5GUARDS

Dynamically setting up 5G local network slices for security and safety services

SMART CITIES

More and more security and safety services are exploring the (cost-saving) potential of automated security technology for securing industrial sites, facilities and large public events. Consequently, they increasingly make use of public communication networks (including wireless access networks) for automated and controlled tasks – from control rooms at on-site central or remote locations. Current 4G networks are however not able to fulfill the stringent end-to-end quality-of-service (QoS) requirements of these security services – in terms of low latency, high-throughput, high-quality streaming.

In the context of 5GUARDS, the project consortium wanted to investigate how the network slicing concept of future 5G networks could provide the means to meet the connectivity requirements of these security services. “Network slicing aims at providing the ability to allocate resources on demand by creating multiple isolated logical networks on top of a common shared physical infrastructure”, explains Tijs Grootjans, project lead of the 5GUARDS project. “We primarily focused on emergency or operational use cases for 5G network slicing in the public (e.g. fire departments) and industrial (e.g. large industrial sites) sectors.” A major asset of the project is the involvement of multiple industrial and academic players who cover the complete 5G network – from the radio link over the radio access network to the core network.

The outcomes

1. Core slicing: architecture for setting up security slices, and algorithms for automatically placing virtual network functions

The project partners defined an architecture which provides the ability to on-demand set up security slices completely isolated from other network slices to ensure reliable communication independent of the traffic load on the underlying physical mobile network. In this way, the required quality of service for security applications can be achieved with the cost efficiency of a common mobile network. They also designed algorithms for automatic placement and chaining of virtual network functions on the physical infrastructure under constraints of latency, legislation, or hardware-related aspects. Simulation results have shown that the provider revenue can be improved significantly through coordination of the composition and embedding tasks. Both an exact algorithm for optimal placement and a scalable heuristic for large networks have been developed, improving the acceptance ratio with 15% over existing (exact) algorithms.

2. RAN slicing: new mechanism for migrating terminals to and from security slices

Mechanisms have been designed for dynamically creating QoS-guaranteed security slices in the access node, connecting them to the appropriate core slice, and migrating terminals to and from this security slice when emergency situations arise. For the particular case of unmanned aerial vehicle (UAV)-based security solutions, the altitude dependence of interference has been studied: the optimal altitude of the UAV flight varies between 10-22.5 meters depending on the considered environment (rural, suburban or urban). The potential of massive multiple-input multiple-output (MaMIMO) beamforming technique was also investigated. The partners conclude that for sub-6GHz frequencies, usage of beamforming can be extremely beneficial and 30dB improvement of signal-to-interference-plus-noise ratio (SINR) can be achieved. Looking further, the use of mm-wave frequencies can offer a wide bandwidth suitable for high-throughput slices. Using adaptive beamforming procedures, such a link could easily transport data from cameras on-board of drones or other high-throughput equipment over several hundreds of meters.

3. Dynamic software reconfiguration: enabling network control to become directly programmable

As part of the project, software-defined networking (SDN)-principles were applied in combination with the 5G architecture to achieve network programmability and a well-defined interface for applications. With SDN, it is possible to apply 5G slicing concepts on large-scale networks, reconfiguring core and access point nodes to allow separation of high priority and best effort network traffic. A mathematical approach based on integer linear programming (ILP) was designed and implemented, allowing to evaluate the optimality of network flow allocations in cases where high-priority traffic must take precedence over other network traffic.

Download the leaflet

Download leaflet 5GUARDS

5GUARDS

Dynamically setting up 5G local network slices for security and safety services.

5GUARDS is an imec.icon research project funded by imec and Agentschap Innoveren & Ondernemen.

It ran from 01.04.2017 until 31.03.2019.

Project information

Industry

- Accelleran
- Ericsson Belgium
- Orange Belgium
- Rombit

Research

- imec - IDLab - UGent
- imec - IDLab - UAntwerpen
- imec - Persys
- KU Leuven - ESAT-TELEMIC
- imec - SMIT - VUB

Contact

- Project Lead: Olivier Van Rompaey
- Research Lead: Steven Latré
- Proposal Manager: Werner Van Leekwijck
- Innovation Manager: Stefan Van Baelen