Interconnected IoT Smart Spaces

Requirements from a critical 5G vertical

G. Carrozzo*, G.Insolvibile*, M. Pardi*, N. Ciulli*, Sergios Soursos**, Ivana Podnar Žarko§,
* Nextworks, Pisa, Italy, Email: {g.carrozzo, g.insolvibile, m.pardi, n.ciulli}@nextworks.it
** Intracom SA Telecom Solutions, Athens, Greece, Email: souse@intracom-telecom.com
§ University of Zagreb, Faculty of Electrical Engineering and Computing, Zagreb, Croatia, Email: ivana.podnar@fer.hr

***Abstract*— IoT is recognized as the key vertical technology area that will deeply integrate and make use of the upcoming innovative 5G network control and localization solutions. Industry 4.0 for future factory automation, Intelligent Traffic Systems (ITS) for autonomous vehicles, eHealth for smart medicines packaged with wireless modules, and Smart Energy are some of the key 5G vertical scenarios which all have IoT platforms as core enabling technology. This paper presents some key design results on the interoperation of IoT Smart Spaces from the H2020 symbIoTe project and derives some specific requirements on 5G networks originating from the design and implementation activities on IoT Smart Spaces.**

Keywords*— *IoT, interoperability of Smart Spaces, 5G Verticals

I. INTRODUCTION

IoT is commonly recognized as one of the key vertical technology sectors which is motivating research of new network transmission and control technologies in 5G [1]. Smart objects living in IoT platforms are generally low power, energy efficient devices (with battery operation of 10 years or more, require low latency (below 1ms) to implement a fast loop of sensing-reaction-control and as typically deployed in large set (>100K per area) thus posing scalability issues to the overall functional and connectivity control. Smart devices deployed in smart IoT spaces have also specific needs in terms of QoS, reliability, security, and privacy, above all when applied/deployed in industrial environments. Examples of these smart environments are the interconnected smart home and the smart office when commuting within the smart city, or smart airports/train stations, stadiums or shopping malls, where it is increasingly critical to efficiently orchestrate the control of the various sensors and actuators deployed in the smart networked environment.

IoT is a critical vertical business on top of the 5G network. The state of the art is fragmented in a large series of silo/proprietary solutions, which on the one hand integrate connected objects within local environments/ smart spaces (e.g., home, office, etc.), and on the other hand connect smart spaces with back-end cloud hosting components. Interoperability and federations of IoT platforms are not a market reality today yet, and there is limited collaboration and access to services and resources provided by the different IoT platforms. The H2020 symbIoTe project [2] is working exactly to remedy this fragmented environment, and proposes to converge towards an interoperation framework and architecture for various IoT platforms. In symbIoTe, various platform federations can securely interoperate, collaborate and share resources. Even more important, through symbIoTe smart objects can migrate among IoT domains and platforms, thus implementing a "smart object roaming" (ref. Fig. 1).

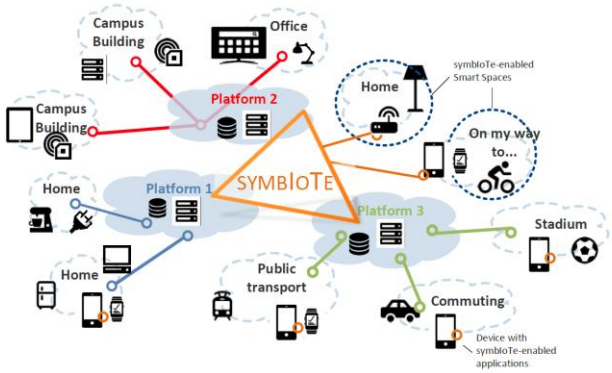

Fig. 1. Different IoT islands and ecosystems integrated in symbIoTe

This paper presents some key aspects of the symbIoTe research on the interoperation of IoT Smart Spaces which translate into requirements for the 5G network. In fact, IoT interoperation can be realized with current networks but definitely benefits of the 5G solutions for highly performant connections and flexible control to implement reliable and efficient control loops.

II. SYMBIOTE SMART SPACES

The symbIoTe Smart Spaces (SSP) are environments (residence, campus, vessel, etc.) where one or more IoT platforms provide coordinated services. Such environments are typically related to a physical space (e.g. a smart residence space is bound to a house or building), but in the more general case SSP can extend to a broader physical space (e.g. a smart campus or smart city), leveraging on highly performant network connections and services in between.

An SSP comprises both virtual and physical objects, such as gateways and smart objects. To cooperate in a federated system like symbIoTe, the SSP needs to include a series of modules to enable operations related to authentication, authorization, discovery and registration of smart objects, as well as to resource access [3]. The key design objectives that should be pursued to implement SSPs can be summarized in:

- Dynamic discovery and automatic configuration of resources
- IoT platform interoperability at the SSP level
- Support for nomadic devices
- Resource access always guaranteed and very low latency connections for control loops (e.g. for actuation of commands from an IoT controller).

