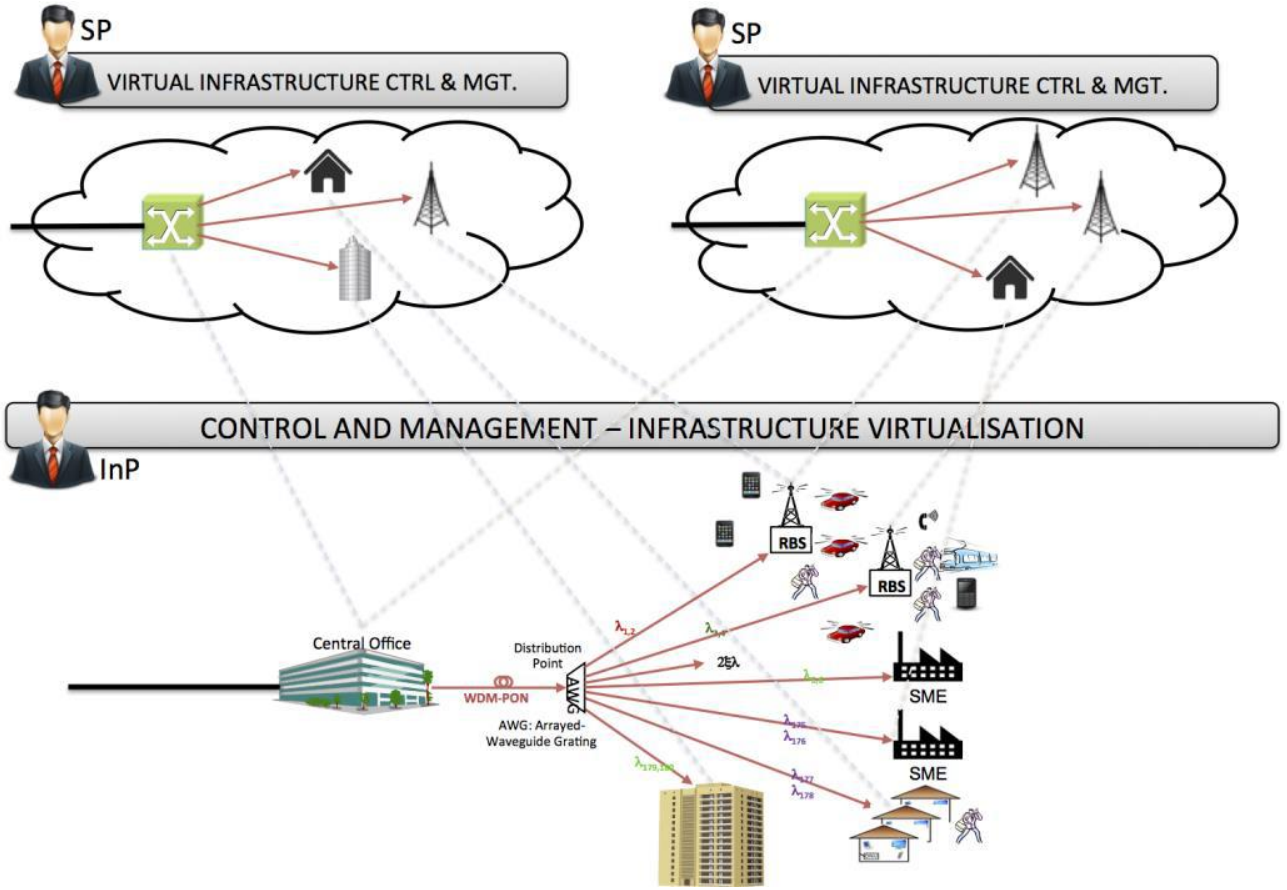
Paravirtualised Secure, Low-Latency Routing Hierarchy:
H_0: D-D (=D2D)
H_1: D-RRH-D (=D2I)
H_2: D-RRH-RRH-D
H_3: D-RRH-RAN-RRH-D

RAN – Radio Access Node
BBU – Base Band Unit
D2D – Device-to-Device
CPRI – Common Public Radio Interface
RRH – Remote Radio Head
IMU – Intelligent Management Unit
D2I – Device-to-Infrastructure



Paravirtualized Security: A thin network management layer that coordinates access over multiple optimised hierarchical routing protocols.

Infrastructure Virtualisation



CHARISMA virtualised C&M converged 5G wireless/wireline infrastructure scenario

Project Objectives

- Distributed security with self-configured setup of secure and fast virtualised sub-networks enables Internet of Things (IoT) and instantaneous machine-type communications (MTC) control.
- End-to-end security based on software-defined networking, physical layer security (PLS), smart-optical hardware pluggable with frame or packet inspection and secure router identification (Trust Node).
- *Virtualized-Security,* featuring
  - End-to-end security service chain
  - Distributed (decentralized) security as opposed to centralized security in 4G
  - Enabling rapid development of novel and flexible security functionalities
  - Physical layer security based on reciprocity in a virtualized open access infrastructure for mobile virtual network operators, network and service providers and physical infrastructure providers.

CHARISMA Security

- ***End-to-end security across all layers of the converged and virtualised open access network.*** Novel cross-layer approaches for e2e security derived from software security, network coding, deep packet inspection and physical layer security.

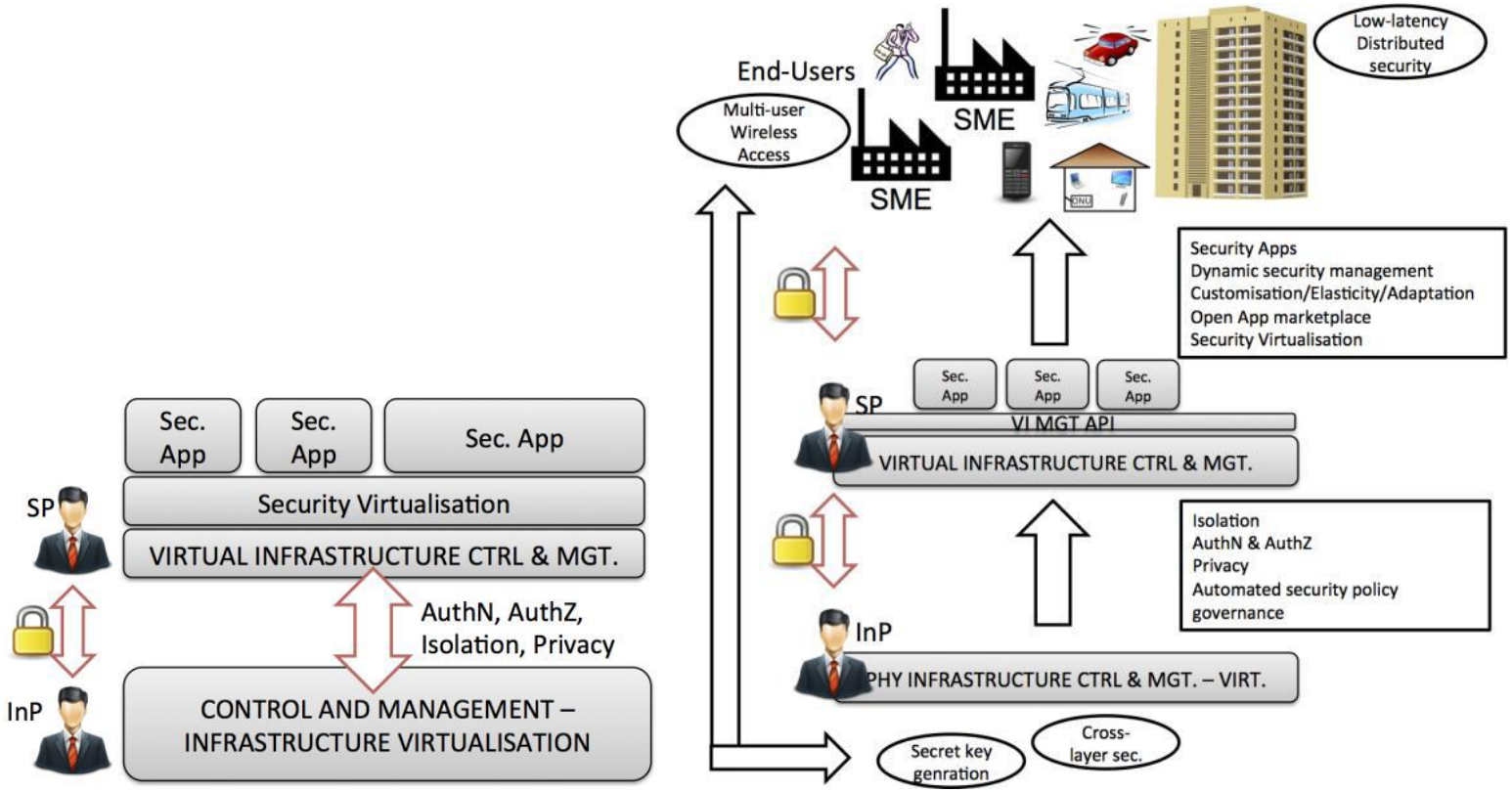
- ***Data Confidentiality***. CHARISMA will investigate novel Physical Layer Security (PLS) approaches for secret key generation at the physical wireless/optical layer in the framework of shared randomness in communication channels with impaired reciprocity. Lightweight secure network coding approaches will be sought offering data confidentiality through virtualized software pieces;

- ***Data integrity*****.** Deep packet inspection (DPI) of virtualised security functions, dynamically deployed and combined with behavioural modelling of the virtualized network components, can identify spam attacks, detect intrusions or anomalous behaviours;

- ***Provider isolation***. New methodologies providing isolation between tenants of the physical infrastructure. We will exploit information-centric network (ICN) concepts and software-defined networking (SDN) to provide separation based on the content compared to the traditional VLAN mechanisms used within data centres;

- ***Authentication and Authorisation***. Recursive trust delegation mechanisms will be exploited for the different stakeholders' relationships involved in open access networks. Role- and policy-based authorisation mechanisms .

Virtualised Security



CHARISMA virtualised security functions and security service value chain