The SSP as a whole exposes (i.e. register, provide access to) the resources it contains, regardless of which "local" IoT platform they belong to. Since each IoT Platform manages its own devices according to its internal protocols (which shall remain opaque for the overarching cross-platform control and orchestration), discovery and auto-configuration functions remain in charge of the specific IoT Platform but results communicated to the cross-platform layer through a unified information model and proxy functions.

Functional elements of the SSP are depicted in Fig. 2.

- The **InnKeeper** is a module that allows a new device to register to the SSP and keeps a registry of locally registered IoT apps and smart devices.
- The **Resource Scanner** scans the local network for well-known devices and device gateways (e.g. Z-Wave devices/gateways, Smart TVs, storage systems, etc.).
- The **Resource Access Proxies (SSP RAP and SDEV RAP)** allow direct access to the Smart Space and Smart Device resources respectively. They can also act as network controllers to coordinating access to the wireless medium.

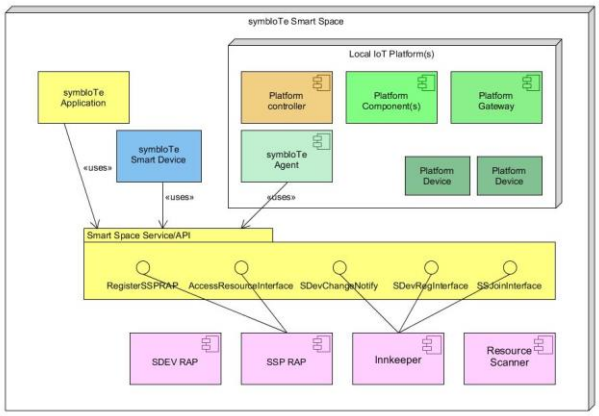

Fig. 2. symbIoTe Smart Space architecture

The Cloud Domain provides unified and secure access to platform resources which have been registered to third parties. It also allows the formation of platform federations, where collaborating platforms can easily exchange information and perform bartering and trading actions. Depending on the IoT platform to be integrated, the Smart Space Middleware needs to be deployed either as a cloud component or at intermediate edge cloud facilities or within the local platform. To optimize the performance of the IoT sensors-actuators control loop in this structured environment from the cloud to the edge down to the platform, it is general design choice to implement cross-platform functions in a way that can be hierarchically deployed from the Cloud Domain down to the Smart Space and dynamically reused and re-planned/re-deployed to adapt topology or scenario changes or to better respond to the roaming of users across the various interconnected spaces. In this context, having the possibility to rely on extremely reliable and very low latency network connection, isolated connectivity environments and automatic network function deployment control tools (SDN/NFV) is of critical importance.

In particular, network slicing has emerged as a most promising game changer in NFV/SDN-enabled 5G networks. A network slice in 5G is defined as a logical infrastructure encompassing several communicating functional elements -- some of them specific to a vertical industry -- that are realized over a shared physical infrastructure. Apart from the network specific aspects of a network slice (i.e. software-defined stitching of virtual network functions), from a purely IoT perspective the allocation of a 5G network slice involves the configuration of the underlying physical infrastructure and connectivity services capable to meet the requirements of an IoT system (ref. Fig. 3).

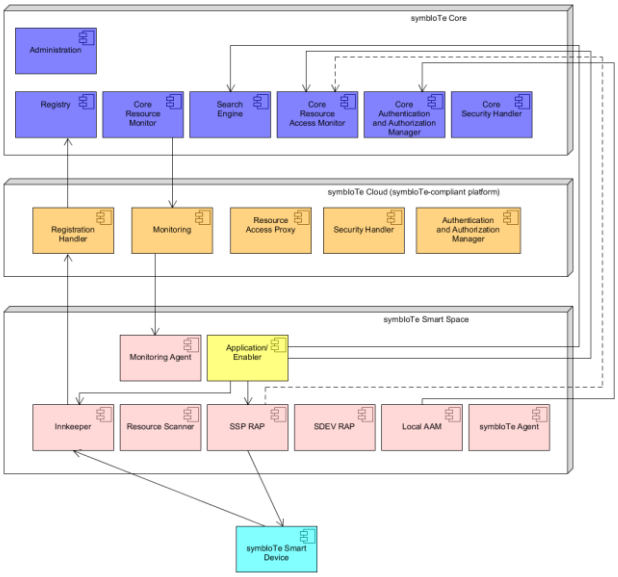

Fig. 3. Split of functions across the Application, Cloud and SSP domains.

ACKNOWLEDGMENT

This work is supported by the H2020 symbIoTe project, funded within the EU Horizon 2020 framework programme under grant agreement No 688156. Authors thank the entire symbIoTe consortium for the valuable discussions.

REFERENCES

[1] 5GPPP, 5G empowering vertical industries, https://5g-ppp.eu/wp-content/uploads/2016/02/BROCHURE_5PPP_BAT2_PL.pdf

[2] H2020 symbIoTe project, https://www.symbiote-h2020.eu/

[3] symbIoTe deliverable D4.1, "symbIoTe Smart Space Middleware Tools, Protocols and Core Mechanisms", Feb. 2017, https://www.scribd.com/document/338680628/D4-1-symbIoTe-Smart-Space-Middleware-Tools-Protocols-and-Core-Mechanisms